TURNING THE TIDE AGAINST ONLINE CHILD SEXUAL ABUSE

MICHAEL SKIDMORE,
BETH AITKENHEAD and RICK MUIR

JULY 2022

THE POLICE FOUNDATION
The UK's policing think tank

TURNING THE TIDE AGAINST ONLINE CHILD SEXUAL ABUSE

Acknowledgements

This study would not have been possible without the generous support of the Dawes Trust, to whom we are very grateful. The views expressed in this report are solely those of the authors.

We would like to express our gratitude to the NSPCC, the National Crime Agency, the National Police Chiefs' Council and others from across the police service, for the invaluable support that was given to this research. Furthermore, we would like to thank the many practitioners who gave up their valuable time so the work could benefit from their knowledge and experience.

Finally, the team would also like to express their gratitude to all those who attended meetings of the project's National Advisory Board, whose feedback and insight has been invaluable.

About the Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Its mission is to generate evidence and develop ideas which deliver better policing and a safer society. It does this by producing trusted, impartial research and by working with the police and their partners to create change.

Cover: istockphoto

CONTENTS

GLOSSARY

CAID	Child Abuse Image Database
CEOP	Child Exploitation And Online Protection Command
CSA	Child sexual abuse
CSAE	Child sexual abuse and exploitation
CSAM	Child sexual abuse material
CSE	Child sexual exploitation
KIRAT	Kent Internet Risk Assessment Tool
MLAT	Mutual Legal Assistance Treaty
NCMEC	National Center For Missing And Exploited Children (US)
OCAG	Online child abuse activist groups
P2P	A network of computers in which users can communicate and share files stored on their computer with other users on the network (ie Peer-to-peer)
ROCU	Regional Organised Crime Unit

A note on terminology

We are conscious that there can sometimes be negative connotations associated with the term “victim” and therefore some people prefer “survivor”. We entirely respect this view, however, for the purposes of this report we have tended to use the word “victim” as this is the term used most frequently with statutory agencies such as law enforcement, whose effectiveness is the subject of this report. In using this term we understand it to mean all those who have experienced crime, irrespective of whether it has been disclosed or the criminal justice outcome.

SUMMARY

The internet has enabled the production and consumption of Child Sexual Abuse Material (CSAM) on an industrial scale. It has also created new opportunities for adults to sexually abuse and exploit children. The volume of online child sexual abuse offences is now so great that it has simply overwhelmed the ability of law enforcement agencies, internationally, to respond. However, there is nothing pre-determined about this situation. Public policy can make a difference. This report looks at what can be done to help "turn the tide" on online Child Sexual Abuse (CSA). It does this by first describing the scale and nature of online CSA, second, assessing the ability of the police and law enforcement to investigate these crimes, third, by examining the service provided to victims of online CSA and, finally by looking at what more can be done to prevent online CSA in the first place.

THE SCALE AND NATURE OF ONLINE CHILD SEXUAL ABUSE

Online CSA is now a high-volume crime: in a single year Facebook alone reported 18 million CSA images on its platform and at least 13 per cent of children claim to have experienced sexual solicitation online whether from another child or an adult. Technological advances and the introduction of more robust legislation has led to more of these offences being identified and for the police, this has created a monumental surge in demand on criminal investigation and child protection services. There was over a 450 per cent increase in sexual grooming offences reported between 2016-17 and 2020-21 and the volume of obscene publications offences (most of which relates to CSAM) has increased by over 800 per cent since 2012-13.

There is a diversity of underlying online and offline behaviours and abuse depicted in CSAM, ranging from a consensual image-exchange between two children to the recording of the rape of a child by an adult perpetrator. As children get older and gain more freedom to go online, the risk of exposure to online solicitation increases. While most children do not experience these kinds of harms on the internet some are particularly vulnerable. Research indicates that the children most at risk are those who for various reasons find it harder to establish relationships offline, who are lonely or isolated or who are attracted to risk taking behaviour. . In 2019 the Internet Watch Foundation (IWF) found that most of the images it identified depicted children below the age of thirteen and a third had been generated by the children themselves.

The internet has lowered the barriers to engaging in all types of CSA offending. It provides a space for child abusers to expand and diversify their previous offending behaviour and an entry point both for individuals with a deviant sexual interest including those who might otherwise never have committed a sex crime. Serious CSA offending is enabled by an internet environment that allows otherwise isolated offenders to form online communities which can encourage and promote extremely serious sexual abuse.

Online CSA offenders are a highly diverse group. They can be broadly located within a pyramid structure, with most offenders at the bottom of the pyramid whose offending is confined to less serious (in relative terms) CSAM offences (the viewing of images), followed by those who groom and sexually exploit children online, through to a smaller number who also commit serious contact abuse offences. An offender's position within this pyramid structure may not be fixed over time, and an overriding concern among authorities is the prospect that CSAM offenders (those viewing images online) may escalate to the most serious crimes.

The relationship between online CSA and other forms of sexual abuse is poorly understood. The evidence demonstrating a linear pathway from CSAM offending to more serious abuse is mixed. Many perpetrators of serious offline abuse also engage in CSAM offences, but evidence from the police and offender support services suggests that large numbers of those who are arrested for CSAM offences are not found to be involved in other forms of abuse. Research shows that contact sexual abuse occurs in response to a wide range of factors that can include CSAM offending and a sexual interest in children, but also other risk factors that include opportunities in the home or local community (i.e. access to children) and deviant personality disorders. Participation in online sexual grooming can indicate a motivation to meet and abuse children but for large numbers of offenders the offending is confined to online spaces. All of this offending is serious and important to deal with, but a robust evidence base is vital to be able to assign priority, resources and interventions effectively to deal with the most serious offending and the highest risk.

Recommendation 1

The National Police Chiefs' Council and the National Crime Agency should commission research to improve its empirical understanding of online CSA offences, the offenders who commit them and their risk profile. This would support more informed and targeted resource allocation and strategic decision-making and would enable practitioners to make more accurate assessments of risk.

INVESTIGATING ONLINE CHILD SEXUAL ABUSE

Demand on the police in terms of recorded CSAM offences increased by 121 per cent between 2015 and 2018, although some of the larger forces have seen increases many times that, including in one an increase of 437 per cent.

As the caseload has risen, the proportion of recorded offences leading to a positive criminal justice outcome has fallen. The number of reported cases that led to a charge or summons fell from 51 per cent in 2014 to just 9 per cent in 2018. This in part reflects the growing use of 'Outcome 21', a diversionary measure for those suspects under the age of 18, which was used in just 0.4 per cent of cases in 2014 but in 31 per cent of cases by 2018.

The fact that just one in 10 cases led to a positive criminal justice outcome is also reflective of the complexity of investigating online CSA. Gathering digital evidence is inherently complex due to the growing volume of devices and data, the use of anonymisation technologies by offenders and the cross-border nature of the investigations which require the cooperation of law enforcement and private sector actors overseas. Requests for legal assistance from overseas territories is a prolonged and highly precarious process which can impede both criminal investigation and safeguarding efforts.

Recommendation 2

Working with international partners, the Home Office should look into how it can speed up the mutual legal assistance treaty process, the process of securing legal cooperation in other countries.

A single online CSA case crosses into the remit of multiple organisations (for example, law enforcement partners, children's services and technology companies) in multiple law enforcement jurisdictions. However currently, a decision to invest resource can be swiftly undermined due to the challenge of different public authorities working to different priorities and standards. There is no universal language of risk and harm. For example, there may be considerable investment by an investigation team in the National Crime Agency to develop intelligence on a suspected CSAM offender, which may be swiftly undermined if the recipient police force assesses that the case does not constitute a risk and so a response is not in the public interest. There needs to be greater consensus around what constitutes risk and what factors should drive priorities across different public agencies in relation to online CSA.

Recommendation 3

We recommend that the National Crime Agency explores the feasibility of establishing common standards for risk assessment and case prioritisation across policing and partner agencies.

To manage the high demand arising from reported CSAM, the police use the Kent Internet Risk Assessment Tool (KIRAT) to prioritise and sequence their investigations. Practitioners told us of a number of problems with the risk assessment process which should be addressed: many suspects are simply assigned as low risk because of a lack of available information, some practitioners lacked an understanding of the contextual factors that might contribute to risk and the focus was solely on the risk of contact abuse rather than the risk of a suspect committing serious online offences such as grooming or exploitation. Work to refine this assessment tool is underway, which is critical to ensure the police can target resources to the cases that present the greatest risk.

Recommendation 4

The National Police Chiefs' Council should continue to review the prioritisation framework used by police forces (KIRAT) to address existing gaps and to ensure that it takes into account the risk of a suspect engaging in serious online offending.

Specialist teams collect huge volumes of CSAM during their investigations of suspects and face the substantial task of processing and grading these images for administrative and legal purposes. This task takes up considerable amounts of resource but more importantly, there are ongoing concerns about the psychological harm that this continuous exposure to CSAM can cause to police staff. There have been advancements in the technology, notably the Child Abuse Image Database for processing known CSAM, but more is needed to alleviate this burden on police staff.

Recommendation 5

The Home Office and police forces should increase their investment in technologies to process, analyse and grade CSAM. These tools need to be embedded in the work of all specialist investigation teams.

In recognition of the potential harms caused by this exposure to CSAM, specialist investigations teams implement rigorous protocols and supervision to support their staff. However, in some police forces the volume of CSAM suspects exceeds the capacity of specialist teams. Consequently, cases are assigned to officers outside of these teams and without access to this intensive support network.

Recommendation 6

Police forces should actively monitor the impact of CSAM investigations on generalist officers and staff. They need to establish channels for accessing support that are clearly communicated to encourage officers or staff who are negatively impacted by their work to seek help.

Given the rising volume of CSAM offences referred to the police there are serious capacity issues at all levels of investigation. 69 per cent of senior stakeholders reported insufficient resource in their digital forensic teams to tackle online CSA and 52 per cent reported insufficient resource in their specialist investigation teams. An even higher proportion (72 per cent) reported a lack of resource in their local police teams, and 59 per cent in their generalist investigation teams. As a result of capacity issues in specialist teams CSAM cases can be passed to generalist officers who often lack the training to investigate and identify risk appropriately.

There are significant skills gaps throughout the workforce: for example, 64 per cent of staff in dedicated online CSA roles had not completed the specialist child investigation training course. When asked if they thought officers in generalist teams received sufficient training to respond to online CSA only a third thought that there was sufficient training in online investigation and only 40 per cent thought that there was adequate training in collecting and managing digital evidence. The main barrier identified was the absence of core digital training programmes for officers in non-specialist roles.

Recommendation 7

As part of a wider strategic assessment of workforce skills, the National Police Chiefs' Council and the College of Policing should map current skills against required capabilities in relation to tackling online CSA. This exercise should then inform a new national plan to recruit and train the people required to address identified skills deficits.

Given the speed of technological change police information systems are creaking under the pressure to collect, process and assess the vast amounts of data collected in the search for evidence and intelligence on offending and risk. 60 per cent of CSA leads described the management of digital evidence as a very significant challenge.

Recommendation 8

Over the next decade the government should increase investment in the information technology required to keep pace with the changing threat of online child sexual abuse.

Law enforcement agencies should take a more proactive approach in relation to online CSA, focusing on safeguarding children and targeting the most serious offenders who would otherwise remain unidentified.

Currently too much work is focused on investigating private sector referrals of CSAM offences, large volumes of which involve low risk suspects. The way resources are prioritised needs to be reviewed to ensure that there is more of a balance between investigating reactive CSAM referrals (suspects viewing images online) and proactively identifying the harder to find offenders who are perpetrating the most serious abuse.

Recommendation 9

The National Police Chiefs' Council and the National Crime Agency should review their approach to risk and proportionality in relation to CSAM offences. The aim should be to protect more children from harm by dedicating more investigative resource at proactively identifying serious offenders, in particular those involved in grooming and possessing first generation material.

The experience of arrest for CSAM offences can have a profound impact on an individual's personal, family and working life. Both police data and practitioner accounts highlight the significant risk of suicide within this group of offenders. In 2014 these cases constituted almost a

quarter of suicides occurring during the course of police investigations. The police have begun to systematically collate suicide data from police forces which is an important step to accounting for their effectiveness in managing these suspects.

Additionally, arrests can have a huge impact on the suspect's family. They may be left with questions about the nature of the offence, the risks the suspect poses to them and other criminal justice processes. In some cases the support given to suspects' families is limited.

Recommendation 10

We recommend that police forces collate robust statistics on suicides and attempted suicides linked to CSAM suspects and national statistics should be published annually by the National Police Chiefs' Council. Appropriate support services should be engaged to minimise the risk of suicide among this group.

Recommendation 11

The National Police Chiefs' Council should commission research to understand the gaps in emotional support for families affected by the arrest of an online CSA suspect. This should provide the basis for greater support for these family members.

In recent years there has been a rise in so-called "paedophile hunters", groups of vigilantes operating online to identify child sex offenders. Online vigilantism is likely to remain a permanent part of this field, given the inevitable constraints on law enforcement to proactively detect and disrupt all online offenders and the fact that the internet creates opportunities for citizen-led investigation. These groups can produce vital new leads, but some groups can also impede investigations for example, by producing inadmissible evidence, while others have a primary focus on meting out their own vigilante justice. This can lead such groups to act illegally and to people being publicly "named and shamed" for an unproven offence. For these reasons there is a need to steer these groups away from harmful or counterproductive practices.

Recommendation 12

We recommend that the police continue to use evidence produced by online citizen groups where appropriate but that they should also make available structured guidance for those who wish to work lawfully and cooperatively to limit the potential for harm.

There is a tension in the investigation of online CSA between focusing on the most harmful offenders (such as those who are physically abusing local children or who are engaged in serious online abuse such as the live-streamed sexual abuse of children overseas), versus responding to the very large volumes of CSAM referrals that come from the private sector and which generally involve lower risk offenders whose activities are limited to viewing non live material on the internet.

Investigators told us that the focus on investigating CSAM offences reported by the private sector very often leads them to low-risk offenders (i.e. the investigation does not identify their involvement in other forms of sexual abuse), meaning that most do not receive a custodial sentence and for convicted offenders in the community, the resources for effective offender management are very limited. The limitations in the criminal justice outcomes, services for managing and addressing risk, mixed with the sense that current reactive strategies are failing to target the most harmful offenders, suggests there is a need to change the way lower risk offenders are dealt with.

Research has found very low rates of recidivism from CSAM-only offenders and that for many, the experience of police arrest and a programme of education would likely be sufficient to divert them from further offending. Taking a different approach to this group would alleviate pressure on the criminal justice systemensure more of these offenders are rehabilitated by being referred to appropriate services, while allowing the police to focus their efforts on those who pose a risk of serious harm to children.

Recommendation 13

A criminal investigation remains essential in each CSAM case to identify those in which there is a risk of more serious sexual abuse. Where none is discovered however the police should be able to issue a conditional caution to CSAM only offenders with the following provisions:

- As a minimum, the offenders should be mandated to attend an educational course at their own expense. The courses would communicate the harms from these crimes, address criminogenic attitudes, give information on the law and signpost additional services if needed.
- Compliance with these conditions would be monitored and criminal sanctions imposed in the event of a breach.
- Appropriate safeguarding controls should be in place. Each offender would remain

on police systems so that their risk to the community could be monitored. and with their participation in the scheme revealed via enhanced DBS checks so that they could never work in a role involving contact with children.

This scheme should be trialled in the first instance and would be subject to a full evaluation.

The majority of criminal investigation is focused on addressing the risk of contact sexual abuse from online offenders. This is the case across all law enforcement, including police investigations of local suspects and the proactive online investigations in specialist NCA and Regional Organised Crime Unit (ROCU) teams. The focus on addressing contact abuse is understandable in an area of crime that is both high volume and high risk, and where there is a need to prioritise and target resources. However, this has left a blind-spot in relation to the high volume of CSA which remains confined to online spaces notably the growing volume of cases involving online perpetrators who groom and sexually exploit children and young people in the UK or overseas. Online offending can have a huge impact on victims. More robust systems are needed to account for these online harms and more effective interventions needed to pursue and disrupt the most serious online offenders.

Recommendation 14

The National Crime Agency and the National Police Chiefs' Council should jointly develop a more robust framework for understanding online harm, including for example an index which could guide practitioners to focus on the highest risk offenders.

Recommendation 15

The National Crime Agency should establish a new specialist investigation team that operates in parallel with existing units, but with a specific remit to target, investigate and disrupt offenders who are causing the most serious online harm. The remit of this team would be to investigate online abuse or exploitation reported by victims in the UK and also, cases detected (but not pursued) in the proactive investigations of existing teams. This team should also develop its own capabilities to proactively investigate and disrupt online offenders and networks, working in collaboration with overseas law enforcement agencies.

VICTIM CARE AND SAFEGUARDING

Police forces not only investigate those suspected of committing online CSA but also have a role in identifying and supporting victims. In one police force, 36 per cent of local online CSA demand pertained to a local victim, most commonly of grooming or other sexual activity offences. Whereas the response to CSAM suspects falls to dedicated teams with specialist expertise, the response to victims of online CSA falls predominantly to generalist officers who manage these crimes alongside their wider workload. Inevitably, this introduces inconsistency into the way practitioners identify and manage the risk contained in each incident. Dealing with sensitive cases is complex and challenging, particularly where a child may not acknowledge that they are a victim and given the challenges of digital investigation.

Recommendation 16

The College of Policing should review the training that is provided for generalist constables in providing support to victims of online CSA.

Moreover, there is less of a clear remit for pressurised support services in local authorities that mainly focus on traditional forms of CSA (such as intra-familial abuse).

Our evidence from support services indicates that victims and their families can lack the confidence in their own understanding of the offence and the role the police have in responding, with the consequence that online crimes go unreported. Victims who report crimes do not just want a positive criminal justice outcome, they also want sensitive treatment by officers, timely information, support services where needed and recognition from the state of the harm they have experienced. Many are also in need of protective interventions to avoid repeat victimisation, including information and advice on safe behaviours to avoid further harm or a referral to more intensive support services for children who are at an ongoing risk, especially those who are groomed and sexually exploited. The support services will commonly advise victims and families to report abuse to the police, although they weren't confident about how the police service would respond.

Online abuse can represent offending that is limited to online spaces or can extend from (or into) exploitation in the community (for example, grooming by adults already known to the child or exploitation by local peers). Many of the challenges around identification and intervention are similar to those seen in cases of child sexual exploitation rooted in offline relationships and behaviours. In this context, research has highlighted the

importance of understanding contextual factors in the social or physical environment that underpin the abuse or harmful behaviours. The contextual safeguarding model advocates identifying and targeting interventions to address situational drivers of exploitation in the local community. However, in the case of online situational drivers, which are much less stable and often beyond the reach of practitioners, its application is much less clear.

Recommendation 17

We recommend that the Home Office commissions research on how contextual safeguarding can be provided in an online context.

A significant proportion of the CSAM offences that are reported to the police involve offenders who are themselves children or young people. In one police force, 37 per cent of CSAM suspects were aged under 18 and over three quarters of these were female. In 2018, 41 per cent of all suspects in England and Wales were female, the majority of whom were likely to be aged under 18. The underlying drivers for these offences are not known. Some youth-produced sexual imagery may arise as a result of grooming or sexual exploitation, but the majority is most likely the product of wider social trends affecting a generation of young people entering the developmental stages of their sexuality in a digital age. A survey of young people aged 13 to 17 revealed that 7 per cent had taken and shared a sexual image of themselves.

The fact that under current law any child taking a picture of themselves and sharing it with a peer is guilty of a child sex offence is on the face of it bizarre and has prompted calls for the law to be updated. Defenders of the status quo argue that the law suppresses these risky behaviours among children and young people. However the data indicate that a deterrent approach is not working.

Children would be better safeguarded and supported through education on the nature and risks of online abuse and how to keep themselves safe online Under existing policies, the police do not record a criminal offence against young people (instead utilising so called Outcome 21), however the discretion available creates the potential for inconsistency. Moreover, criminalisation of these behaviours is a cause of tension for victims of abuse and their families, who wish to report a crime but fear criminalising themselves in the process. The result is that some serious cases of online abuse go unreported. A change to the law would shift the onus to welfare and education practitioners, who have the knowledge and capability to guide and support young people and at the same time help to ensure that law enforcement can focus on tackling sexual abuse and exploitation.

Recommendation 18

There should be clearly defined exemptions to the Obscene Publications Act based on age and consent. This would move the emphasis away from law enforcement and towards education and awareness-raising in cases where children are sharing pictures of themselves with other children.

The global connectivity provided by the internet means that there is a responsibility on the police to help identify victims in other countries. Proactive investigation is needed to first identify so-called “first generation” images of recent abuse and second, identify and locate the victim so as to initiate a local response to protect them from the offender and further abuse. The National Crime Agency (NCA) undertakes a great deal of this work, however local investigation teams have a responsibility to identify immediate safeguarding concerns when processing CSAM recovered during their investigations. Proactive victim identification is a relatively new role in policing that calls for a distinctive set of capabilities and our evidence showed local police teams lacked a common understanding of the role and requisite capabilities. It also highlighted the complex and resource-intensive nature of these investigations, exacerbated by the continuous pressure to respond to the high volume of CSAM offenders reported by the private sector.

Recommendation 19

There is a need to consolidate victim identification capability, potentially using a hub and spoke model in which the National Crime Agency at the centre coordinates the activities of victim identification officers in local jurisdictions, with clear lines of accountability to the National Crime Agency for activity and outcomes.

The police have a central database of CSAM that has been subject to examination in previous investigations, but there remains a reliance on manual processes for processing new CSAM and cross-referencing different files to develop new intelligence.

Recommendation 20

As part of proactive safeguarding police forces should develop and embed the use of software to automate and speed up the triage process for identifying newly identified (or ‘‘first generation’’) images and to also identify files containing the same individuals using facial recognition software.

PREVENTION

Preventing harm to children is better than reacting to it once it has occurred. There is a need for a much more systemic approach to prevention in relation to online CSA.

Looking first at protecting potential victims, 89 per cent of police strategic CSA leads told us that education to change the behaviours of local children was very important, more than for any other prevention strategy. 57 per cent believed education and awareness for adult guardians was very important. 51 per cent believed that regulation of the technology industry was very important and 37 per cent thought the same about improved controls and security on online platforms.

Turning to offenders, much more could be done to divert less serious CSAM offenders away from an offending pathway, including targeted communications on URLs in open and dark web spaces that are known to contain CSAM. There is also a need for diversion initiatives that would offer therapy and support to those who understand that they have a problem and are willing to address it. It is much better if we can divert people early on from engaging in these offending behaviours. Currently the Lucy Faithfull Foundation is the largest and most accessed charity providing support and therapeutic services, but it primarily deals with offenders who have already been arrested.

Recommendation 21

The government should invest more in offender treatment services to tackle the behaviours of those who recognise they have problem and are willing to address it.

There are distinctive challenges in monitoring and managing the behaviour of convicted offenders, including the requirement to manage behaviour in more concealed online spaces, the technical capabilities required to do this and the challenge in assigning finite resources to low risk offenders. We found there was wide variation in the resources and capabilities available to teams in different locations, most notably in the availability of technological solutions to facilitate the processes for monitoring offender behaviour and risk.

Recommendation 22

The National Police Chiefs' Council should invest more in the technology required to monitor the activity of convicted online offenders and there should be stronger common standards in relation to the technical capabilities available across police forces.

Education and awareness campaigns should aim to provide children with the knowledge to navigate the internet safely, by helping them understand the signs of grooming or exploitation for example. Such campaigns should also target those young people who may be putting themselves at risk or posing a risk to others, signposting them to support. Education must also also be targeted at parents to help them provide effective guardianship in a changing online environment. Frontline police officers should receive more training on the advice they should be providing to children, parents and schools.

Recommendation 23

The government should review the effectiveness of current work in relation to educating both children and parents about the risks of online CSA.

Recommendation 24

The National Police Chiefs' Council and the College of Policing should review the training available for frontline police officers in providing preventative advice to children and parents in relation to online safety.

Much more could be done to design out online CSA offending through greater use of pop-up warnings and signposts for support and the more widespread adoption of identity authentication. Internet companies should also be deploying the latest means of detecting online CSA on their sites. There is a momentum in government to diversify its approach to tackling online CSA, reflected in the CSA strategy and in particular the Online Safety Bill (HM Government, 2021; UK Parliament, 2022). The Police Foundation's Strategic Review of Policing suggests going further by imposing a duty on private sector corporations to protect consumers from crime, regulated by a dedicated Crime Prevention Agency (The Police Foundation, 2022). This would deliver a more systemic approach to the prevention of online CSA.

1. INTRODUCTION

In the relatively recent past child sexual abuse principally involved physical abuse and mainly took place in family settings. Child sexual abuse material (CSAM) or what used to be widely referred to as "child pornography" was very difficult to access, with hard copy material having to be smuggled by a dedicated group of offenders across international borders. There was little opportunity for people to find such material and therefore only the most determined offenders could get hold of it.

The internet and the associated digital revolution have changed this completely by massively expanding the opportunity for people to share and view abusive material. This includes very many people who, in the absence of the internet, would be unaware that they had a sexual interest in children.

The internet has enabled the production and consumption of online CSAM on an industrial scale. It has also created new opportunities for adults to communicate with children for the purposes of sexual abuse and exploitation. There can be a relationship between online and offline abuse although this happens in complex ways which we shall discuss in this report. The volume of online child sexual abuse offences is now so great that they have simply overwhelmed the ability of law enforcement and policing agencies internationally to respond.

This report seeks to provide a better understanding of the problem of online CSA and to suggest ways of making our response to it more effective and of keeping more children safe from harm. The report has four objectives: it describes the scale and nature of online CSA as its affects children in the UK and internationally, it examines the effectiveness of the policing and law enforcement response to online CSA, it looks at the service provided to victims of online CSA and, finally, it explores what more can be done to prevent the proliferation of online CSA. Throughout, the report makes a number of recommendations for change aimed at both policymakers and practitioners.

THE APPROACH

A mixed-methods approach was used to address our main research questions, including both quantitative and qualitative analyses. The aim was to develop a national perspective on the scale and nature of the problem and response, by getting the perspective from multiple stakeholders operating at the national, regional and local level and where possible, analysing national level data. This national perspective was then contextualised by an in-depth examination of the problem and the response in two police force areas. Our data sources are described in the table below.

Practitioner interviews

Semi-structured interviews were completed with 67 practitioners from a range of sectors. These took place between April 2019 and March 2020. Forty-four interviews were conducted with law enforcement and policing representatives including 14 from the National Crime Agency (NCA) and Regional Organised Crime Units (ROCUs) and 19 from two police forces which provided extensive access to the full range of staff linked to the response. 14 interviewees were from third sector support and advocacy services, eight of whom were practitioners working for the NSPCC. Eight interviews were conducted with stakeholders in the private sector and one with an academic involved in relevant research.

National law enforcement survey

The survey was sent to senior strategic lead officers in all 46 police forces in England and Wales (including the British Transport Police), Scotland and Northern Ireland, and all 10 ROCUs in England and Wales. We received completed surveys between July and August 2019 from 35 police forces/ROCUs. The survey questions covered themes that included the nature of demand and their workforce, resources, decision-making and response to online CSA.

National police data

We received national police data on two Home Office offence categories; “take/make/distribute indecent photographs or pseudo-photographs of children” and “possession of an indecent or pseudo-photograph of a child”. This data represented 42 out of the 43 police forces in England and Wales, covering the five-year period from January 2014 to December 2018. It included aggregated data on the volume and nature of recorded crimes and the linked suspects and victims.

Local police force data

A single police force shared raw data for all crimes with a link to online CSA recorded during an 18-month period between April 2018 to September 2019. An initial dataset was extracted which incorporated all Home Office offence codes pertaining to child sexual abuse. In order to isolate those relevant to online CSA the sample was then refined in stages; first, all offences of indecent images of children and sexual grooming offences were incorporated; second, all other offence-types recorded with a “cyber flag” were retained; and finally, a manual free-text search of the offence summaries (searching for “online” and “image”) was completed. On this basis, a total of 2,151 offences were extracted for analysis.

Literature review

We reviewed the relevant literature across the major themes examined, including the scale and nature of offending and risk, the experience and needs of victims, law enforcement and crime prevention in the context of online CSA. This included reports published by government and other stakeholders and academic articles.

2. THE SCALE AND NATURE OF ONLINE CHILD SEXUAL ABUSE

In this chapter we set out the scale and nature of online child sexual abuse. First, we define what we mean by online child sexual abuse. Second, we describe how big a problem it is, both in terms of its prevalence in society and its representation in demand on policing and law enforcement agencies. Third, we describe the profile of online CSA victims, the kind of harms they are subjected to and what we know about vulnerability and risk. Finally, we describe the characteristics of online CSA offenders. Understanding the very different types of offender, their motivations and the risk they pose to children is crucial to developing an effective response.

2.1 DEFINING ONLINE CHILD SEXUAL ABUSE

This report uses the term online child sexual abuse (CSA) to include crimes that fall into the categories of child sexual abuse and child sexual exploitation as defined by the government:

> *"(CSA) involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children."*
>
> **(HM Government, 2018)**

> *"Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology."*
>
> **(Department for Education, 2017)**

These definitions incorporate a range of sexual offences that are either directed at victims, or in the case of engaging with sexual images of children, represent crimes against the state. The legislation setting out these criminal offences includes:

The Obscene Publications Act (1959): This includes the offences of **"taking, making, distributing or publishing indecent images or pseudo-images of children"**, and **"possession of an indecent image of a child"**.[1] Indecent images refer to sexualised images of children and young people, referred to by some as "child pornography" but in recognition of their abusive nature, these are collectively referred to as Child Sexual Abuse Material (CSAM) throughout this report (images can be the product of abuse but also generate a risk of abuse to children who create and share sexual images of themselves).

Sexual Offences Act (2003): This includes the offences of **"meeting a child following sexual grooming"** which is committed when a person aged 18 or over knowingly meets someone under 16 to perpetrate a relevant sexual offence.[2]

Serious Crime Act (2017): This introduced a new offence which criminalised **any person aged 18 or over who knowingly engages in a sexual**

1. https://www.cps.gov.uk/legal-guidance/obscene-publications -
2. https://www.legislation.gov.uk/ukpga/2003/42/notes/division/5/1/15 -

communication with a child under 16; including sending a sexual communication themselves or encourages a child to make a communication that is sexual.[3]

Child sexual abuse and exploitation can be experienced by any child under 18, though there is some disparity in the age parameters across different legislation. The age at which a child can legally consent to any form of sexual activity is 16, but in the case of children depicted in CSAM, a child is defined as any person aged under 18.[4]

The online element

In the same way the division between every day online and offline life has blurred, the definitional boundaries that delineate online and offline crime have become increasingly difficult to draw. In examining cybercrime, the "cyber" element can mean different things to different people (Brown, 2015). The government and law enforcement in the UK put cybercrime into the following categories, broadly reflecting whether the existence or scale of an offence-type is dependent on the availability of information and communications technology (ICT):

- Cyber-dependent crimes "are offences that can only be committed by using a computer, computer networks, or other form of ICT."
- Cyber-enabled crimes "are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT."
- Cyber-assisted crime "use networked digital technologies … in the course of criminal activity which would take place anyway."

(Levi et al, 2015; McGuire and Dowling, 2013)

Much online CSA represents cyber-enabled offending, especially indecent image and sexual grooming offences which have been fundamentally changed in size and shape by technology. This includes offending by children and young people who take, make or share indecent images of themselves. Technology can intersect with other forms of abuse, including rape and sexual assault. Online spaces can either provide a meeting point or enable an offender to groom or exploit a child already known to them offline. In this regard, some abuse moves closer to the definition of a "cyber-assisted" crime.

In focusing on the law enforcement response, the definitions used in this study will in general mirror the data, structures and resource in policing and law enforcement for tackling online CSA, which are principally configured to manage cyber-enabled CSAM and sexual grooming and communications offences. The latter can range from persistent or insidious attempts to lure the young person into a sexual encounter on or offline, or "fleeting" communications that involve inappropriate sexual comments or questions (Wager et al, 2018).

2.2 THE SCALE OF ONLINE CHILD SEXUAL ABUSE

Although it is difficult to piece together an accurate picture of scale, due to the hidden nature of this type of offending, it is no exaggeration to say that it is taking place on an industrial scale, indicated by reports and referrals from those providing internet services, victimisation surveys and reports to the police.

Online child sexual abuse material identified on the internet

The true scale of online CSAM is unknown. This is because most offences are not reported to the police, these offences principally take place in private and anonymously (Wolak et al, 2005) and there are limits on the ability of law enforcement and other agencies to proactively look for material (for example, see Hurley et al, 2013; Smallbone and Wortley, 2017).

However, we do have data from reports of CSA material identified across the internet and this reveals very large volumes of abusive material on both the open and closed web.

First, most CSAM material, contrary to popular belief, is found on the open internet. The US based National Center for Missing and Exploited Children (NCMEC) collates intelligence on CSAM and sharing activity identified by web companies located in the US. In 2020 they received over 21.7 million reports of CSAM; this includes reports from the public, but the majority (21.4 million) were from companies (predominantly Facebook, now known as Meta).[5] The large tech companies receive user reports and use automated search algorithms to proactively seek out this material. In a six-month period between April and September 2021,

3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/604931/circular-commencement-s67-serious-crime-act-2015.pdf
4. https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children
5. https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf

Facebook or Meta (incorporating Facebook, Instagram and WhatsApp) took action to address 46.5 million pieces of content which it suspected to be linked to child sexual exploitation.[6]

In 2017 the Canadian Centre for Child Protection launched Project Arachnid, a web crawler which automates the search for known CSAM (using photoDNA) and is also directed by intelligence to suspected forums and chat rooms. Over approximately two years it identified 7.4 million suspected CSAM files, leading to 1.6 million take down notices sent to US and Canadian host sites or referred to the INHOPE network.[7] These figures demonstrate that the production and viewing of CSAM is a high-volume crime.

Second, there is material located on file sharing or storage sites. The Internet Watch Foundation (IWF) is a UK-based charity that receives reports from members of the public as well as referrals from the Project Arachnid web crawler. They have seen year-on-year increases in the volume of URLs (or web addresses) that contain CSAM. They identified 252,194 URLs in 2021, an increase of 707 per cent since 2014 (31,266) (IWF, 2020; IWF, 2022). The continuous rise in CSAM will in part reflect the continuous improvements in the technology to discover these images. Very few of the sites hosting CSAM were based in the UK (just 0.15 per cent) with a large proportion (41 per cent) being based in the Netherlands. Very little of the CSAM identified by IWF is located on mainstream social networking sites, with 90 per cent removed from "image hosting boards" and "cyber lockers",[8] often involving companies that are not household names (Home Affairs Committee, 2020). The same pattern was found across the international counterparts of the IWF which collectively identified 223,999 CSAM files in 2018 and the majority were found on image (84 per cent) or file host sites (7 per cent) (INHOPE, 2019).

Peer-to-peer (P2P) networks[9] are one of the most popular channels for accessing and sharing CSAM (Europol, 2019), with an estimated 1 per cent of searches on these networks pertaining to CSAM (Hurley et al, 2013). In a single year (2010-11) there were over 870 million occurrences in which a known CSAM image was shared between two different computers. Just 1 per cent of CSAM was hosted on servers in the UK with 90 per cent hosted in Brazil (Steel, 2009). However, it is estimated that 6.5 per cent of the global demand for CSAM on P2P networks emanates from the UK (Steel, 2009).

Finally, there is material located on the dark web. Globally in 2018, there were 2.88 million online accounts registered with the most harmful CSA dark web sites (NCA, 2019) and the NCA estimates there are 250,000 offenders in the UK accessing CSAM on the dark web (NCA, 2020). The vast majority of sites hosting CSAM are on the open web, but the number identified on the dark web is growing, and each can contain thousands of links to CSAM files (Wager et al, 2018). In 2019 the IWF identified 288 new sites on the dark web (IWF, 2019) and Project Arachnid has reportedly detected approximately 5,500 sites hosting CSAM.[10]

There is a two-way flow of CSAM between the dark and open web with CSAM made available to dark web users by sharing encryption keys to encrypted files on the open web that are otherwise undetectable to the legitimate host.[11] One study identified a small proportion of P2P network users who also operated specialist software for accessing the dark web (Hurley et al, 2013).

6. https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/#content-actioned)
7. https://www.iicsa.org.uk/key-documents/15963/view/HOM003278_001-003.pdf
8. Image hosting boards and cyber lockers are a service provided by a third-party company, providing remote and secure storage of media files and data (including cloud storage) and enable file sharing.
9. Peer-to-peer networks are free and publicly accessible to individuals who download software that connects their computer to other users (or 'peers') in the network, and they contains millions of users globally who use these networks to share and gain free access to popular music, films and other media.
10. https://www.iicsa.org.uk/key-documents/16869/view/CRS000031_031-032.pdf
11. https://www.iicsa.org.uk/key-documents/16869/view/CRS000031_031-032.pdf

The scale of victimisation reported in surveys of adults and children

One of the best ways to understand the prevalence of child sexual abuse is to ask adults and children, through victimisation surveys, whether they have experienced it. In the year ending March 2019 the Crime Survey for England and Wales found that 7.5 per cent of adults had experienced some form of sexual abuse by an adult or child perpetrator before the age of 16 (ONS, 2020). Although as we shall see police recorded child sexual offences have been rising in recent years, the evidence suggests that we have not seen an actual increase in child sexual abuse. Tentative findings from an analysis of survey data indicate that between the late 90s and 2009 there was a slight decline in forced or coercive sexual activity experienced by those under 18 (Radford et al, 2011).

In terms of the experience of online abuse, the Crime Survey for England and Wales shows 5.3 per cent of women and 1.2 per cent of males aged 18-24 had experienced "non-contact abuse"[12] before the age of 16[13], and for women, this is slightly higher than seen in some of the older age categories, indicating a rising trend.[14] The impact that the proliferation of digital technology and media will have on future prevalence is uncertain, but the indications are that online sexual communication involving children is pervasive; one study found between 13 and 19 per cent of children had experienced sexual solicitation online from either an adult or young person and approximately 5 per cent had found the experience distressing (Ospina et al, 2010).

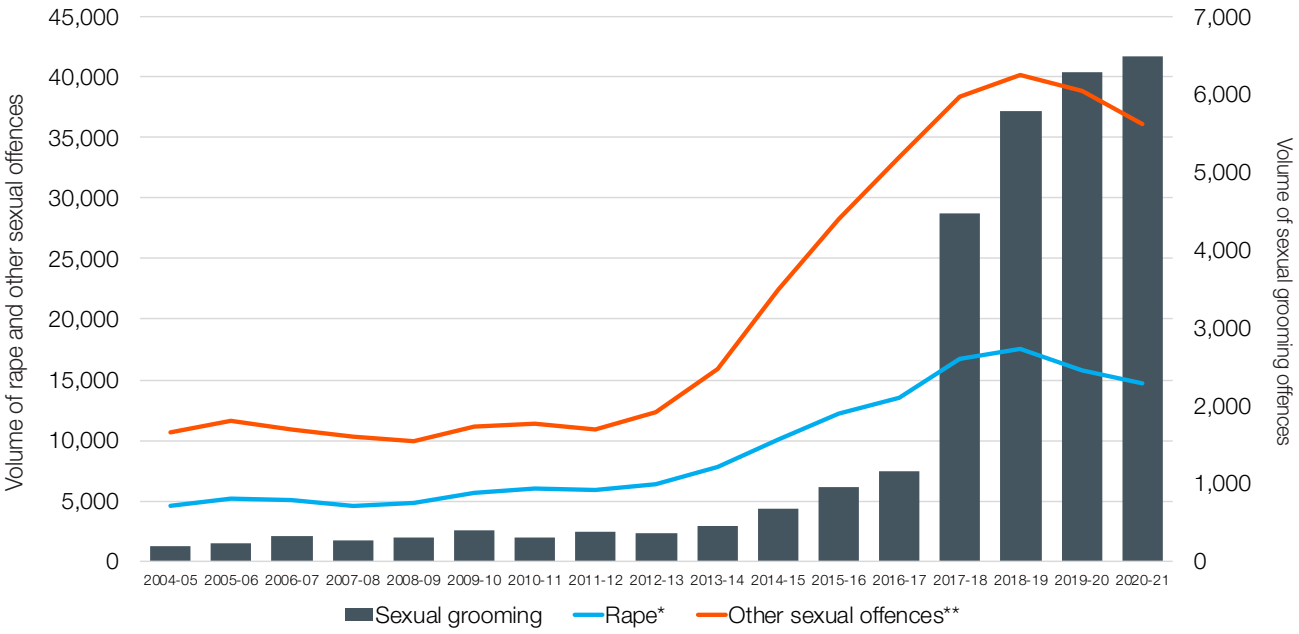
The NCA produced an estimate by comparing data for all convicted child sex offenders on the sex offender register and online offenders (presumably linked to CSAM or grooming offences) discovered through proactive investigation (NCA, 2021).[15] They estimate that there are currently 700,000 UK-based offenders that present "varying degrees of risk to children". This risk encompasses the wide spectrum of offending from CSAM to the most serious crimes such as rape.

Online child sexual abuse reported to the police

We have seen huge growth in reports of CSA to the police in recent years. In 2020-21 there were over 57,312 recorded child sexual abuse offences in England and Wales, more than double the volume recorded in 2013-14 (24,085) (see Figure 2.1).[16] The overall rise in volume reflects increased reporting from victims (including non-recent abuse), improved recording by police and more proactivity to uncover abuse and exploitation. The volume of sexual grooming offences represents a small proportion of overall CSA offending; in 2020-21 it made up 11 per cent of these crimes. However, Figure 2.1 shows a surge in the volume of sexual grooming offences recorded by police, rising by over 450 per cent from 2016-17 to 2020-21, most likely as a result of the introduction of the Sexual Communications Act in 2017.[17,18]

12. Non-contact sexual abuse includes incidents in which someone made the individual watch or listen to sexual acts or look at sexual images; made or shared sexual images of them; deliberately exposed themselves to them; or sent them sexual images or videos of themselves or others.
13. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/childsexualabuseinenglandandwales/yearendingmarch2019
14. In retrospectively asking adults about their experiences of sexual abuse, the crime survey may not adequately represent current trends and context, most notably the significant rise in access to electronic devices and online communications by children and young people in recent years (for example, see Ofcom, 2020).
15. This is called the 'mark and recapture method' that uses inferential statistics to extrapolate from the volume of known entities and estimate the size of the total population (i.e. UK-based CSA offenders).
16. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables
17. The introduction of the Sexual Communications Act in April 2017 introduced new offences for perpetrators who engage in sexual communication with a child, irrespective of their intent or action to commit a subsequent contact offence. Previously, these offences may have not been recorded or captured under other sexual grooming or sexual activity offences.
18. Comparatively, recorded crimes offer a partial measure that lags behind actual patterns in offending due to high levels of under-reporting; some victims are unwilling or unable to disclose the abuse, due to fear or having been groomed by the offender (for example, see Alaggia et al, 2017). Many who experienced rape (76 per cent) or non contact abuse (60 per cent) did not report the abuse to anyone at the time of the offence (ONS, 2020). Local victim data also overlooks the capacity for local online offenders to cause harm outside of the UK, thereby omitting online grooming or exploitation or the facilitation of contact abuse of children and young people overseas.

Figure 2.1 Trends in child sexual abuse offences recorded nationally by police, April 2004 to March 2021[19]



* Includes rape of a male or female under 13 and rape of a male or female under 16.

** Includes sexual assault on a male or female under 13, sexual activity involving a child under 13 or under 16, unlawful sexual intercourse with a girl under 13 or under 16, abuse of children through sexual exploitation and gross indecency with a child.

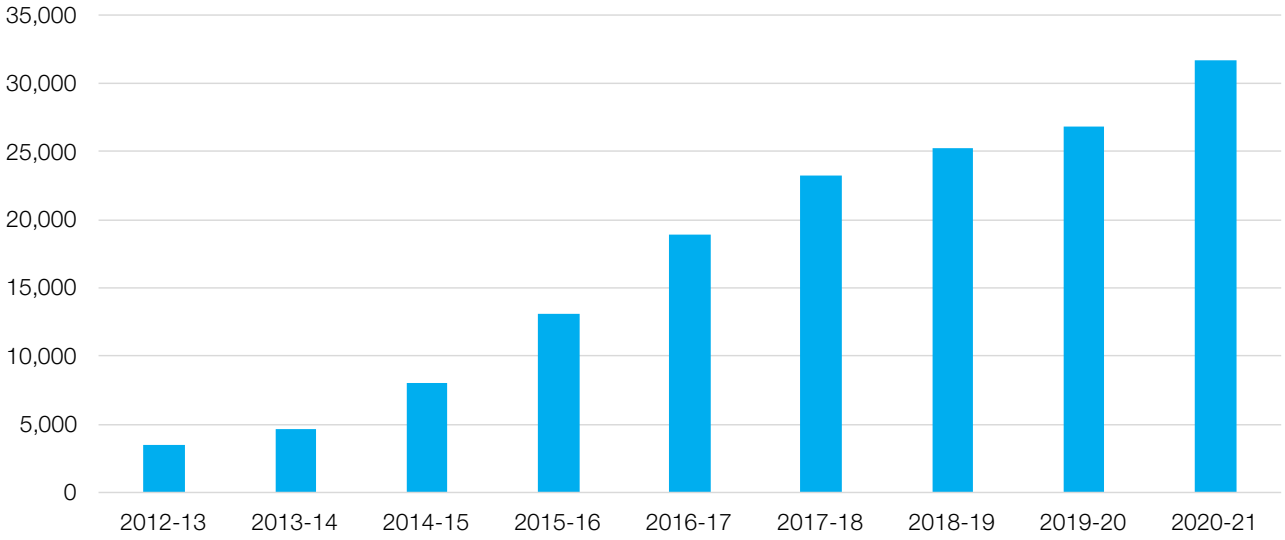
In 2020-21 police forces in England and Wales recorded 31,712 obscene publications offences. Figure 2.2 shows that from a low baseline in 2012-13, there has been a steep and continuous rise in this offending coming to the attention of local police forces (HM Government, 2022). By 2020-21 the volume of recorded offences constitutes over an 800 per cent increase on the number recorded in 2012-13. Obscene publications offences encompass a range of offending behaviours[20], but this rise in volume is primarily attributable to the surge in CSAM offences referred by the technology industry in recent years.

An extract taken from police data which captured *only* CSAM offences showed a total of 18,766 offences recorded by police in England and Wales in 2018. Most (15,171 or 81 per cent) were the offence of taking, making or distributing indecent images of children; police forces recorded an average of 1,264 each month, more than a six-fold increase on the monthly average in 2014 (187). There were 3,595 possession of an indecent image offences recorded in 2018. The volume of these offences remained relatively consistent, perhaps reflecting a crime recording decision to prioritise taking, making or distributing CSAM as the more serious offence (Ministry of Justice, 2012) and the rise in remote storage such as cloud computing and streaming services, obviating the need for offenders to store CSAM on local devices.

19. These figures reflect only offending that is clearly categorised as a CSA or grooming offence in recorded crime. Other categories including sexual assault on a male or female aged 13 and over or causing sexual activity without consent will include victims who are children and young people however this data is not available. It is likely that the offence category of sexual activity involving a child will incorporate online grooming and sexual communication however this data is not available.

20. For example, "possession of extreme pornographic images" or sending "a message or other matter that is grossly offensive or of an indecent, obscene or menancing character". See https://www.cps.gov.uk/legal-guidance/obscene-publications

Figure 2.2 Volume of obscene publication offences recorded by police forces in England and Wales, 2012 to 2021



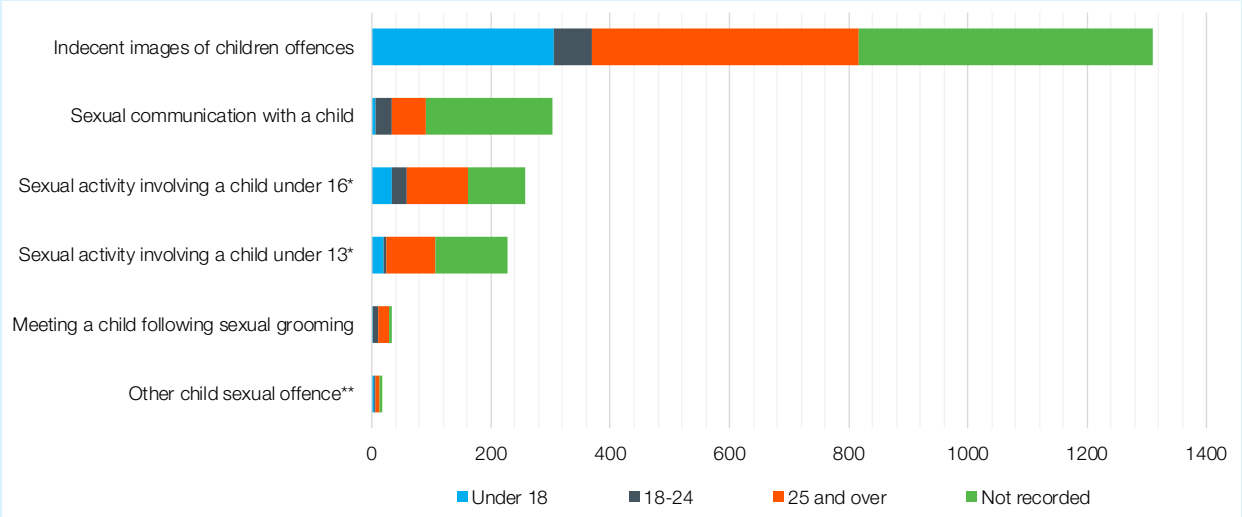
* A minority of the recorded obscene publications offences will not pertain to indecent images of children.

Box 2.1 Online child sexual abuse demand in a single police force

To get a more detailed breakdown of the kind of local police demand related to online CSA we looked at reported offences in a single police force between 2018 and 2019. There were a total of 2,151 offences recorded over an 18-month period, with an average of 120 crimes per month.[21] Figure 2.3 shows a large proportion of demand (61 per cent) is comprised of indecent images of children offences, though together, sexual communications and sexual activity involving a child made up 37 per cent of offences.

The chart also breaks each offence type down by the age of known suspects.[22] Offenders aged under 18 were linked to 37 per cent of indecent image offences, compared to 8 per cent of sexual communications offences. The age of the suspect was missing in 43 per cent of crimes, most likely reflecting the challenges in identifying suspects locally or in other jurisdictions.

Figure 2.3 The distribution of all online CSA crimes and suspect age recorded in a single police force, April 2018 to September 2019



* Incorporates offence categories: sexual activity involving a child, causing or inciting a child under 13/16 to engage in sexual activity and causing a child under 13/16 to watch a sexual act.

** Incorporates all other recorded child sexual offences for which there was a link to online offending, including sexual assault, rape, abuse of a position of trust or abuse through prostitution and pornography.

Box continued overleaf

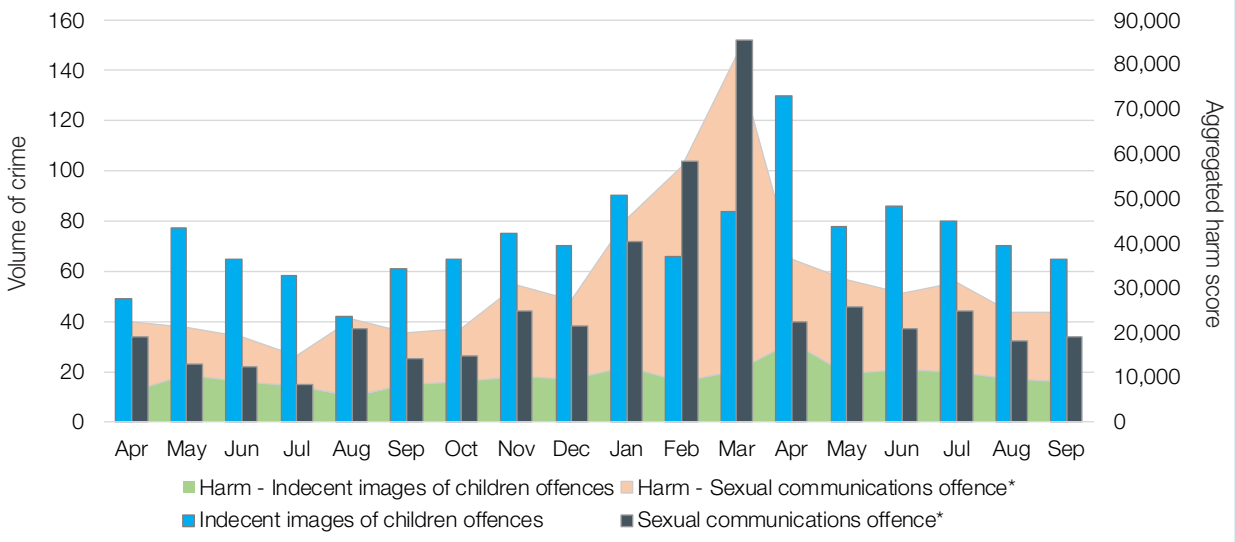
21. This represents crimes recorded but will likely represent fewer offenders, with the potential for a single offender to be linked to multiple crimes concurrently or during the 18-month period.

22. The age of the suspect was recorded for 817 indecent image offences and 91 sexual communications offences.

Box 2.1 continued from previous page

Figure 2.4 shows in the same police force that the recorded rate of both image-based and sexual communications offences was relatively consistent each month, though there were spikes between January and April 2018. Figure 2.4 also shows that although the volumes of sexual communication offences recorded are lower, they are estimated (applying the ONS Harm Index) to be more harmful.[23] However, as will be discussed in a later section, the police response is directed to addressing the risk of contact abuse over and above the reported offence.

Figure 2.4 Monthly patterns in the volume and harm from indecent images of children and sexual communications offences in a single police force, April 2018 to September 2019**



* Incorporates all online communications offences including sexual communications, sexual activity involving a child and causing or inciting sexual activity.

** This chart excludes other recorded child sexual offences for which there was a link to online offending, including sexual assault, rape, abuse of a position of trust or abuse through prostitution and pornography.

2.3 VICTIMS

What do we know about the victims of online CSA? Which children and young people are most at risk and what are the key factors that expose them to harm?

The profile of victims

In 2018-19 police in England and Wales identified and classified over two million unique sexual images of children; 19 per cent depicted penetrative or non-penetrative sexual activity involving a child and 76 per cent were non-penetrative sexual images such as children posing in a sexualised manner alone or with other children,[24] including images that had been self-generated by the child or young person.

In 2020 INHOPE reported that 76 per cent of identified CSAM depicted children ranging from the ages of three to 13 years of age (i.e. prepubescent or pubescent) (INHOPE, 2021). Similarly, the majority of CSAM detected by the Internet Watch Foundation (IWF) contained images of children aged 13 and under. Table 2.1 shows 98 per cent of children were assessed to be aged 13 or under, with 23 per cent aged seven to 10 and 68 per cent aged 11 to 13 (IWF, 2022). A high proportion of the most severe images (Category A) involved younger children;[25] in 45 per cent of CSAM that was classified a Category A image the child was aged 10 or under, compared to just 4 per cent depicting children aged over 13.

23. The harm index reflects the average sentence received by those convicted of the different offences. The scale ranged from 7,973 for homicide to 2 for possession of cannabis. Rape of a male or female child under 16 count among the highest harm crimes (3,895 and 3,883 respectively). Harm scores were applied as a multiplier to indecent image and sexual communications offences, coded in the index as 'Obscene publications, etc and protected sexual material' (score 137) and 'sexual grooming' (score 463). The index was developed using data from 2012-16, preceding the Sexual Communication Act (2017), therefore sexual grooming scores may not fully represent the current nature of these offences. See - https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeseverityscoreexperimentalstatistics

24. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/childsexualabuseappendixtables

25. Category A includes images showing sexual activity between adults and children, including rape, sexual torture or self-penetration; Category B are images involving non-penetrative sexual activity; Category C includes indecent images of children not included in Category A or B.

Table 2.1 The age of children and category of the indecent images detected by the Internet Watch Foundation in 2021

Age of child	Image Category		
	A	B	C
0 to 2	1,171 (78%)	294 (20%)	32 (2%)
3 to 6	7,238 (47%)	4,343 (28%)	3,841 (25%)
7 to 10	12,217 (22%)	10,869 (19%)	33,457 (59%)
11 to 13	23,129 (14%)	33,758 (20%)	113,095 (67%)
14 to 15	1,261 (26%)	1,078 (23%)	2,448 (51%)
16 to 17	432 (43%)	78 (8%)	502 (50%)
Total	45,448	50,420	153,375

Source: IWF Annual Report, 2022

This age distribution in CSAM will in part be a product of process, due to organisations most likely prioritising CSAM depicting younger children and the inherent challenge in determining the ages of post-pubescent children; they need to be confident the image is illegal before taking the action to issue a notice to web companies. Furthermore, the nature of abuse depicted in CSAM reflects a risk profile that can vary depending on the age of the child. Older children have greater freedom to access and spend more unsupervised time online, and so are susceptible to sharing sexual images and are more accessible to prospective online offenders (Ospina et al, 2010; Whittle et al, 2013). Prepubescent children have less of an independent online presence and a high proportion of CSAM involves some of the most severe abuse, commonly perpetrated by a family member (Seto et al, 2018).

Self-generated imagery

In 2021 almost three quarters (72 per cent) of images identified by the IWF were classified as self-generated by children (IWF, 2022). The statistics on self-generated CSAM often do not however provide an accurate picture of the underlying social and behavioural contexts in which the images were produced. These can range from sexual risk-taking, a consensual exchange between two children in an age-appropriate relationship, pressure or bullying from a peer, "revenge porn"[26] or victimisation by an adult perpetrator.

Sexual communications and the sharing of sexual images (i.e. sexting) is rising among young people. A survey of approximately 1,000 13 to 17 year olds in the UK revealed that 7 per cent had taken and shared a sexual image of themselves (Martellozzo, 2016).

Research (Martellozzo, 2016; Wager et al, 2018) has found that:

- These communications can entail the exchange of sexualised messages and/or images, but young people report more commonly receiving sexual images than sending them.
- Images are more likely to depict females.
- When images are shared, it is most commonly with someone known to the child offline such as a current or potential boyfriend or girlfriend. Of most concern was the subset of young people who reported they had either not wanted to send the image (20 per cent), or they had not known the person to whom they had sent the image (31 per cent).

The risk factors

Exposure to the online environment

The digital environment influences young people's exposure to risk and harm during the developmental stages of their sexuality. With access to the internet, more young people are being exposed to sexual material, and they display fewer inhibitions and more impulsive behaviour when online, often failing to recognise the long-term consequence of sharing a sexual image that might never be removed from the online space (Hamilton-Giachritsis et al, 2017; Martellozzo, 2016; Martin, 2014; Palmer, 2015). Many young people lack awareness of the illegality of this behaviour and where they have shared images with an adult, they very often do so in full knowledge of a perpetrator's age (NSPCC, 2016; Whittle et al, 2013).

26. Revenge Porn is defined by the government as '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' - https://www.gov.uk/government/publications/revenge-porn

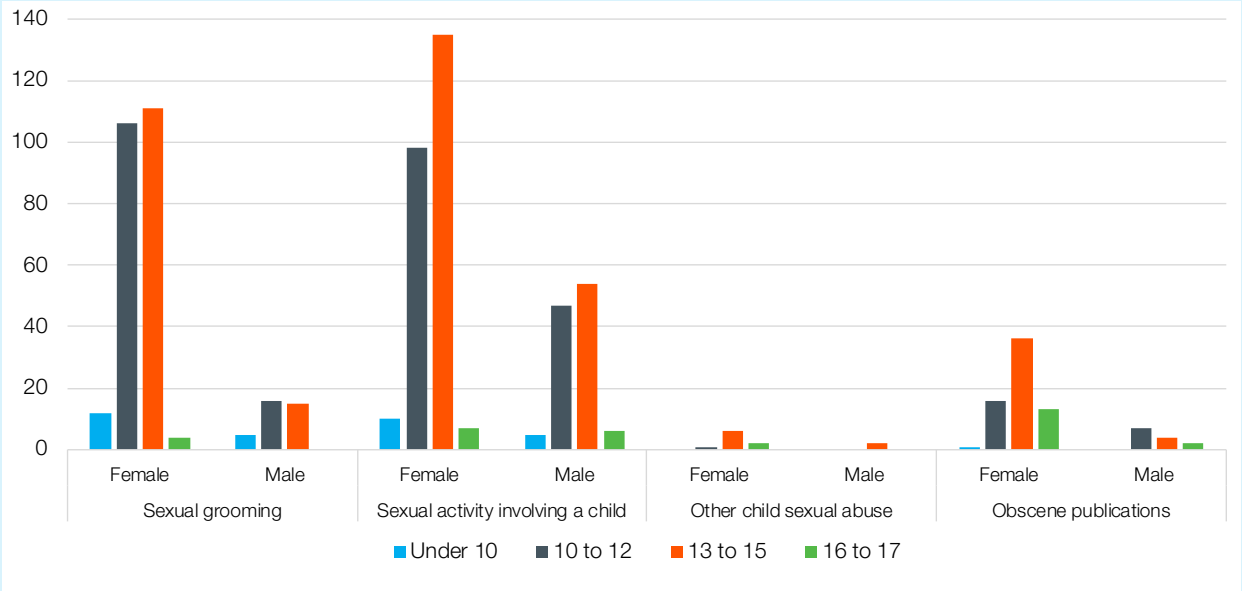
Box 2.2 A profile of victimisation from a single police force

Online CSA is represented by a number of separate offence categories that include indecent images of children offences (included in obscene publication laws), sexual activity involving a child, sexual grooming and other child sex offences recorded (or flagged) with a link to cybercrime. Over an 18-month period in one police force online sexual activity and grooming were the most frequently recorded offences. "Sexual activity involving a child" offences comprised half of all recorded offences (50 per cent), which includes offences of causing or inciting a child to watch or engage in a sexual act. These were especially prominent among offences targeted at male victims.

Sexual grooming offences comprised over a third of offences (37 per cent), nearly all of which were sexual communications offences; there were 13 reported incidences of a child meeting with a perpetrator after being groomed (linked to eight unique victims[27]). "Other child sexual abuse" represents some of the most serious sexual abuse – including rape or sexual assault – and represented a minority of the recorded offences (3 per cent).[28]

Over three quarters (77 per cent) of all online CSA offences involved a female victim. The most common age categories for both genders were 10 to 12 or 13 to 15[29]. Children under ten were linked to 5 per cent of offences recorded in this period.

Figure 2.5 The distribution of online CSA victimisation recorded by a single UK police force, by age and gender



* Age and/or gender were missing in 44 cases.

There were 571 unique victims recorded in this period. 31 per cent had been a victim of more than one offence; most often they were linked to two offences (in 163 cases) with a minority (12) who reported between three and five offences in this period.[30] In most cases of repeat victimisation (96 per cent) the offences were reported concurrently or within a couple of days of each other. Just over one in 10 victims (13 per cent) had been flagged with a vulnerability, most commonly for being on the child protection register and/or assessed to be a child at risk (5 per cent). A similar proportion (4 per cent) were recorded as having a physical or mental health issue. Other vulnerabilities included domestic violence, alcohol use or a child sexual exploitation risk.

In 226 cases the age of both the victim and suspect was recorded and in 32 per cent of those cases the age difference was under two years. In 44 per cent of cases the perpetrator was 10 or more years older than the victim.

27. This analysis looked at the distribution of online CSA offences, but some victims reported multiple offences in this period (175).
28. Links to online in these cases could only be discerned if recorded with a cyber flag or if the description made explicit mention of terms that indicated the role of online and so may underestimate the role of online and offline child sex offences.
29. In the case of young people aged 16-17 it is no longer illegal to engage in sexual communications online, though some may have reported the offence retrospectively
30. Victimisation that preceded this 18-month period was not include in the data.

Routine activity theory posits that much offending stems from opportunities that arise from the everyday routines of both offenders and victims (for example, see Leukfeldt and Yar, 2014) and with children and young people spending increasing amounts of time online it stands to reason the scale of the threat will grow.

Vulnerability

Most children and young people use the internet without experiencing harm and display a resilience to unwanted sexual contact (Livingstone, 2017; May-Chahal and Palmer, 2018). Research indicates that vulnerability to online CSA is not uniform or evenly distributed and there are certain characteristics that can make young people vulnerable to exploitation in different ways. One common characteristic is the desire to engage in interactions that were not possible offline; for example, young people who are lesbian, gay, bisexual or transgender may be drawn to online communities and contacts, and young people with mental health problems or learning difficulties were also more at risk (Palmer, 2015). Another study distinguished the vulnerability profiles of those looking for affection, attention or relationships online, in some cases due to loneliness or negative experiences offline, from others who take risks and lack inhibition when online, suggesting the risks to one may be dissimilar to the other (Webster et al, 2012). These various characteristics can manifest in online behaviour and signal vulnerability to prospective offenders (Webster et al, 2014).

Online and offline vulnerability

In some cases, on or offline abuse are inextricable from one another. It has been estimated that between a third and half of online abuse victims already know the perpetrator offline (May-Chahal and Palmer, 2018). A study which examined CSAM offenders who also perpetrated contact abuse found that it was commonly opportunities in the offline world in the form of established relationships in the family or community, which differentiated them from image-only offenders (Babchishin et al, 2014). The implication is that the underlying vulnerabilities that expose children to risk may not differ whether in an online or offline context.

Harm

The harms from online abuse can be acute, with the technological interface facilitating or extending control, blackmail and the ability to revictimise, with victims experiencing self-blame and emotional trauma that can be exacerbated by the knowledge that a permanent record of their abuse is continuously available for others to view (Hamilton-Giachritsis et al, 2017; Martin, 2015). The harm can also be more acute when the response from the victim's peers, family or practitioners is unsupportive. Clearly the harm from the contact abuse that creates first generation CSAM is extremely severe.

2.4 OFFENDERS

In this section we describe what is known about online CSA offenders. First, we point out that contrary to popular belief, online CSA offenders are a very diverse group, ranging from young people exchanging self-generated images between themselves, through to those who come across CSAM online but are unlikely to commit contact abuse, through to organised groups of paedophiles determined to cause serious harm to children. It is vital that law enforcement and partners understand these distinctions so that they can focus their limited resources on pursuing the most serious offenders.

Second, we describe the different pathways into online CSA offending for adult CSA offenders, including the psychological factors that typically draw people into these patterns of behaviour and the situational opportunities that exist online.

Finally, we describe the characteristics of the most serious online CSA offenders who pose the most risk to children and young people online.

Three facts about online child sex abuse offenders that go against conventional wisdom

Online CSA offenders are highly diverse in terms of their personal backgrounds, offending motivation and risk. In fact, the data belies a number of assumptions about online CSA offenders: that they are all adult males, that they are sophisticated and determined criminals and that online abusers are also offline abusers. Below we explore each of these assumptions in turn.

1. The vast majority of identified suspects are adult men

Table 2.1 shows a high volume of take, make, or share indecent images suspects known to police in the England and Wales are actually female, with the proportion rising from one in five in 2014 to 41 per cent in 2018. In our study of data from one local police force we found that 37 per cent of indecent image offences were recorded with a suspect who was aged under 18.[31] Of these 77 per cent were female. This indicates

31. See Figure 2.3 earlier in the section - data relates to crime recorded during an 18-month period, April 2018 to September 2019.

Table 2.2 The volume of CSAM suspects recorded nationally by police, by gender

Year	Take/make/distribute indecent photographs or pseuro-photographs of children			Possession of indecent photo of pseudo images of a child		
	Female	Male	Total	Female	Male	Total
2014	475 (19%)	1,998 (81%)	2,473	157 (9%)	1,632 (91%)	1,789
2015	1,576 (29%)	3,895 (71%)	5,471	336 (12%)	2,519 (88%)	2,855
2016	3,421 (35%)	6,265 (65%)	9,686	402 (12%)	3,063 (88%)	3,465
2017	5,234 (38%)	8,579 (62%)	13,813	486 (14%)	2,956 (86%)	3,442
2018	5,312 (41%)	7,710 (59%)	13,022	481 (16%)	2,519 (84%)	3,000

* Gender was not specified in 3,974 (6 per cent) of recorded offences

a rising volume of youth-produced sexual imagery. We ought to bear in mind the data reveals little of the context behind these offences, which can range from consensual sharing to exploitation or coercion (Arthur, 2018; Tener et al, 2015).

2. Online child sex abuse offenders are sophisticated online criminals

While there are very many sophisticated criminals operating in this space causing considerable harm to children, large numbers of those people viewing CSAM are not in any way sophisticated. The fact that most CSAM material reported to the authorities is from the open internet indicates that it is accessed with limited use of tactics or technology to evade detection. A misplaced faith in online anonymity is thought to underpin a high volume of offending (Smallbone and Wortley, 2017).

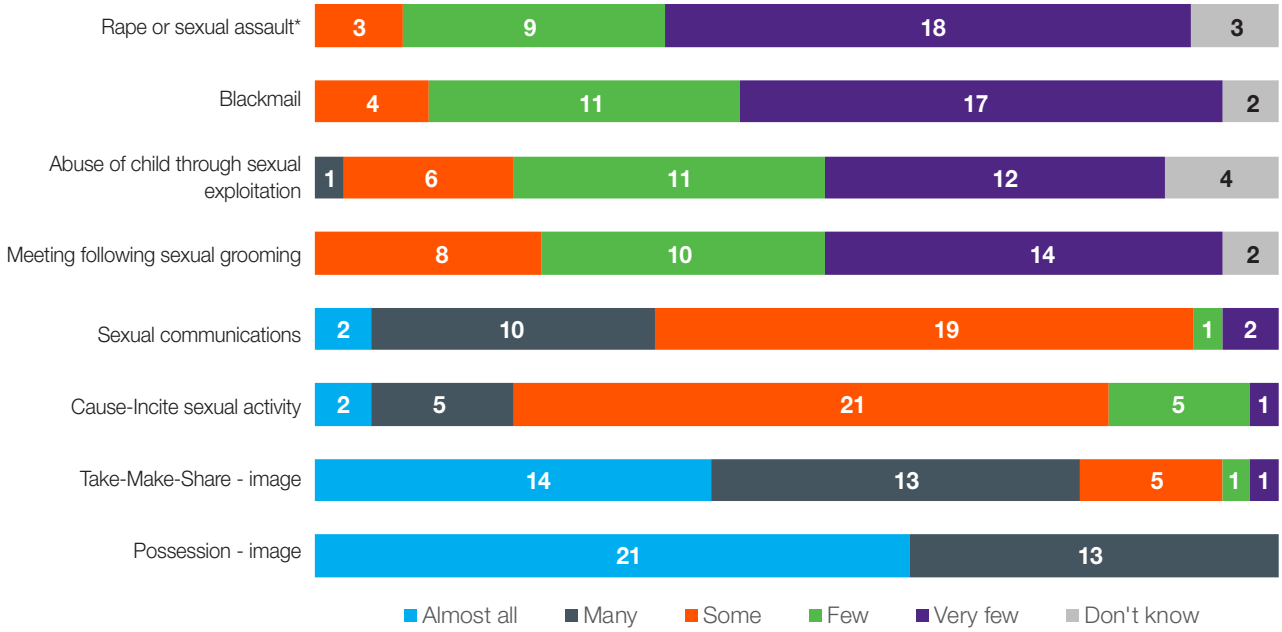
Online grooming offenders often do not fit the stereotype of the determined predator. Research has identified different offender types, that include some who seek intimacy and develop a misguided belief they are in a relationship; others who are "adaptable", displaying few signs of other CSA offending or motivation but adopting some sophistication in their approach to grooming a victim online; and 'hyper-sexualised' offenders who fit more closely to the stereotype of an online predator, adopting sophisticated methods to engage large numbers of children and young people, and engaging with CSAM and online communities of offenders (Webster et al, 2012).

This research is echoed in an in-depth analysis of 75 cases from the US. This research found that the strength of motivation to sexually abuse minors varied between groups, as did the degree of deception or reciprocity with the victim (Tener et al, 2015).

Table 2.3 The typology of online grooming offenders identified in US research (Tener et al, 2015)

"Cynical" offender – 35 per cent	The "experts" - 32 per cent	"Affection"-focused – 21 per cent	"'Sex-focused" – 12 per cent
Fully aware they were committing crimes. Some sophistication and deception but usually targeted at a small number of children, without getting emotionally attached. In addition to meeting victims online, many targeted children already known to them offline. Some engagement with CSAM was common.	Fully aware they were committing crimes, adopting sophisticated methods to target and deceive children and evade detection. Targeted high volumes of children online and did not get emotionally attached. Common to collaborate with other online offenders and possess large volumes of CSAM.	Experienced genuine feelings and engaged in a reciprocal exchange with the victim. In some cases, unaware they were communicating with a minor or of the illegality of their actions. Face-to-face meetings commonly occurred as a progression of the "relationship". Rarely found to otherwise engage with CSAM.	No specific sexual interest in children but were seeking to arrange a sexual encounter with another online. And if approached they engaged in reciprocal exchanges with someone underage. In some cases, the child misrepresented their age, though on discovering their real age some continued with the encounter.

Figure 2.6 The offending of online CSA offenders investigated by police and law enforcement agencies



3. Online abusers are also offline abusers

There is a commonly held belief that those viewing CSAM on the internet are also likely to go on to commit contact abuse against children. In fact, most of those who the police come across do not fit this stereotype. Our survey of strategic leads tackling online CSA across local police forces shows that the majority of online CSA offenders they investigate are linked to CSAM offences, but few are involved in direct forms of abuse such as rape, sexual assault or sexual communications (see Figure 2.6).

All practitioners in our survey reported that most offenders they investigated were found in possession of CSAM and 79 per cent of practitioners reported that offending linked to taking, making, or sharing CSAM was common.[32] Offenders linked to sexual communications, causing or inciting sexual activity from a child, or meeting following sexual grooming,[33] were less common in their investigations; for example, 71 per cent of practitioners reported that few or very few offenders they investigated had met a child following sexual grooming and 81 per cent said that few or very few had raped or sexually assaulted a child.

The survey responses will in part reflect the sheer numbers of CSAM offences being referred to the police by industry as well as the capacity of the police to uncover more serious offending when it has occurred. But it nevertheless strongly suggests that there is a pyramid-shaped distribution of offenders, with most online CSA offenders perpetrating the least serious CSAM offences, with a smaller number engaging in grooming and a minority at the top of the pyramid engaging in the most serious online and offline abuse.

Pathways into offending

What motivates and enables people to become online CSA offenders? Below we set out the different factors identified in research, which can be grouped under two headings: the psychological motivation to offend and the opportunity to do so made available in the online environment.

Psychological/motivational factors

i. Sexual interest

A sexual interest in pre-pubescent or pubescent children is clearly a major risk factor for perpetrating child sexual abuse offences (Beier et al, 2014). However, there is not a neat overlap between a clinical diagnosis of a "sexual preference disorder" and online CSA offending. This is of course in a large part because clinicians are concerned with maladaptive sexual interest in children who have not reached sexual maturity (principally pre-pubescent or pubescent children), whereas the criminal justice system is concerned with stipulations in law that regulate sexual behaviour involving children and young people up to the age of 18.

32. A number of survey respondents highlighted that of the many who 'take, make or share' images, most did not 'take' indecent photographs of children. The legal definition of 'making' an image refers to producing a digital copy of an image, for example this includes scenarios in which an image is downloaded onto a personal computer or sent in an email.

33. Causing or inciting sexual activity can involve either online or offline offending.

Furthermore, CSA offences are not necessarily rooted in an entrenched sexual interest in children and can derive from other situational or psychological conditions (Babchishin et al, 2014).

> *"There are different motivations for looking at these [CSAM] images, not only a sexual preference disorder … It is highly likely that someone with a sexual preference for children will view these images, though most [CSAM] offenders do not have a sexual preference disorder."*
>
> **(Support services – specialist practitioner)**

A large-scale survey in Germany led to estimates that 4.1 per cent of the adult male population experienced sexual fantasies that specifically involved pre-pubescent children (Dombert et al, 2016). 3.2 per cent reported having had a sexual experience involving pre-pubescent children; 1.7 per cent had used CSAM, 0.7 per cent had used CSAM *and* experienced sexual contact with a child and 0.8 per cent had experienced sexual contact but not engaged with CSAM.[34] In 2015 the NCA extrapolated from this that 3 per cent of adult males in the UK (approximately 772,000[35]) may have a sexual interest in young people, 250,000 of whom may have a sexual interest in pre-pubescent children.[36]

Most people when thinking about CSA offending will describe offenders as paedophiles, but many online CSA offenders do not meet the clinical definition of paedophilia. According to the American Psychiatric Association (APA) paedophilia constitutes an "atypical sexual interest" that is clinically diagnosable if certain definitional criteria are met; "*recurrent, intense sexually arousing fantasies, sexual urges, or behaviours"* involving children, experienced for a period of at least six months (APA, 2000). It is only classified as a clinical *disorder* if it is causing distress or impairment to either themselves or to others, including a child victim unwilling or unable to give legal consent (APA, 2013). A final determining factor is the age of the individual and the age-differential with the victim; paedophiles must be at least 16 years old and must be at least five years older than the victim (Thibaut et al, 2016). The definition does not include the viewing of CSAM, but it is considered a strong diagnostic indicator (Seto, 2010).

There are a number of facets of paedophilia relevant to risk management and the criminal justice response:

- Paedophilia does not represent all types of sexual interest in children but specifically interest in children who are pre-pubescent (generally younger than 11).[37]
- The experience, behaviour and risk presented by individuals with paedophilia are not homogeneous and for some their "paraphilic" fantasy is essential to sexual arousal whereas for others this preference is more episodic and can co-exist with other sexual interests (Thibaut et al, 2016).
- Not all who experience paedophilia act on their sexual interest.
- Many CSA offenders do not experience paedophilia. Among those who engage with CSAM or online grooming, many are unlikely to meet clinical definitions of paedophilia or a paedophilic disorder on the basis that the law works to a much broader focus of sexual offending involving children and young people up to the age of 18.[38]

CSAM-only offenders can score highly on assessments of sexual deviancy, and the absence of contact offending is theorised to reflect either the presence of protective factors or the absence of criminogenic factors. For example, greater self-control, victim empathy and self-management when coping with stressful or difficult situations reduces the attractiveness of these crimes (Babchishin et al, 2011; Elliott et al, 2012). Those who experience paedophilic desires in conjunction with antisocial personality traits, and attitudes such as a disregard for societal norms or the safety of others, or a lack of remorse, impulsivity and persistent rule-breaking are associated with the propensity to engage in contact abuse offences (American Psychiatric Association, 2013; Babchishin et al, 2014). One study concluded that offenders who only engage with CSAM may constitute a different type of offender, displaying less motivation to perpetrate other sex offences and thereby requiring different prevention, treatment and risk management approaches (Dombert et al, 2016).

34. Sexual contact encompassed a range of sex offences that included sexual assault (for example, sexual touching and kissing).
35. Extrapolated from UK census data which estimates that there are 25,735,739 males aged over 18 living in the UK in 2020: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland
36. https://www.dailymail.co.uk/news/article-3132884/750-000-British-men-want-sex-children-Shock-new-abuse-statistics.html
37. Hebephilia is a sexual interest in pubescent children (generally age 11 through to 14) but is not a diagnosable disorder (Zonana, 2011).
38. For example, an analysis of P2P CSAM found three quarters of searches were for CSAM of children between 11 and 16, with the predominant age being 14 years (Steel, 2009).

ii. The psychological impact of the online environment

Multiple psychological phenomena have been found to mediate an individual's propensity to offend online. The content of CSAM is far-removed from a person's offline reality and so internal barriers that would otherwise inhibit offending are lowered, with offenders able to cognitively distance themselves from the sexual abuse depicted in the images and absolve themselves of responsibility (Howitt and Sheldon, 2007).

The viewing of sexual images depicting young people can create a cognitive association between young people and sex, but it does not necessarily engender a belief that it is socially acceptable (Elliott et al, 2012). The ability to disassociate themselves from the harm to unknown others is one element of the online disinhibition effect which can influence online behaviours. Key factors are anonymity, which allows people to cognitively distance their partial online identity and accordant actions from their full (offline) selves, the opportunity to be invisible which amplifies disinhibition and the blurring of personal fantasy with social reality, with some not recognising the harm their online behaviour causes (Suler, 2004).

> *"Online offences are the easiest to commit, people can commit and [they] might have some sort of internal rationalisation where they don't see it as committing an offence because they have a distance between themselves and whatever they are looking at…and maybe they don't make the leap to it being real people suffering real things"*
>
> **(Local police force – specialist online CSA investigation)**

The situational opportunity to offend online

Criminologists have long theorised that a motivated offender is not in itself sufficient for a crime to occur, but rather there needs to be adequate opportunity to perpetrate the offence, commonly arising in the course of everyday life – this is called routine activity theory (Cohen and Felson, 1979). Prior to the internet there were very limited opportunities to view CSAM because of the low availability of hard copy CSAM. This was the product of a "cottage industry" supplying material to only the most determined of offenders (Carr, 2017). The scale of opportunity to access and share CSAM has seen overwhelming growth with the spread of the internet. Offending is to some extent the product of the online environment itself, not only in providing greater opportunities to those already motivated to offend, but also in drawing in those who would not otherwise have offended.

There is perhaps an uncomfortable truth that the sexual interests and behaviours of people online, and the digital spaces that accommodate these, are a little at odds with the laws in relation to CSAM, bringing many to the fringes of criminality. First, the adult pornography market openly capitalises on a demand for sexual images of youth. One example of this is so-called "jailbait" or "barely legal" pornography that includes actors who are close to legal thresholds or made to appear so (Bartlett, 2014). In 2019 there were 39 billion searches made on a mainstream pornography website and one of the most frequent search terms was "teen"[39]. Independent researchers found 'preteen' was the third most frequent search terms in age-related online sex searches (Ogas and Gaddam, 2012).

Second, children and young people are themselves engaging in sexualised behaviour online due to increasing access to technology, digital media and exposure to pornography at a younger age (Hamilton-Giachritsis, 2017; Flood, 2009). A significant number of young people produce and share sexual imagery of themselves; a quarter of 14–17-year-olds in the UK (25 per cent) self-reported they had sent a nude or sexual image to someone they were interested in and half (48 per cent) had received one from another young person (McGeeney and Hanson, 2017). These broad social trends suggest that both supply and demand for sexual imagery of young people is rife.

Engagement with CSAM can become compulsive and lead to "fantasy escalation" whereby an offender turns to increasingly explicit and extreme material (Whittleand Hamilton-Giachritsis, 2017). Interviews with CSAM offenders in the UK indicated that most had not intentionally sought out CSAM but rather it was the result of "entrenched pornography use" and spiralling online behaviour.[40] Their initial engagement with CSAM was described as "incidental" rather than "purposive", a step that was neither difficult nor complex to take and to some extent, encouraged by online "pop ups and progressive links" that directed their browsing.[41] Curiosity now provides sufficient impetus to perpetrate these crimes, particularly in an environment in which CSAM is widely available and thereby normalised and/or there is a low perceived risk of getting caught (Quayle and Taylor, 2002; Wolak et al, 2005).

39. https://www.pornhub.com/insights/2019-year-in-review#searches
40. https://www.iwf.org.uk/news/new-research-shows-action-needed-to-stop-people-seeing-indecent-images-of-children-for-first
41. The veracity of these claims depends on offenders providing an honest account, and it is possible that some use these external factors to rationalise or neutralise their own actions.

Many practitioners interviewed for this research considered that it was the ease with which CSAM can be accessed and shared that was fuelling the growing volumes of these crimes, and linked to this, the ease by which children and young people could themselves produce and share sexual imagery. Some highlighted the increased prevalence of children and young people on social networking sites and the low barriers in place for engaging with them. This has led to new methods of abuse. For example, the gradual progression through the different stages of abuse has for some been replaced with rapid engagements with large numbers of children that quickly become sexual and exploitative in nature (CEOP, 2013; Finkelhor, 1986).

> *"Kids will always find a way around these things but some of it is just too easy … let's not make it so easy to have access to these children."*
>
> **(NCA – specialist investigator)**

Such widespread criminal opportunity leads to higher volumes of offending by those motivated to seek or create opportunities to offend, but also draws in other less motivated perpetrators who react to opportunities when they are presented (Wortley and Smallbone, 2006). In providing an entry-point for more offenders, the online environment not only creates more crime, but also increases the risk that offenders will be drawn into a pattern of repeat offending and/or escalation to more serious online and offline sex crimes. However, the evidence of an upward trajectory in seriousness for CSAM offenders is unclear (see below).

Understanding serious online child sex abuse offenders

Having described some of the pathways into online CSA offending we now turn to the most serious and determined perpetrators of online CSA.

Escalation from CSAM offending to contact abuse

Psychologists have theorised that repeated exposure to CSAM has the potential to foster maladaptive thinking on the appropriateness of child sexual relations and thereby increase the risk of engaging in a contact offence (Taylor and Quayle, 2003). The challenge is that much of the empirical evidence derives from studies that use relatively small samples of offenders, is skewed to represent the more serious offenders entering custodial or clinical settings within the criminal justice system, or else drawn from data in which salient factors are absent (for example, characteristics such as paedophilia or antisocial personality traits). This means they struggle to explain the differences in risk or behaviour between offenders (Seto et al, 2011). The equivocal nature of the evidence base is a major challenge for practitioners who need to be able to conduct robust risk assessments to ensure resources are quickly directed towards the most serious offenders and abuse.

Most studies have sought to measure the association between engaging with CSAM and concurrent or subsequent involvement in more direct forms of abuse. They have adopted a variety of approaches that include examining either the offence history or recidivism of known CSA offenders, or collecting self-reported data from known offenders or the general public. Few studies have been able to unravel the causal direction between engaging in CSAM and committing other abuse.

While the barriers to engaging in CSAM are much lower and seem to present an entry-point to offending, many who perpetrate other forms of CSA concurrently engage with CSAM. To illustrate, a study of offenders arrested by US law enforcement for any CSA offence, found 55 per cent were "dual offenders", engaged in both CSAM and other forms of abuse, but this association was much weaker (14 per cent) among those arrested for a CSAM offence (Wolak et al, 2005). A more recent review of multiple studies into CSAM offenders found that 12 per cent had a contact abuse offence recorded prior to their online offence (Seto et al, 2011).

The view of practitioners in our study was however near unanimous that investigations seldom revealed CSAM offenders to have engaged in contact abuse. In cases where the police did uncover contact abuse offending, it was commonly in the context of intra-familial abuse.

> *"There's a huge amount of people who will restrict their behaviour to image offending … There's an underlying [reasoning] that if you look at these images you will commit contact abuse against children, this is not true."*
>
> **(Support services – specialist practitioner)**

> *"We have identified a small number of cases where [rape or sexual assault] has taken place. Most cases have been within familial settings."*
>
> **(Local police force - online CSA strategic lead)**

However, studies which only capture cases that are detected and convicted miss the majority of offenders who are not caught. Self-reported offending in surveys can develop a clearer picture of prevalence,

depending on the representativeness of the sample and the truthfulness of the responses.[42] Studies that have focused on offender populations have generated divergent findings. Taken overall, the research indicates that 55 per cent of CSAM offenders disclosed a prior contact sexual offence (Seto et al, 2011), though this ranged from 84.5 per cent of respondents in a US offender treatment programme to 32.8 percent in another study (Bourke and Hernandez, 2008; Coward et al, 2009).

Multiple studies indicate that much of the contact abuse depicted in CSAM, particularly that involving pre-pubescent children, includes older males who are known offline to the victim, (commonly family members) and already engaged in the abuse (Seto et al, 2018; Smallbone and Wortley, 2017). The causal direction between CSAM and offline abuse is difficult to ascertain but some suggest there is a sizeable gap between thought and action. Multiple studies have identified key distinctions between contact, internet and "mixed" offenders, for example on measures such as the perceived social acceptability of child sexual offences, self-control, victim empathy and antisocial disorders (Babchishin et al, 2014; Elliott et al, 2012). Studies suggest that rather than the online offence itself, it is extraneous risk factors relevant to conventional offline sex crime that continue to determine the risk of contact offending, including situational factors such as having access to children in their everyday environment (Babchishin et al, 2014; Seto et al, 2011).

Practitioners perceived a large contingent of CSAM offenders to be "fantasists" and unlikely to engage in contact abuse. On arrest many expressed feelings of remorse, a desire to desist or in some cases, had failed to recognise the illegality of their actions. Many offenders exhibited few technological precautions for covering their tracks and were fully compliant with the police investigation. Moreover, some reported it was rare to find CSAM suspects in possession of "first generation" images which can indicate a link to more serious online or offline abuse.

> *"It surprised me how easy a lot of these [offenders] are …they roll over, especially when we roll up with the equipment, a lot of the time they will assist."*
>
> **(Local police force – specialist online CSA investigation)**

> *"… people don't seem to realise that fantasising and acting on it by viewing images is an offence. Often when they go out on a warrant, people will say 'oh but it was just a fantasy, I wasn't doing anything'".*
>
> **(Local police force – specialist online CSA investigation)**

Recidivism studies indicate that few CSAM offenders go on to perpetrate the same or more serious sex offences; this may reflect limits on their motivation to offend or may indicate that this is a group that is highly responsive to the deterrent effect of law enforcement. One study found that fewer than 5 per cent went on to be caught for a new sexual or violent offence,[43] and recidivism was even lower for those with no prior contact offence (Babchishin et al, 2011; Seto et al, 2011). A more recent study in the UK examined the rate of reconviction over five years for CSAM offenders who had no prior convictions for a sexual offence and only 2.7 per cent went on to be convicted of a more serious sexual offence. (Elliott et al, 2019).

There is some divergence between the reported experience of police on the ground and academic (particularly self-report) studies on the scale of association between CSAM offending and more serious sex crimes. This may reflect the challenges for police in detecting further offending or that the existing research evidence does not adequately capture the full diversity of CSAM offenders. In recent years, the availability of CSAM has risen dramatically in parallel with the considerable growth and advances in online communications and media (Zonana, 2011), and furthermore, in the last five years the net of offenders is likely to have been substantively widened by the surge in offence referrals from mainstream US technology companies. The research is potentially lagging behind the changed composition of offenders coming to the attention of law enforcement.

Recommendation 1

The National Police Chiefs' Council and the National Crime Agency should commission research to improve its empirical understanding of online CSA offences, the offenders who commit them and their risk profile. This would support more informed and targeted resource allocation and strategic decision-making and would enable practitioners to make more accurate assessments of risk.

42. The challenges in interpreting self-reported data from offenders in criminal justice or treatment settings include offenders unwilling to divulge the truth, or else feel pressured to answer in a way that shows their engagement with treatment and some have used polygraphs which are deemed unreliable. For example, see - http://medcraveonline.com/FRCIJ/FRCIJ-06-00213.pdf

43. In most studies the follow-up time period was four years or less.

Online grooming

The online environment can facilitate a meeting point between an offender and a victim, but the context of the encounter varies. Types of grooming scenarios include:

- The offender met the victim online and had an online sexual interaction.
- The offender met the victim online and had an online sexual interaction which moves to an offline sexual interaction.
- The victim was known to the offender offline, and online communication was used to establish or maintain sexual interaction.
- There was a sexual interaction with a victim known to them offline, and online exploitation through producing and sharing CSAM

(Seto et al, 2018; Tener et al, 2015)

There is little research that has explored the relationship between different online grooming behaviours and the risk to children, though persistent offending that targets personal vulnerability and incorporates more serious criminality such as blackmail and threats is indicative of high risk. Furthermore, the more motivated an offender, the more children they will victimise.

Some of our police interviewees held the view that those who engage in grooming behaviour on the open web were among the riskiest online offenders, because of the direct contact with children which introduced the potential to escalate into a contact offence.

> *"I think groomers are more dangerous [than CSAM offenders] … grooming is that one step further, actively making contact to get access to a child … you don't know that person's motivation, for some it's just fantasy."*
>
> **(Local police force – specialist online CSA investigation)**

However, the large numbers of offenders willing to engage in an online sexual encounter with children and young people poses a challenge for investigators in determining who to focus on:

> *"It's like shooting fish in a barrel, there's so many of them … you wouldn't have to be on a platform very long before you see some of this taking place."*
>
> **(NCA - Specialist investigator)**

The link to serious and organised crime

This section will examine the nature of serious and organised crime in the context of online CSA, with a specific focus on the characteristics of "organisation" and complexity and the relationship they have to the seriousness of offending.[44]

The formation and growth of criminal networks in general has been a core component of research into organised crime to help understand where criminal associations form, who is most likely to be drawn into offending and how crime groups organise themselves and their activities. Co-offenders are essential to a range of organised crime offences that require access to resources, knowledge or capabilities that might otherwise be unavailable. The more capacity they possess to forge links to others the greater their capacity to offend. Trust between offenders is of central importance and some criminal networks are for this reason constrained to immediate social ties such as in the family or workplace (Kleemans and van de Bunt, 1999; Kleemans and de Poot, 2008), although community hubs can provide a space in which criminals and like-minded individuals converge and socialise (traditionally social clubs and pubs), and thereby form new collaborations and draw newcomers into offending (Felson, 2003).

Many of the requirements for criminal cooperation such as trust and convergence settings are the same for online offenders, but the scope and nature of collaboration has been radically changed. In seamlessly enabling anonymous communication on a global scale and in highly adaptable digital spaces, many of the limits to fostering collaboration have eroded. The importance of offline social bonds has been reduced, permitting more flexible and loosely organised online networks that can quickly coalesce and dissipate. Offenders can more quickly build social and criminal capital in online spaces and therefore links are more quickly forged and newcomers can more quickly enter into criminal networks. There is greater access to new capabilities or resources to commit crime by drawing on a global pool of contacts. Finally, the traditional role of physical threats or violence as a means to maintain control are replaced by formal rules of conduct for members of online communities, often controlled by those in possession of the technical or criminal resources most valued by the community (Leukfeldt et al, 2017; Nurse and Bada, 2019; Odinot et al, 2017; Soudjin and Zegers, 2012; Wall, 2015; Yip et al, 2012).

44. It is worth noting that serious and organised criminals are underrepresented in official statistics on online CSA offending due to limits in contextual detail required to differentiate these offenders from the rest and the fact that these offenders are simply harder to detect.

Historically, individuals with a sexual interest in children were isolated in the absence of any obvious convergence settings to meet like-minded others. However, online networking opportunities have been harnessed by otherwise disconnected individuals with a sexual interest in children and young people. Spaces for these offenders to come together virtually include internet chat relays, communications applications, the dark web, or other private networks and also on the open web, in discussion forums and chat rooms, live streamed video sites, photo galleries and peer-to-peer networks (Westlake and Bouchard, 2016). The motivations to meet with like-minded others include the practical search for co-offenders who can facilitate offending (such as to gain access to CSAM) and also a desire for "human companionship", reinforcement and support from like-minded others (Tremblay, 2006; Davidson and Gottschalk, 2011).

Stakeholders described the motivation to become involved in such groups:

> *"'The facilitation of communities where people can be themselves and it's a lot about contributing to those communities."*
>
> **NCA - Specialist investigator)**

> *"…you have people who are potential offenders, who are onset offenders, who are actually looking at their sexual ideation, or minor attracted ideation towards children, and they're trying to understand what is this that I'm feeling, why am I looking at kids in a sexual way? And they start looking on Google or going into search groups or going on to websites, and what happens then is they start to interact with a community."*
>
> **(Private sector representative)**

Different spaces provide different functions, with more visible convergence settings on the open web providing a space to meet, and more closed and private network spaces providing places to plan or perpetrate offences (Nurse and Bada, 2019). In our interviews practitioners described covert means of reaching out to prospective co-offenders on the open web, such as posting a sexually suggestive image of a child or embedding files in file-sharing networks with inconspicuous names, to signal their presence to other like-minded individuals.[45] Online hubs can provide a focal point around which others can coalesce; they can involve a hierarchical structure and serve to develop stable ties between co-offenders and in the most serious cases, migrate to offline offending (Broadhurst et al, 2014; McGuire, 2012).

Interviewees in law enforcement described variation in structure across different forums. Some were very organised with clear hierarchical roles such as site hosts, administrators, moderators, super moderators, and evidence of systematic sharing of knowledge and resource. Examples include the provision of a directory of sites containing CSAM or a "paedophile handbook" to guide offending. Other online communities represent loose collectives that are less stable.

Different individuals linked to a network vary in the extent of their involvement and engagement. On dark web forums law enforcement interviewees described a differential status across different members, which can depend on their assigned role in the forum or on their contribution. Some were described as "consumers" and others "sharers" and members active in on or offline abuse to produce new CSAM were especially valued in some communities. Furthermore, those deemed as potential security risks for the group could be targeted and forced out.

> *"Anyone with access to kids and who provides images of these kids, they will be top dog [in the online communities], and others will try to protect them to make sure they don't get caught … there's a definite social hierarchy in these online environments."*
>
> **(NCA - Specialist investigator)**

There are various characteristics of online communities that can escalate the risk of harm posed by those involved:

- Communication with like-minded others creates an environment that provides support for deviant sexual interest, which can reinforce and validate the individual's motivations and potentially lead to entrenchment or escalation in offending.
- There are platforms which actively encourage members to engage in more serious on or offline abuse of children in order to produce new CSAM.
- The indication is that some of the most severe abuse, especially of pre-pubescent children or more violent abuse, is contained in CSAM shared by online communities.
- Online communities provide a stable element which allows for the continuous regeneration of members, which perpetuates CSA offending regardless of the continued involvement of specific core actors in the group.

45. For example, 'pre-teen hard-core' is communicated as PTHC.

- Online communities facilitate the formation of markets for the commercial exchange of CSAM or as one practitioner described, a "cottage industry" in live streamed sexual abuse in overseas countries such as the Philippines.
- Those in closed online communities are among the most technically capable offenders, rendering them more able to evade detection and requiring more proactive law enforcement intervention to uncover the offending.

The use of technology to evade detection

The levels of capability demonstrated by offenders varies considerably. The most sophisticated offenders (in some cases as part of a network) employ multiple strategies that restrict opportunities for law enforcement to attribute their online accounts or activity to their identity or location offline. Offenders who operate on the dark web are perceived by some in law enforcement to be the "more technically-minded individuals". Access requires specialist software and the enhanced anonymity creates significant barriers to detection for law enforcement (IICSA, 2020). The capacity for co-offenders to share knowledge and resources, including providing access to software packages, lowers the technical barriers for others to remain concealed. However, many of the online tools to conceal their activities or identities are embedded in mainstream technology such as VPNs (Virtual Private Networks), device encryption, end-to-end encrypted messenger and chat room services, cryptocurrencies and advances in media streaming which permit access to CSAM or a child without any need to download a file. The rise of cloud computing adds further challenges for investigators to trace the evidence.

> *"'… with live streaming there are people out there evading any detection because of the programs they use … live streaming isn't included in [industry] referrals, there is no trace on a live stream."*
>
> **(Local police force – specialist online CSA investigation)**

The extent to which offenders take pains to cover their tracks, may signal the strength of the motivation to offend and persist. However, the advances in secure storage and transfer of data using mainstream technology appears to have narrowed the gap between what might conventionally be considered "serious" or "organised" and everyday online security. The concern of some in law enforcement is that despite the increasing volumes being detected by industry, there remain substantial numbers of more committed and "savvy" offenders who remain undetected and untraceable. In such cases detection relies on an offender either making a mistake or on a covert or other in-depth online police investigation.

2.5 SUMMARY

This chapter has brought together evidence collected from police forces in England and Wales, and from the published research, to develop an empirical perspective on the scale and nature of online CSA. The volume of offences recorded by the police has surged in recent years, reflecting not only patterns in offending behaviour but also greatly improved systems and processes for detecting these online crimes, particularly in the technology sector. Online CSA offending is now a high-volume crime with well over 18,000 CSAM offences reported to the police in 2018 and more recently, over 6,000 sexual grooming offences reported in 2020-21. This creates a high volume of high risk offending and an unprecedented scale of demand for police intervention. Moreover, this constitutes only crimes that have been reported, with many serious crimes remaining hidden in plain sight on mainstream platforms, or in harder to reach spaces such as the dark web.

The problem of online CSA encompasses a wide spectrum of offending behaviour and risk. While most children do not experience these kinds of harms on the internet some are particularly vulnerable. CSAM includes depictions of extreme forms of contact sexual abuse but also includes a growing volume of images that are generated by children themselves. The latter is reflective not only of patterns in exploitation but also a wider trend among young people for sharing sexual images through digital technology. Identifying the most serious and high-risk cases is challenging without an understanding of the social and behavioural contexts behind the image or communication.

Adult online CSA offenders are a highly diverse group, who can be broadly understood to form a pyramid structure, with most at the bottom of the pyramid limited to less serious CSAM offences, followed by those who engage in grooming children online, through to a smaller number who commit serious contact offences or are engaged in organised and complex criminality to produce or proliferate CSAM. The evidence on the pathways taken by offenders is equivocal, notably the patterns in escalation to the most serious forms of abuse, which presents a major obstacle to risk assessment which is crucial for targeting resources and intervention.

Box 2.3 The impact of the Covid-19 pandemic on child sexual abuse

The restrictions imposed on the public during the coronavirus crisis displaced much of everyday life into online spaces, creating the conditions for more cybercrime victimisation (Halford et al, 2020). The same was likely for online CSA, with increases in the amount of unsupervised access to the internet leading to increased opportunities for offenders to contact children on gaming, chat groups, via email or through social media (Europol, 2020). However, barriers to reporting online abuse or exploitation will have been exacerbated under the lockdown conditions of the pandemic, in which frontline practitioners (such as in schools) had less contact and so were less able to identify potential risk. It is expected that the true impact of the pandemic will take time to surface. Support lines reported an increase in callers with online CSA concerns during this period; the NSPCC reported a 60 per cent increase in the period from April to August 2020 (NSPCC, 2020) (this could reflect increased victimisation but also an increase in public concern through this period). The IWF reported that in 2020 they processed 153,350 confirmed CSAM reports which was an increase of 16 per cent from 2019.[46] There was a 77 per cent increase from 2019 of images that were "self-generated", though it is not known the extent to which this reflects exploitation or consensual image-sharing between children and young people.

Overall increases in online activity lends itself to more opportunities to perpetrate CSAM offending. There was a concern that the restrictions on movement would displace the most serious offline abusers into engaging with CSAM and related online communities and that it could lead to a rise in the most harmful online offending such as demand for live-streamed abuse. Moreover, there were concerns that increased availability of CSAM may "stimulate demand" from individuals who would otherwise not have perpetrated these crimes (Europol, 2020). Europol reported a "surge" in referrals of CSAM from the technology industry during the initial lockdown period, rising sharply from under 200,000 in January, to over one million in March (Europol, 2020). The volumes quickly reduced to normal levels in May, but it is difficult to disentangle genuine trends in offending from uneven levels of proactivity by companies in detecting CSAM on their platforms. Their capability to detect, moderate and refer CSAM was considerably impaired by a reduction in personnel, mandatory home-working and technical challenges during the pandemic. Consequently, any reduction may simply represent a lag in referrals and will potentially surge once normal functions resume. Facebook reported increases in content related to child nudity or CSA in 2020.[47]

46. https://www.iwf.org.uk/news/%E2%80%98grave-threat%E2%80%99-children-predatory-internet-groomers-online-child-sexual-abuse-material-soars

47. https://transparency.facebook.com/community-standards-enforcement#child-nudity-and-sexual-exploitation

3. INVESTIGATING ONLINE CHILD SEXUAL ABUSE

In this chapter we ask how good the police and law enforcement agencies are at detecting online CSA offenders and explore the challenges faced by investigators. Before looking at the question of effectiveness we briefly describe how the law enforcement response is configured in England and Wales.

3.1 AN OVERVIEW OF THE LAW ENFORCEMENT RESPONSE

Online CSA is a crime that is cyber-enabled and crosses borders. There is therefore a need for extensive international law enforcement collaboration, alongside strong partnership working between national and local investigators. It requires a truly local to global effort.

In recognition of the growing and borderless nature of online CSA, the UK government introduced CEOP (Child Exploitation and Online Protection Command) in 2006, drawing together policing, child protection and industry experts into a single national hub (Home Office, 2010). CEOP was subsumed within the National Crime Agency (NCA) which now leads investigations into the most serious and complex crimes that require a national or international response, or those that require specialist capabilities unavailable in other agencies.

Different investigative capabilities are available at each level of the response, influencing how resources are allocated to different crimes. The most serious and complex offenders are within the remit of the NCA, GCHQ, ROCUs and a select few of the larger police forces with specialist proactive capabilities to detect and investigate. Local police forces will generally deal with the reactive demand reported to them, much of which will be at the less complex end. Figure 3.1 below outlines the range of channels through which reports of and intelligence about online CSA can reach a local police force.

Across law enforcement in England and Wales the resources for tackling online CSA have been consolidated into specialist investigation teams. In our law enforcement practitioner survey 73 per cent of respondents stated specialist CSA teams were involved in almost all or many of their investigations and over a third stated the same for specialist victim identification practitioners (39 per cent) (see Figure 3.2 below). This largely reflects police structures specifically for managing CSAM offenders referred by industry. In managing the referrals these teams employ consistent systems and protocols to assess, prioritise and develop the intelligence for each suspect using desk-based online investigation techniques. This requires specialist capabilities that are not readily available in the general workforce and moreover, in containing this workstream they protect officers and staff in the wider workforce from continuous exposure to harmful CSAM.

Figure 3.1 The reporting and intelligence channels into local police forces

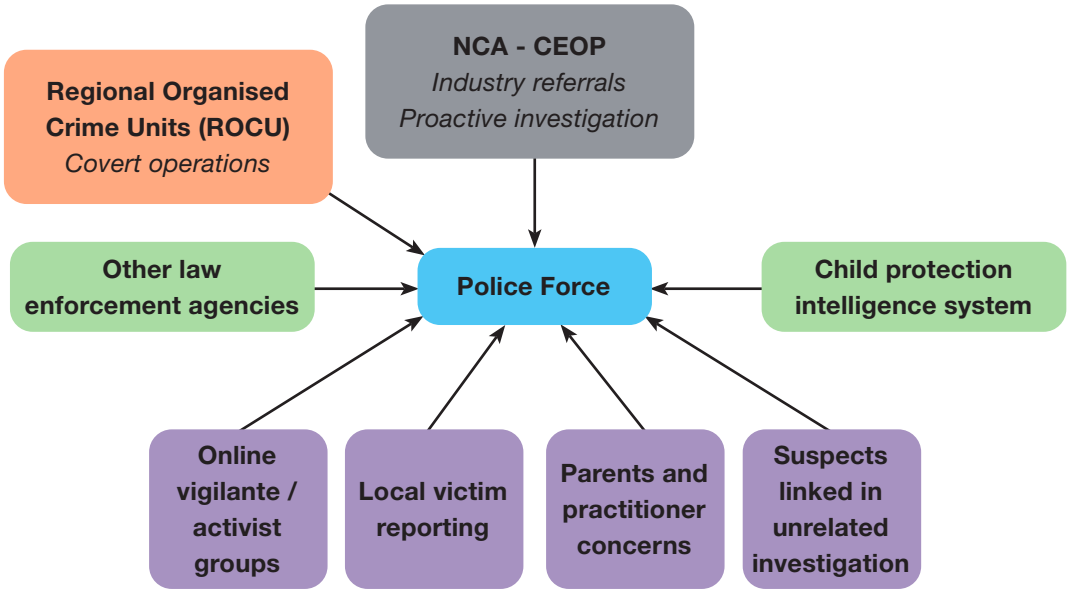
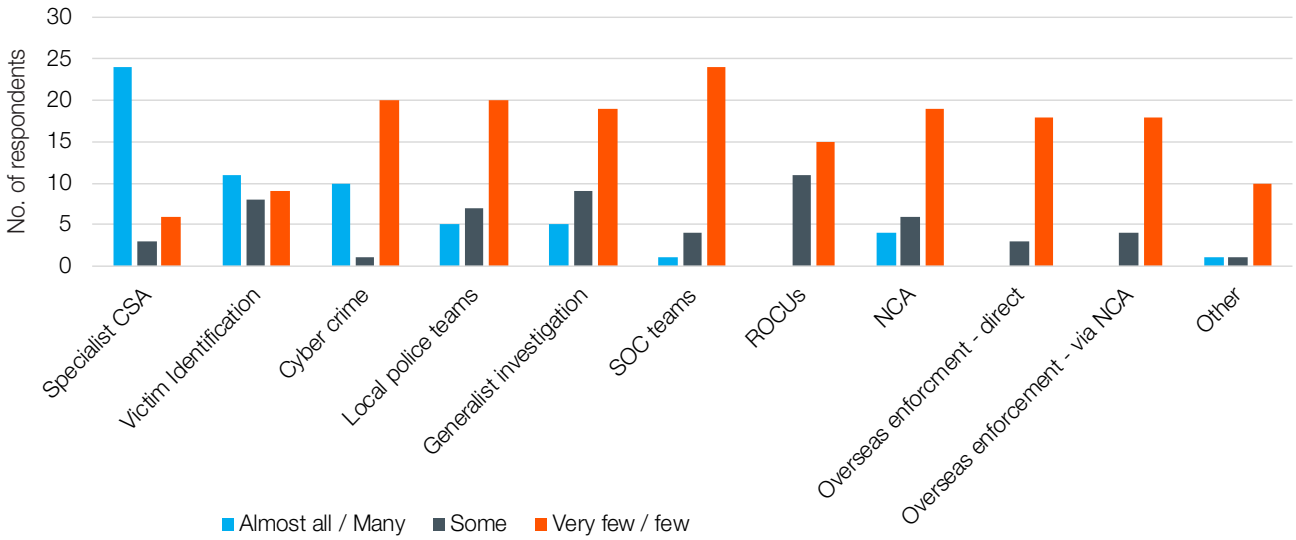


Figure 3.2 The proportion of online CSA investigations involving each law enforcement department or agency



Some respondents reported that their generalist investigation (42 per cent) or local policing teams (38 per cent) were involved in at least some of their investigations. This likely reflects the various other channels through which online CSA crimes are reported, including reports from local victims of online grooming and information on offending that can arise during unrelated local investigations.

The specialist resources available in regional, national or international law enforcement agencies are principally oriented to proactive investigation to identify serious offenders and protect children from abuse, which may then be referred to local investigation teams. Consequently, they contribute less to the reactive investigations carried out by local practitioners; the few examples pertained to the identification of a non-local child in need of safeguarding.

> *"On a few occasions we have gone directly to overseas law enforcement, this is only because a child has been at immediate risk of harm."*
>
> **(Local police force – online CSA strategic lead)**

Online CSA is accorded high strategic priority and thereby stands apart from other cybercrimes. With a workforce that has not kept pace with online crime, the preferred option has been to pool investment and expertise into specialist investigation teams in each police force; variously called Paedophile Online Investigation Team (POLIT), Online Child Abuse Investigation Team or Abusive Image Units, but sharing the same core function to manage the CSAM investigations disseminated by the NCA. Table 3.1 shows the number of investigators and other staff in these specialist teams in 29 police forces. To place the figures into context, figures for the number of investigatory and public protection resources for each force were collected and analysed alongside the survey data.[48]

In the 29 police forces respondents reported a total of 494 full-time equivalent staff responding to online CSA, comprising 1.8 per cent of the total investigative workforce (26,770). There was a reasonably consistent allocation of resource in the different areas, ranging from 4.8 per cent in one police force to 0.7 per cent in another; the proportion tended to be lower in larger police forces. A number of factors can explain the variation, including the wider range of national or regional investigative functions performed in larger forces but also variation in whether online CSA investigations are assigned to non-specialist teams. For example, one respondent stated "[local] detectives investigate medium and low risk CEOP referrals".

The structures for tackling CSAM were relatively standardised across police forces, though with variance at the fringes. Criminal investigators comprised 88 per cent of the online CSA resource and the number of dedicated investigators rose relative to the size of the workforce. However, this was not the case for victim identification officers,[49] with a consistent average of 1.6 officers reported in each police force irrespective of its size, indicating that capacity is particularly low in larger police forces. Six police forces had no victim identification

48. These were collected from https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2019 - workforce statistics are compiled by function and those included were staff working in intelligence, investigations, public protection and investigative support. All other staff functions were excluded. In addition to providing a reference point for online CSAE investigative resource, these figures give an indicative measure for the relative size of each police force.

49. The role of victim identification officers is to proactively analyse the data retrieved in the course of an investigation to identify any immediate risk of sexual abuse to a child.

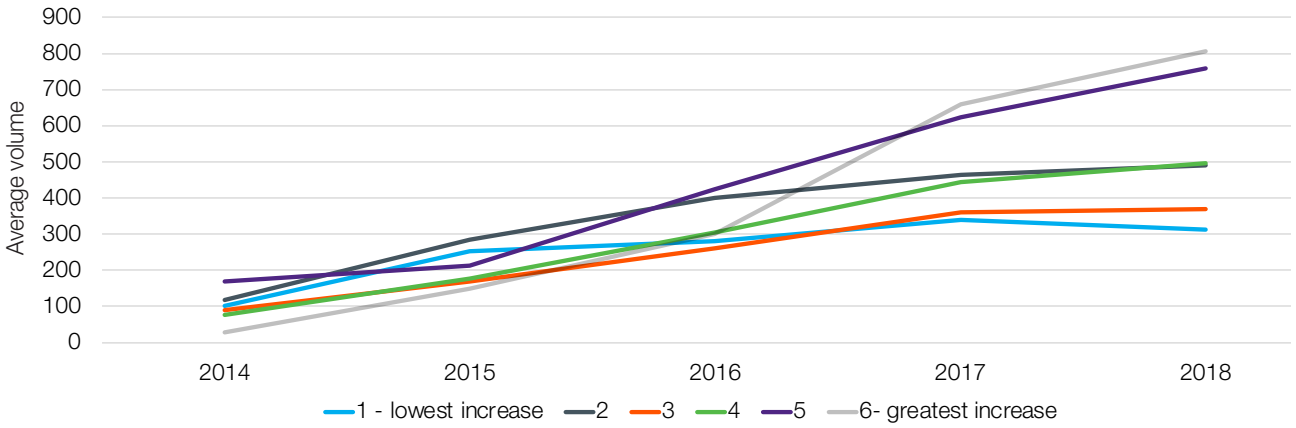
Table 3.1 The police workforce for tackling online child sexual abuse and exploitation

Size of the investigation / public protection workforce*	Average No. FTE staff	% total investigation public protection resource	Average No. dedicated investigators	% FTE staff	Average No. Victim identification officers	% FTE staff
Over 800	26.9	1.30%	24.3	90.20%	1.6	5.10%
600 to 800	16.2	2.50%	14.5	89.30%	1.5	8.40%
Under 600	10.1	3.00%	8.2	80.7%	1.6	14.40%
Total	17.0	1.80%	15.0	88.00%	1.6	8.20%

* There were 8 police forces with an investigatory or public protection workforce of 800 or more, 11 had between 500 and 800 and 10 had under 500.

** The percentages of FTE staff do not make up 100 as some respondents described a small number of staff with other functions.

Figure 3.3 The average volume of recorded CSAM offences in 2014-18, by police forces that experienced different rates of change in demand[50]



* The groups were stratified into six groups based on the percentage point change in demand between 2015-18, ranging from the lowest (Group 1), a 0-49 percentage point change, to the highest (Group 6), 300 percentage points and over.

staff, although two stated it was a role undertaken by other investigators in the unit. Other practitioners do play a role in identifying children at immediate risk of harm, but with a main focus on children within their jurisdiction, often those living with or otherwise linked to local image-based offenders. Some reported other capabilities, with five forces using dedicated intelligence resource and another, a small in-house digital forensics team to assess and analyse the evidence.

3.2 THE EFFECTIVENESS OF THE RESPONSE

Demand

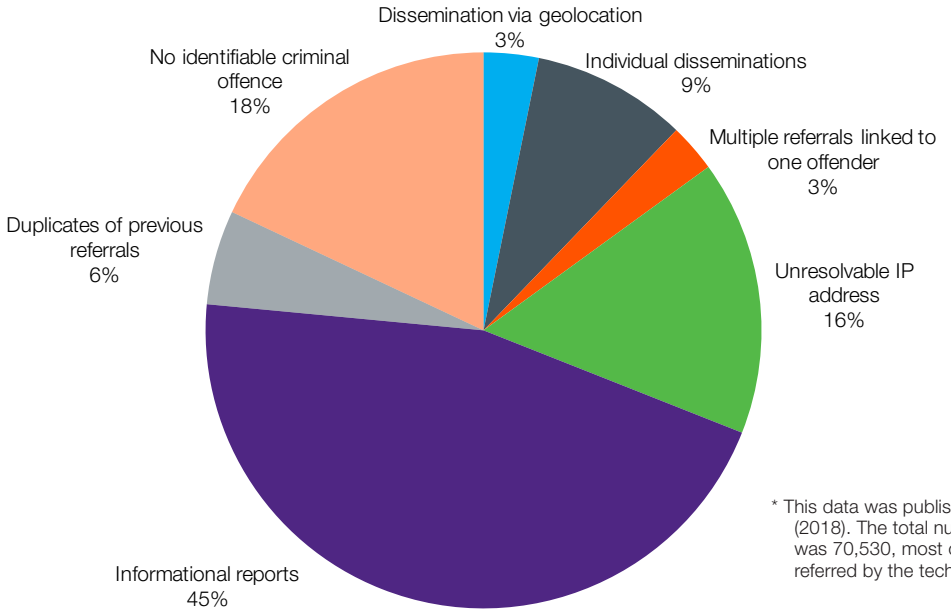
The total number of CSAM offences recorded by the police saw a dramatic change in the period 2015 to 2018, rising by 121 per cent from 8,506 to 18,766. From a low baseline this surge in demand from CSAM offences was not evenly distributed across police forces, ranging from an increase of 8 per cent in one police force and 437 per cent in another.

To help illustrate this point, we grouped police forces to reflect the scale of change in the volume of recorded CSAM, ranging from Group 1 that contained six police forces and saw a rise in demand of less than 50 per cent, to Group 6 containing two police forces that saw a rise in excess of 300 per cent. In addition to an overall rise across all police forces, Figure 3.3 reveals a subset for which the increase in volume was particularly acute. Group 5 incorporates one police force that by 2018 recorded the highest volume of annual CSAM offences, rising from a total of 625 in 2015 to 2,298 in 2018.

If we are to assume that the rise in reporting is evenly distributed across the population and that the volume of offences will reflect the relative size of each police force, from a low baseline volume that was comparable across all the police forces in 2014 the rise in demand has been felt particularly sharply in several larger police forces areas.

50. Police forces were grouped based on the size of the change in annual volume, comparing total crimes recorded in 2015 with those recorded in 2018; this period was chosen due to the very low baseline of recorded offences in 2014 for some forces. There was some variation in the number of police forces contained in each group; Group 1 = 6; Group 2 = 9; Group 3 = 8; Group 4 = 8; Group 5 = 5; Group 6 = 2.

Figure 3.4 The attrition of referrals to the NCA over a period of 12 months, 2016-17*



* This data was published by the NCA (2018). The total number of cases was 70,530, most of which were referred by the technology industry.

Attrition

There is considerable attrition between cases reported to the NCA and those that are disseminated to police forces for investigation. Just 31 per cent of cases referred to the NCA are assessed as eligible for a response (Figure 3.4). In over half of eligible cases, they were unable to locate the suspect and for the remainder, there was a need for the NCA to conduct a desktop investigation to assess and develop the intelligence so as to identify an offender or address (denoted "individual disseminations" in the chart).

Referrals to the NCA encompass images, videos and communications that vary in severity, ranging from penetrative sexual abuse to erotic posing while partially clothed. In order to be classified an indecent image officers need to appraise key contextual factors[51] that determine whether it crosses into the legal definitions of indecency and also judge whether the subject of the image is under 18; both are inherently subjective and the closer to the line, the less certain the assessment (Franqueira et al, 2017; Kloess et al, 2017; Wells et al, 2007). There is a tension for examiners, anxious that no victim gets missed, but with the pragmatic need to focus on material that most clearly depicts criminality, it seems unavoidable that some criminality depicted in the "borderline" images will be missed.

Outcomes

The distribution of outcomes achieved from police investigations has seen significant change in the period between 2014 to 2018 (see Figure 3.5). Most notable is the increase in suspects diverted from a criminal justice system response, alongside investigations that do not progress due to evidential difficulties; by 2018 these outcomes respectively comprised 31 and 29 per cent of all recorded outcomes. The former cases, recorded as "further investigation to support formal action not in the public interest", reflect a shift in policy towards CSAM crimes perpetrated by local children and young people (so called peer to peer offending), with the police rightly now oriented to taking an educational rather than a criminal justice response in these cases (so-called "Outcome 21").[52]

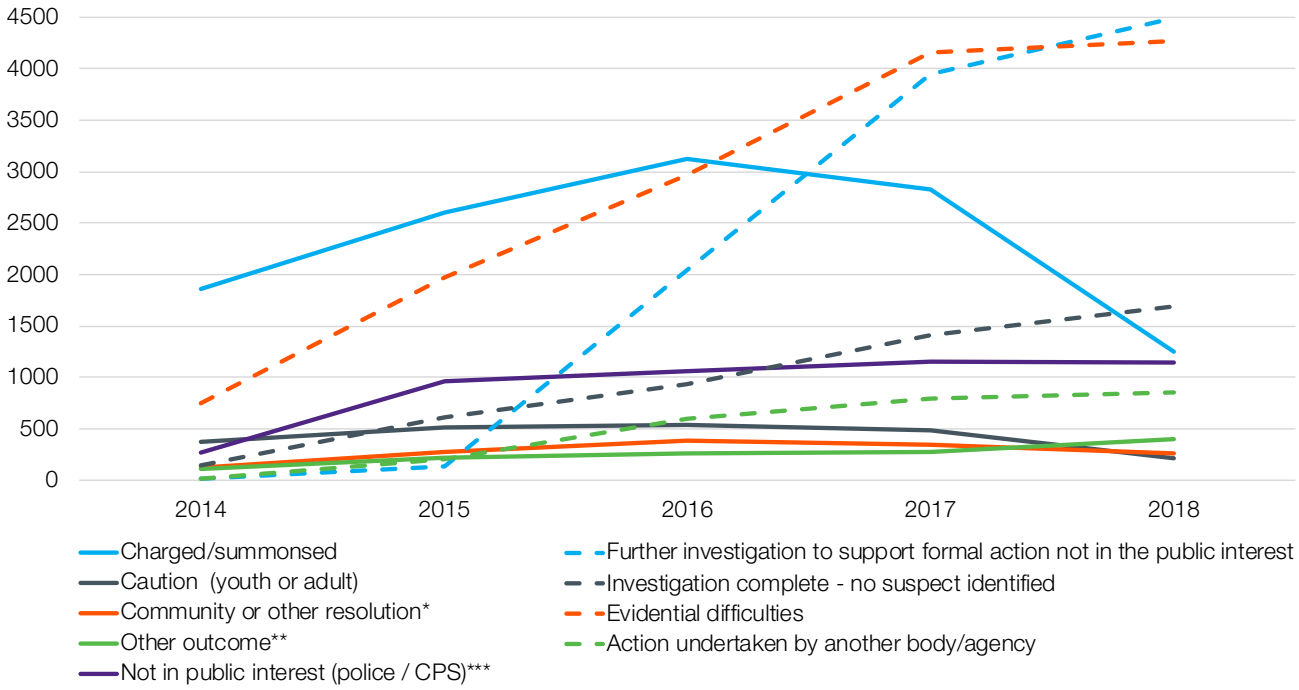
The number of suspects who were eventually charged saw a considerable decline from 2016, falling from a quarter (26 per cent) of all outcomes in 2016 to less than one in ten (9 per cent) in 2018. This almost certainly reflects the more widespread use of Outcome 21 in relation to children and young people who offend.

It is worth noting that police detection rates have generally fallen in recent years, partly due to more complex caseloads, partly due to austerity and partly due to more rigorous crime recording practices, which have added a lot more low priority cases onto the books. The average detection rate for police recorded crime now stands at 7 per cent, which is just under the detection rate for CSAM offences.

51. For example, the context in which an image is shared is assessed not to be exploitative such as the case for viral images which misguided users share due to 'moral outrage' or the image itself is deemed not to be exploitative.

52. Outcome 21 was introduced from January 2016 on a voluntary basis and became mandatory across police forces from April 2016.

Figure 3.5 The police investigation outcomes for CSAM offences, 2014-18[53]



* Comprised of categories 'taken into consideration', 'penalty notices for disorder', 'cannabis/khat warning', 'Diversionary, educational or intervention activity, resulting from the crime report, has been undertaken and it is not in the public interest to take any further action'

** Includes 'offender died', 'prosecution time limit expired', prosecution prevented – suspect under age, suspect too ill or victim too ill or dead' and 'no crime'

*** The majority were assessed not in the public interest by police (96%)

Table 3.2 The police investigation outcomes for CSAM offences, 2014-18

Recorded outcome	2014	2015	2016	2017	2018
Charged / summonsed	1854 (51%)	2605 (35%)	3124 (26%)	2826 (18%)	1250 (9%)
Caution (youth or adult)	373 (10%)	514 (7%)	538 (5%)	492 (3%)	214 (1%)
Community or other resolution*	123 (3%)	282 (4%)	385 (3%)	349 (2%)	258 (2%)
Other outcome**	110 (3%)	216 (3%)	263 (2%)	273(2%)	400 (3%)
Not in public interest***	269 (7%)	966 (13%)	1056 (9%)	1153 (7%)	1149 (8%)
Outcome 21******	15 (0.4%)	138 (2%)	2042 (17%)	3951 (26%)	4493 (31%)
Investigation complete – no suspect identified	145 (4%)	618 (8%)	934 (8%)	1413 (9%)	1690 (12%)
Evidential difficulties	749 (21%)	1967 (26%)	2971 (25%)	4153 (27%)	4270 (29%)
Action undertaken by another body/agency	15 (0.4%)	205 (3%)	591 (5%)	788 (5%)	854 (6%)
Total	3653	7511	11904	15398	14578

* Comprised of categories 'taken into consideration', 'penalty notices for disorder', 'cannabis / khat warning', 'Diversionary, educational or intervention activity, resulting from the crime report, has been undertaken and it is not in the public interest to take any further action'

** includes 'offender died', 'prosecution time limit expired', prosecution prevented – suspect under age, or suspect too ill or victim too ill or dead' and 'no crime'

*** This outcome is determined by either the police of CPS, though the majority were assessed not in the public interest by police (96%)

**** This refers to 'further investigation to support formal action not in the public interest', used to divert young people from a criminal justice response.

53. There was no outcome recorded in 15 per cent of cases (9,102) which for most, is likely to denote investigations that were ongoing.

Many recorded online CSA offences are embedded within wider sexual offence categories such as sexual grooming and sexual activity involving a child that are not all perpetrated online, meaning there are barriers to examining patterns in the national data. Table 3.3 shows the outcomes for investigation of CSAM, sexual grooming and sexual activity crimes in a single police force.[54] This provides an illustration and cannot be generalised to the whole police service. Across the different offence types, the proportion of investigations that led to a suspect being charged/or summonsed was approximately one in ten (broadly in line with the national figures mentioned above). A slightly higher proportion of CSAM offences led to a charge/or summons (14 per cent) than sexual grooming cases (9 per cent) and sexual activity cases (10 per cent).

The average number of days for a charge or summons to be brought in a CSAM offence was 107 days, much higher than in the other two offence types (31 and 53 days).[55] The average number of days to reach a non-criminal justice outcome for a CSAM offence was 30 days. This may reflect the time taken to process the large caseload of CSAM referrals.

Table 3.3 The outcomes and average number of days taken for criminal investigations in a single police force, for crimes recorded April 2018 to September 2019[56]

	CSAM		Sexual grooming		Sexual activity involving a child	
Outcome	**No. cases**	**Av. days**	**No. cases**	**Av. days**	**No. cases**	**Av. days**
Charged / summonsed	122 (14%)	107	22 (9%)	31	27 (10%)	53
Caution or diversionay outcome*	390 (44%)	30	6 (3%)	113	30 (11%)	49
Investigation closed**	373 (42%)	62	206 (88%)	52	214 (79%)	71
Total	885		234		271	

* Includes caution, community or other resolution, not in the public interest (including 'Outcomes 21') and action taken by another body or agency.

** Includes investigation completed with no suspect identified and cases closed due to evidential difficulties.

*** This table omits all investigations with no recorded outcome at the point of extraction (n=562) or for which relevant data was missing (n=2). Multiple offences may be linked to a single suspect; one outlier, a single offender linked to 189 recorded charge / summonsed outcomes, was excluded from the analysis.

54. These offences were screened to select cases the police had flagged as cybercrime or that were identified to have an online dimension based on a manual review of the offence summary. CSAM includes take/make/distribute indecent photographs or pseudo-photographs of children and possession of an indecent photograph or prohibited image of a child. Sexual grooming includes the offences of engaging in sexual communication with a child and meeting a female child following sexual grooming (including those reported by vigilante groups). Sexual activity involving a child includes sexual activity with, involving or in the presence of child, causing or inciting sexual activity, causing a child to engage in sexual activity, causing a child to watch a sexual act and causing sexual activity without consent.

55. This was calculated by taking the difference between the date each offence was reported (or in the cases of CSAM, referred by the NCA) and the date the outcome was recorded on to the police system.

56. This included all the outcomes that were recorded up to the point of extraction from the police database in February 2020.

Box 3.1 A note on sentencing trends for CSAM offences

It is worth noting that fewer people are going to prison from CSAM offences than in the past. This in part reflects a reduction in the number of CSAM offences prosecuted in court, which fell from 22,545 in 2015-16 to 11,096 in 2018-19 (CPS, 2019). This is partly explained by streamlined sentencing that means each individual offender can be charged with fewer CSAM offences for the same outcome, however it is also a result of fewer cases being referred by the police.

Between 2014 and 2020, the total number of offenders for whom a successful prosecution led to an immediate custodial sentence remained relatively stable, constituting a quarter (25 per cent) of all sentences in this period.[57] However, proportionally this has declined over time, falling from 28 per cent in 2014 to 19 per cent in 2020.

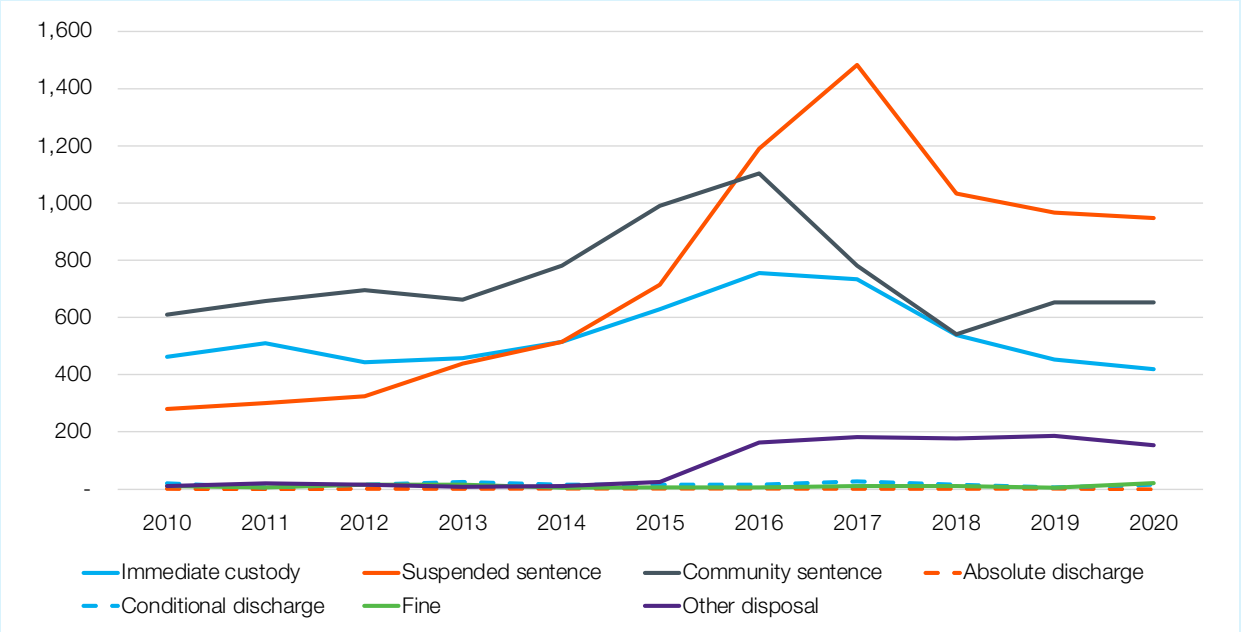
The most significant change to sentencing is the increased number of suspended sentences, rising from 20 percent in 2010 to 43 per cent of all sentences given in 2020. Community sentences are also prominent, accounting for 30 per cent of all sentences in 2020. There has been an overall decline in community sentences which appears to coincide with the increase in suspended sentence disposals.

This may indicate the use of greater controls on convicted offenders while in the community.[58] In 2017 and 2018 23 per cent of convicted offenders received an immediate custodial sentence, and this is often for relatively short periods (Justice, 2019).

Sentencing in courts is influenced by the volume of CSAM, the age of victims and the levels of indecency depicted in the recovered material, factors that are not necessarily associated with risk of contact abuse (McManus et al et al, 2015). In the criminal justice system, non-custodial sentences are hard-wired into the guidelines, and practitioners expressed support for this system but with concerns that the public may perceive offenders to have evaded justice (Palmer et al, 2018). Furthermore, with a propensity to attribute value to criminal justice outcomes, practitioners in the police expressed "frustration" when weighing up resource spent against the sentences received.

> *"Not many offenders get a sentence, the sentence isn't always proportionate to the amount of resource we're putting in … people think this is the worst crime ever, but not many are going to prison for it".*
>
> **(Local police force – specialist online CSA investigation)**

Figure 3.6 Criminal justice sentences for convicted CSAM offenders, 2010-20



57. This includes offences of taking, permitting to be taken or making, distributing or publishing indecent photographs or pseudo photographs of children, possession of indecent photographs of a child and possessing prohibited photographs of a child and possessing prohibited images.

58. Suspended sentences are conditional, in that they will impose conditions to which the offender must abide in order to avoid a more severe sanction.

3.3 THE CHALLENGES OF INVESTIGATING ONLINE CHILD SEXUAL ABUSE

With just 9 per cent of CSAM cases leading to a charge or summons, concerns have been raised about the quality of the police response to online CSA (Home Affairs Committee, 2018). While much of the recent decline in charging rates reflects a justified policy decision to divert more cases involving suspects under 18 away from a criminal justice response (Outcome 21), it is worth reflecting on the challenges to effective criminal investigation in this space.[59]

Gathering digital evidence

The single most significant obstacle in securing a positive outcome is collecting sufficient evidence to attribute the crime to a suspect, a suspect who initially is known only by an online username, account number or Internet Protocol (IP) address that digitally locates an offender's access-point to the internet (i.e. the device used to access the internet).

The starting point is commonly to trace these digital identifiers to an address or person through the submission of subscriber checks to the relevant web company or internet service provider. Once a suspect's real-world identity or location has been revealed, there is a requirement to collect evidence of the reported offence or other offending, commonly through a process of search, seizure and examination of internet-enabled devices.

Practitioners described a multitude of obstacles put in place either by the technology, suspects who purposefully seek to evade detection or other circumstances that to a varying extent put the process of evidence-gathering out of police control.

Without a trace: Encryption technology can be used to hide and render untraceable an online offenders' real-world identity. Practitioners highlighted the use of virtual private networks (VPNs) to connect to the internet, end-to-end encryption services and the dark web as the key barriers to either identifying suspects in the first place or uncovering evidence of their offending.

Attribution: Attributing a crime to a location or device does not always attribute a crime to an individual offender, especially if access-points or devices are in use by multiple users. For example, this would be the case with a search that leads to a public-access wi-fi (such as in a hotel) or a multi-occupancy household.

The absence of evidence: Everyday technologies such as encrypted devices that are only accessible to the owner (e.g. smartphones) can put them beyond the reach of investigators, and while there are legal channels to compel suspects to provide access these are complex and protracted processes that need to be used sparingly.

Offenders can also delete evidence of criminality and elect to use services that automatically deletes messages that are sent (for example, certain messaging apps). In some cases, the victim or family member who reports a crime delete messages on the victim's device before the visit from the police.

Furthermore, people don't need to store files on their device anymore due to streaming and cloud computing technology, and while offenders can seamlessly move across borders, the police must enlist protracted processes of engagement with the relevant overseas jurisdictions. Deriving evidence from these technologies was cited by several practitioners as a key challenge to responding. When asked to identify challenges to criminal investigation they highlighted:

> *"The ability to identify the existence of cloud accounts held by suspects and clear protocol/ guidance as to how to capture this evidentially … [and] obtaining evidential product from non-UK based ISP/social media companies."*
>
> **(Local police force – specialist online CSA investigation)**

> *"Platforms that anonymise the offenders' accounts and refuse to cooperate with law enforcement. Cloud storage accounts being [a] means of storing and sharing [data]. Encryption of devices and platforms being only online."*
>
> **(Local police force – specialist online CSA investigation)**

Capabilities in the private sector: online CSA investigations encompass a vast range of private sector stakeholders whose internal capabilities and systems are governed by different technologies and policies. For example, there is variable capability among internet service providers for resolving (or matching) an IP address to a physical address and some web providers afford more anonymity to their users than others.

59. It should be noted that while law enforcement and safeguarding are considered the key measures of success, criminal investigation can produce a range of other benefits, such as risk reduction in the form of offending that has been prevented, offender management, disrupted criminality and the reduction of victim vulnerability and victims who experience positive contact and feel safer as a consequence.

Information sharing

In our survey, the limited availability, and delays in accessing intelligence or evidence from technology companies were among the most commonly described challenges. Specifically, practitioners highlighted applications for evidence from private companies which are often overseas and can be slow to respond or non-responsive, or which use a technological infrastructure that restricts the scope to collect evidence. There are few other areas in which a public police response of this significance is so dependent on the policies and processes of businesses in the private sector, many of which are based in other countries.

The information the police receive from the NCA on local CSAM offenders is not standardised, coming from a range of different companies, working to internal policies that can change over time. Consequently, there is high variability in the comprehensiveness and timeliness of the information provided, which impacts the prospects for investigation.

In addition to internal systems for detecting and processing offences on a platform, referrals need to pass through bottlenecks in NCMEC, the NCA and local police teams, and so a police investigator may eventually respond to a crime that took place six to 12 months ago.

In one extreme example, a social media company had run a "sweep" of its platform, finding evidence of offending from nine years previously. The many aspects of a suspects' life that may have changed in even six months (for example, changes in address, online accounts, or electronic devices) may mean evidence is lost, and in turn courts become more hesitant to issue arrest warrants. Moreover, if the information was insufficient to proceed, an investigator may have to go back to the company for more information which they may not provide.

> *"We don't really have sight of how they're [individual social media platforms] identifying content … It feels like everyone uses their own processes … we're kind of beholden to what we're given."*
>
> **(NCA – Specialist practitioner)**

Many enquiries lead to companies in overseas jurisdictions, requiring application to the local judicial authorities in that country to assist with collecting the evidence (i.e. the Mutual Legal Assistance Treaty or MLAT). The police must use this process sparingly due to the protracted nature and precariousness of the process.

> *"Law enforcement and prosecuting organisations should work together more closely in an attempt drastically reduce the time duration of the MLAT procedure."*
>
> **(Local police force – specialist online CSA investigation)**

> *"[The MLAT] process is only instigated for our most concerning suspects where evidence has not been recovered via other means and we have not yet been able to prosecute any of these. We currently have three such cases involving MLAT one has been through the UK process and is sat with US authorities – this is now 16 months since the MLAT application."*
>
> **(Local police force – online CSA strategic lead)**

Recommendation 2

Working with international partners, the Home Office should look into how it can speed up the mutual legal assistance treaty process, the process of securing legal cooperation in other countries.

Functional cooperation

Like other areas of cybercrime, the assessments and response to online CSA are often spread over a multitude of nodes in law enforcement and other sectors within the UK and internationally, reflecting the different aspects of the response (for example, investigation, prevention and child protection) and the geographic diffusion of offenders, victims, web companies and evidence. Therefore, practitioners tasked with responding are often wholly reliant on disparate organisations to facilitate or take ownership of the case. To illustrate, a local police officer described a routine response to a local victim involving the submission of devices to the local digital forensics teams, charter applications to relevant web companies to collect evidence on the suspect, and then a process of referring evidence to the relevant police force in the UK or overseas where the offender is suspected to be located. None of the organisations in the chain to produce this evidence will know the product of the work, either in terms of investigatory outcome or even whether a decision was taken to proceed with the case.

Practitioners described considerable friction in decision-making across the different layers of law enforcement, between police forces in the UK and other organisations that operate with different cultures and priorities. The consequence is that extensive investment of resource into investigation or safeguarding can be swiftly undermined in cases that come to depend on the cooperation of external organisations (Snell, 2016).

For example, specialist officers in a local police force described responses from practitioners in the local authority and Crown Prosecution Service (CPS) that were not always commensurate with what they expected. In part this is because there is no universal language of risk, with each agency working to priorities and a caseload that gives its own perspective for assessing the merits of a given case.

This incongruence or ambiguity over values and priorities is also experienced from the top, with the NCA processing high volumes of CSAM referrals but retaining little influence over the outcome:

> *"I spent three to four weeks trying to find that person and [local investigators] will say oh, that's a moral outrage case or they've sent that for comedy value [and so will not progress] … we need some guidance on what's public interest."*
>
> **(NCA – Specialist practitioner)**

Recommendation 3

We recommend that the National Crime Agency explores the feasibility of establishing common standards for risk assessment and case prioritisation across policing and partner agencies.

These organisational frictions are writ large when engaging with overseas law enforcement, who can operate to political values and priorities, legal systems and protocols that are at odds with those in the UK, affecting both criminal investigation and safeguarding outcomes. For example, practitioners described a requirement of the US authorities for there to be evidence of a criminal offence before they will intervene, meaning an investigation that identifies an unevidenced risk to a child will not lead to an intervention. In part this reflects the low thresholds of risk in the UK relative to other countries, but also varying levels of law enforcement capacity and capability in the different countries, which leads to frustration and considerable uncertainty over outcomes:

> *"Even countries who you would think would be all over it, just aren't."*
>
> **(ROCU specialist online CSA investigation)**

> *"Half the time we don't know what's happened (with the referral) … I suppose it's our way of saying we've done as much as we can."*
>
> **(NCA – Specialist practitioner)**

Box 3.2 Managing the welfare of officers investigating CSAM offences

Research is starting to identify the short and long-term emotional, cognitive, social and behavioural consequences for officers regularly exposed to CSAM in the course of their duties (Powell et al, 2015). Secondary trauma and post-traumatic stress are a concern, including physical and emotional stress responses such as fatigue, headaches and fluctuating moods, and it can also place a strain on personal relationships (Burns et al 2008; Craun et al, 2015; Tehrani 2016). In recognition of these risks the National Police Chiefs' Council (NPCC) produced guidelines and protocols in managing the welfare of specialist online CSA teams. The recommendations include annual psychological assessment for existing staff and recruitment policies that screen individuals for suitability and limiting candidates to those who volunteer (i.e. no forcible transfers).

In both interviews and surveys, many described the negative impact that can be caused by exposure to CSAM.

> *"This is still in its infancy, no one has been able to study the long-term impacts of looking at this stuff for 20 years … it worries me that we could potentially be really damaging people."*
>
> **(NCA – Intelligence Officer)**

There was variation in the levels of welfare provision described in different police forces, ranging from the minimum recommended standard in national guidance to more comprehensive support programmes that included training in recognising secondary trauma, access to force psychologists, shortened review periods and psychological debriefs after investigations. In our survey, some local specialist leads described having no specific policies to guide recruitment and day-to-day working. However most relayed protocols for structuring the work of specialist investigators to minimise harmful exposure and embed support mechanisms into the daily routines of the team.

> *"Grading [is] not done alone, regular breaks, no more than four hours per day, no viewing in [the] final hour of duty. Once every six months the staff are seen by a welfare officer, and every one month de-briefed by a supervisor. There are also welfare information leaflets, paper and online available in all offices."*
>
> **(Local police force – online CSA strategic lead)**

Box continued overleaf

Box 3.2 continued from previous page

There was tension in maintaining these policies and managing the overwhelming volume of images that required grading, and some described bending the protocols in the interest of managing the workload. Image grading is primarily an administrative process for evidential and legal purposes and in and of itself does not necessarily further investigations. There have been significant steps in Artificial Intelligence technology to analyse and grade images, although it is not yet adopted across all forces or specialist teams. Use of such technologies would go some way to easing strain on investigators both with their workloads and unnecessary exposure to CSAM that may lead to increased traumatisation over time.

Recommendation 5

The Home Office and police forces should increase their investment in technologies to process, analyse and grade CSAM. These tools need to be embedded in the work of all specialist investigation teams.

In relation to the available support, there was variation in the attitudes from investigators across different specialist teams. Some were satisfied with provision and others viewed the protocols in place as perfunctory (or "tick-box") exercises that fell short of what was needed. One investigator felt the reality was that the organisation leaned too heavily on the personal resilience of each member of staff. One senior officer emphasised the need to tailor monitoring and welfare to each individual, rather than rigidly impose the same protocols that may be of less benefit for some.

"Each member of staff is different, some share more, some manage their own welfare and some have more personal resilience than others … [while there are some happy to ask for help] we are working hard to create a culture where they are happy to do so."

(Local police force – online CSA strategic lead)

Close and attentive supervision was one of the key requirements in delivering support for officers for the following reasons:

- Many described a culture in which officers were inhibited from coming forward, with some describing 'fear' in the team, of being honest about how they felt and expressing their need for help. Reasons included embarrassment and the potential consequences for remaining in the team.
- The reluctance of many officers to come forward required supervisors to be closely attuned to each individual staff member to proactively monitor their behaviour. It is "unpredictable what triggers a negative response", depending on each individual and their reaction to the specific content in the CSAM (Powell et al, 2015).
- Finally, there was the risk that continued exposure desensitises officers who become less able to effectively identify the harm and risk contained in CSAM.

"The POLIT team have two Sergeants and an Inspector who monitor staff welfare and workloads daily. They are acutely aware of [the needs of] each member of staff … and use a PDR system to check in on staff."

(Local police force – online CSA strategic lead)

Another important element was a supportive and open culture within the unit; one senior officer placed emphasis on "team social activities". This was considered to help bolster individual resilience and in building relationships between colleagues; others in the team could help to identify any who might be struggling in their work.

"You need comradery, to take a break, have a laugh, to have good interpersonal skills, and recognise if things are getting too much, to take a step back."

(NCA – specialist practitioner)

There was variable support for a restricted tenure policy which imposed limits on the length of time any single individual could work in a specialist unit. Some considered this necessary to restrict long-term exposure that could be detrimental to an officers' or staff members' health and to mitigate the risk they become desensitised to these crimes. However, this fails to account for the variability between staff in their personal motivations and resilience, and in a highly specialist area of policing, can lead to the continuous drain of knowledge and experience from the team. Some considered departures from the team should be based on personal choice or individual assessments by supervisors or occupational health professionals, instead of a uniform and arbitrary time constraint.

Box continued overleaf

Box 3.2 continued from previous page

"In truth, a lot of people enjoy the job because it's important … also because we manage them and look after them well, probably more than anywhere else in the force … there's a risk [that] people become process-driven … I'd hope our DS would pick up on this straightaway … I'd expect them to know the staff inside and out and spot when things aren't right."

(Local police force – online CSA strategic lead)

The policies and provision described here pertain to staff working in specialist units regularly exposed to CSAM. However, in some (particularly smaller) police forces there continues to be the need to allocate these crimes to officers in generalist investigation teams. A number of practitioners expressed concern over the potential unmet need for support and welfare, with less consistency and active supervision and instead a reliance on officers coming forward for help, which as discussed, many are reluctant to do.

"Some of the support available to non-specialist officers is reliant on those officers self-identifying problems which in turn [is] reliant on an individual's experience, service, views on dealing with mental health issues and ability to ask for help."

(Local police force – online CSA strategic lead)

Recommendation 6

Police forces should actively monitor the impact of CSAM investigations on generalist officers and staff. They need to establish channels for accessing support that are clearly communicated to encourage officers or staff who are negatively impacted by their work to seek help.

3.4 AREAS FOR IMPROVEMENT

In this section we highlight four priority areas for improvement that would enable the NCA, the police and partners to pursue online CSA offenders more effectively.

Gaps in the risk assessment of offenders

The Kent Internet Risk Assessment Tool (KIRAT) is a standardised framework adopted by police to make sense of the demand from CSAM offending. Despite the name, KIRAT is referred to as a "prioritisation" tool rather than a risk assessment tool. It is a standardised framework used to appraise each CSAM suspect to help practitioners decide which cases merit a more urgent response. At its root, it is founded on the assumption that CSAM offending has an intrinsic association with contact abuse (Long et al 2016), and examines various mediating factors such as previous offending history and access to children, to assess the likelihood that a suspect will engage in these more serious sex crimes. In principle, this tool does not discount the potential for any CSAM suspect to perpetrate contact abuse, it merely guides practitioners on how to sequence their investigations.

This framework offers a standardised and auditable trail, intended to give practitioners the confidence to engage in high-stakes decision-making. With such low tolerance of risk, practitioners inevitably expressed some anxiety about relying too much on an actuarial measure, some of which pertains to problems they identified with the way KIRAT works:

- **Blind-spots**: As described earlier, intelligence for online behaviour can be unreliable as an indicator of contact abuse offending, therefore they rely on alternative risk indicators from offline settings (for example, employment that gives them access to children), the availability of which is highly variable. For example, many suspects were found to have had no prior contact with the police or partners so were absent from their systems. In short, the absence of information need not mean the absence of risk.

"if you don't know much about your suspect, KIRAT low does not mean low risk, it just means we don't know much about that person."

(Local police force – specialist online CSA investigation)

- **Application**: The continuous flow of new referrals meant that the lowest risk cases can stagnate at the bottom of the pile. This led to divergent interpretation and application between police forces, with some assigning the cases to non-specialist officers and others providing no response at all.

"… all of them have to be dealt with, all of it's a priority … if you have a low priority case and it's been lying around for a period of time, you can't not respond because you keep getting mediums through."

(NCA – Specialist practitioner)

- **Professional judgement**: The actuarial measures often did not account for contextual factors observed and considered salient by practitioners. This potentially reflects a lack of understanding, experience or confidence in using and interpreting KIRAT, with some practitioners more readily applying their own professional judgement than others. Notably, one police force had developed their own "matrix" to supplement KIRAT, to systematise the inclusion of other factors they considered relevant.
- **False positives**: as indicated earlier, the perception of many that only a minority of investigations are uncovering evidence of contact abuse, indicates a propensity for higher risk cases to not bear out. One overseas practitioner suggested it potentially reveals faults in an approach that assumes an association between CSAM offenders and contact abuse. The alternative interpretation is of course the potential failure of investigators to find it.
- **Online harm**: It takes no account of the risk a suspect will engage in serious *online* offending.

Recommendation 4

The National Police Chiefs' Council should continue to review the prioritisation framework used by police forces (KIRAT) to address existing gaps and to ensure that it takes into account the risk of a suspect engaging in serious online offending.[60]

Capacity

The rising volume of CSAM offenders is placing a considerable strain on specialist teams in the NCA and local police forces, creating an unabated flow of demand seemingly unaffected by the continuous law enforcement activity. Many perceived that in dealing with such widespread offending, law enforcement represented a sticking plaster rather than a solution. Practitioner concerns were amplified by a perspective that much of their efforts were directed to managing the "really low hanging fruit", rather than the most serious and persistent sex offenders responsible for proliferating CSAM.

"We can't arrest our way out of this, there's too many people viewing these images."

(NCA – Specialist investigator)

"[It is the local police] teams who are dealing with it, are constantly having to fight fires rather than getting on top of the work they've already got … Day-to-day, [you] receive one referral after another, not feeling like you are really making a difference."

(NCA – Specialist investigator)

In dealing with such high volumes of offending the quality of investigations can suffer and worse still, there is the chance that serious offenders slip through the net. In processing each CSAM referral, a criminal justice outcome can be achieved independently of any safeguarding outcome, with the former constituting a reactive policing response to a reported CSAM offence and the latter, more complex and resource-intensive proactive investigations to discover hidden offending and risk. It is a scenario in which *process* can be emphasised over proactivity, to manage the continuous flow of offences for what they are (i.e. indecent image offences) rather than seek to identify the hidden risks that may lie underneath.

"The challenge is volume. If you don't have volume you can focus on tactics, skills and techniques, but volume means you are under pressure to churn out outcomes."

(Local police force – specialist online CSA investigation)

"… you become process-driven, most of the time it's develop intelligence, get a warrant and execute it."

(Local police force – specialist online CSA investigation)

Proactivity in this context is primarily rooted in specialist technological and safeguarding capabilities, to conduct comprehensive searches and examinations of digital devices and data and identify risks in the suspects' local community. It is the mismatch between the availability of specialist resources to undertake this more proactive work and the high volume of demand that constitutes the most significant shortfall in capacity. In our survey, when asked for the issues that caused the greatest challenges to the local response, many highlighted the deficit in specialist investigation and digital forensic resources. Specialist resources spread too thinly across volume crime meant impaired and slower investigations. There were considerable delays to accessing critical digital forensics teams, with one reported to be "fighting a six to 12 month backlog".

60. The National Crime Agency reports that KIRAT is currently under review and a new iteration of the assessment will be introduced in the near future.

"The biggest challenge is sheer volume of the amount of referrals and cases, the second leads from the first and that is the volume of work being created for the digital forensic teams …"

(Local police force – specialist online CSA investigation)

"Managing the year-on-year increase in demand with no matched uplift in resources to reflect … The pressure on digital forensic examiners to examine devices timely and thoroughly."

(Local police force – specialist online CSA investigation)

This deficit in the right kinds of resources, naturally leads specialist teams to make use of any pressure valve that is available to them. In some police forces lower risk CSAM suspects (and many online grooming offences) are referred to generalist investigation or other local police teams to respond, teams less able to engage in proactive investigation to identify hidden crime and risks. It was indicated in interviews that some local investigation teams did not proceed with an investigation if the case was deemed low risk..

There is a lack of resources at the different levels of investigation. Over two thirds (24 or 69 per cent) of senior stakeholders reported insufficient resource in their digital forensic teams to tackle online CSA and over half (17, 52 per cent) reported insufficient resource in their specialist investigation teams. An even higher proportion (23 or 72 per cent) reported insufficient resource in their local police teams, and 59 per cent (19) in their generalist investigation teams. The capability deficit among generalist officers exacerbates the situation, with limits in standardised skills and knowledge exaggerating inconsistencies and the risk of missed investigative and safeguarding opportunities. A small number of police strategic leads highlighted the limits in the capabilities of generalist local police teams as a key challenge in undertaking effective investigation, a particular issue with the increase in youth-produced images by local children and young people.

In a sign of how stretched investigative teams are, there is software available to all police forces to identify offending in certain online spaces, and as "the only work stream [they] can control" this can simply be "switched off" while they manage the crimes already on their books. As described earlier, in lieu of a criminal investigation there are considerable challenges in identifying a suspects' risk. Therefore, a filter used to withhold or downgrade the response based on preliminary assessments or a specific reporting channel, runs counter to the overarching ethos of policing guided by the principles of harm reduction and safeguarding.

In addition to the core work of criminal investigation there is also an immense administrative challenge in managing large datasets comprised of CSAM and online communications retrieved from suspects' devices, or in the case of the NCA, referred by industry or others.

"[We are] very much focused on the victims in these images … for the purposes of investigation they might only need 200, but if there's a million images, we'll look through them."

(NCA – Specialist investigator)

Newly identified images (i.e. those not already on the CAID system) are themselves treated as a virtual crime scene that can reveal victims, children at risk and other suspects. Furthermore, there is a continued reliance on manual processes for categorising images to inform decision-making in the justice system (i.e. grading Category A-C). This was described to be one of the most time-consuming tasks by practitioners, and the lower the grade of the image the more labour-intensive the process due to the difficulties determining whether it meets the definition of indecent. Technology was posited as one solution to this "informational strain", with the potential to develop software to automate the detection and categorisation of CSAM using image recognition technology. One senior practitioner in an overseas law enforcement agency questioned the value of grading images as it detracted from getting on with the business of investigation and safeguarding:

"That's not what we should be doing, we should be investigating the crimes within these images … "

(Overseas law enforcement – specialist practitioner)

There is a concentration of duties on pressurised operational teams, not just to investigate online CSA suspects, seize and examine digital evidence, but also to process large datasets to generate new intelligence on victims or children at risk and the heavy administrative task of classifying images to aid decisions in the criminal justice system.

The compromise in concentrating knowledge and capability in discrete units can be to marginalise the problem and erode capability in the wider workforce (Chatterton, 2008). This is increasingly apparent in the context of online CSA that has grown to overwhelming volumes, with an over-reliance on a subset of specialists or experts creating a bottleneck at pinch-points in the system which slows the process. In reality,

work that was once designated "specialist" is spilling over into the everyday work of other teams, and this requires effective diffusion of relevant knowledge and skills to work effectively with the technology, victims and investigative protocols (especially for engaging with industry or overseas law enforcement agencies). Local victims of online CSA make up a considerable demand on the policing frontlines and one response officer described the investigations as "daunting" and "protracted", and difficult to manage alongside all other competing demands. Similarly, specialist investigators are required to complete data analyses at crime scenes to assess and triage prospective evidence, a task that was historically the remit of digital forensic teams.

"It's resources, not enough people being pumped into it, too much red tape … devices can go through [assessment] and highlight new offenders, which call for more intelligence gathering and further law enforcement, and there's just no money and resources to deal with it."

(NCA – Specialist investigator)

"[The] frontline response and neighbourhood officers to recognise and be able to provide a quality initial response to online CSA is minimal, confidence and competence levels of frontline resources are therefore also low."

(Local police force – specialist online CSA investigation)

"No doubt there is someone in the force sat on a number of [CSAM] cases and they don't know what to do with [them]"

(Local police force – specialist online CSA investigation)

A capability deficit in digital investigation not only has implications for the likely outcome of an investigation, but also operational decision-making on the time and resource to invest into the discovery and development of evidence. Formal and informal assessments for the proportionate use of police resources take into account the seriousness of the crime, but also the resource requirement and likelihood of success (i.e. viability), which can be as much the product of professional competence as it is the complexity of the case (Skidmore et al, 2020). Tasks that are left in the least sure hands will be most affected, especially in areas of digital evidence recovery which is critical in the work to proactively identify investigative and safeguarding opportunities. In the case of non-localised victims, offenders or risk, visibility is entirely dependent on being able to draw data and insight from digital sources.

"Sometimes we have come across investigators that will go, 'I've found x amount of images, that's enough for me to charge … and we've gone back and looked at the evidence and go 'did you see the guy had been paying for the streaming to take place, did you see he was actually grooming this child, did you see he was actually booking tickets to travel over to see this country?' and they'll go 'no, no, but we actually got a conviction so it's ok'."

(Private sector representative)

"[Generalists in the police] don't know what they're looking for and taking everything [in terms of devices/ data] is not proportionate. You need to know what you're looking for and when you get it back [from forensics], you have to know what it means".

(Local police force – specialist online CSA investigation)

The barrier to embedding sufficient technical capability is that the existing baseline is too low to keep pace with the volume and speed of change in cyber criminality, and skills and knowledge are falling short at all levels. The assumption that overall technical capability would rise naturally with each intake of younger, digital-native recruits has not borne out. More familiarity with everyday "user technology" such as apps and devices does not equip someone with the skills to undertake investigations that demand increasing amounts of technical understanding. This is particularly salient to specialist teams that need to recruit from within the generalist workforce.

"It's almost like it's going the opposite way … you would assume new people would be coming in with a reasonable level of knowledge but it's almost the opposite to that really."

(Local police force – specialist online CSA investigation)

In addition to raising overall baseline capability, the workforce configuration might become more aligned to the demands on policing that in this context call for expertise in digital forensics and child protection. In our survey, practitioners commonly cited the challenge of the lack of capacity in digital forensics teams to meet the scale of demand, causing extensive backlogs that prevent investigations being progressed at sufficient speed.

"Greater investment into the hi-tech [i.e. digital forensic] crime units. If they gave me ten more cops in [the specialist investigation team], I'd use them … but the hi-tech crime unit is already creaking. We don't always need it at the front-end, but more in the back office."

(Local police force – specialist online CSA investigation)

"Managing the year-on-year increase in demand with no matched uplift in resources to reflect [the increase], however, this is not unique to online CSE … [and the] pressure on digital forensic examiners to examine devices timely and thoroughly."

(Local police force – specialist online CSA investigation)

Recommendation 7

As part of a wider strategic assessment of workforce skills, the National Police Chiefs' Council and the College of Policing should map current skills against required capabilities in relation to tackling online CSA. This exercise should then inform a new national plan to recruit and train the people required to address identified skills deficits.

Skills gaps

There are various ways in which to equip the workforce with the skills and knowledge needed to deliver an effective response. This includes embedding knowledge through the provision of training or providing accessible information hubs, either in the form of technological aids or specialists that can be contacted for advice. The knowledge-requirement covers a range of elements needed to investigate crimes and identify risk:

- Key legislation and the nature of offending and risk.
- Online investigative techniques.
- Crime scene investigation techniques including the ability to triage and target the collection of digital information either as evidence or intelligence (including that indicative of risk).
- The use of technological equipment to aid data retrieval and assessment at a suspect or victim's address.
- Image grading techniques.
- Skills to engage and conduct formal interviews with suspects, victims and children at risk.
- Effective risk assessment and understanding of safeguarding protocols.

"[Digital forensics is] definitely a knowledge gap … the officers need a couple of days input really. What is a digital device, what might you find on there? In some regards, they think [digital forensics teams are] the magic bullet, but we're not."

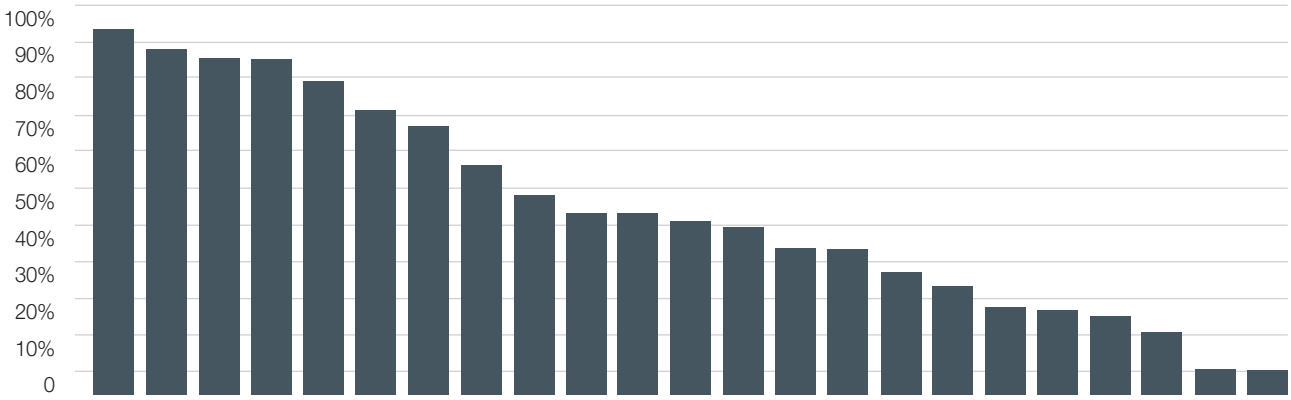
(Local police force – specialist online CSA investigation)

"[We've produced software that is] a little bit complicated, a bit technical … there are vast differences in the skills, training and competence across users [in the police]."

(Local police force – specialist online CSA investigation)

A survey of police officers in the UK and other European countries found a high proportion had not received any specialist training to tackle online CSA (Davidson et al, 2016). In the UK only 16 per cent of officers had received specialist training on online CSA, 38 per cent had received more general training and 47 per cent had received none. These findings are echoed in our survey of police strategic leads, though with wide variation between local police forces. Overall, nearly two-thirds (64 per cent) of staff in dedicated online CSA roles had not completed the specialist child investigation training course (see Figure 3.7).[61] In five police forces respondents reported that none had received any training, whereas in three, over 90 per cent of staff had receive the training. Some stated that training was only provided to criminal investigators in the team.

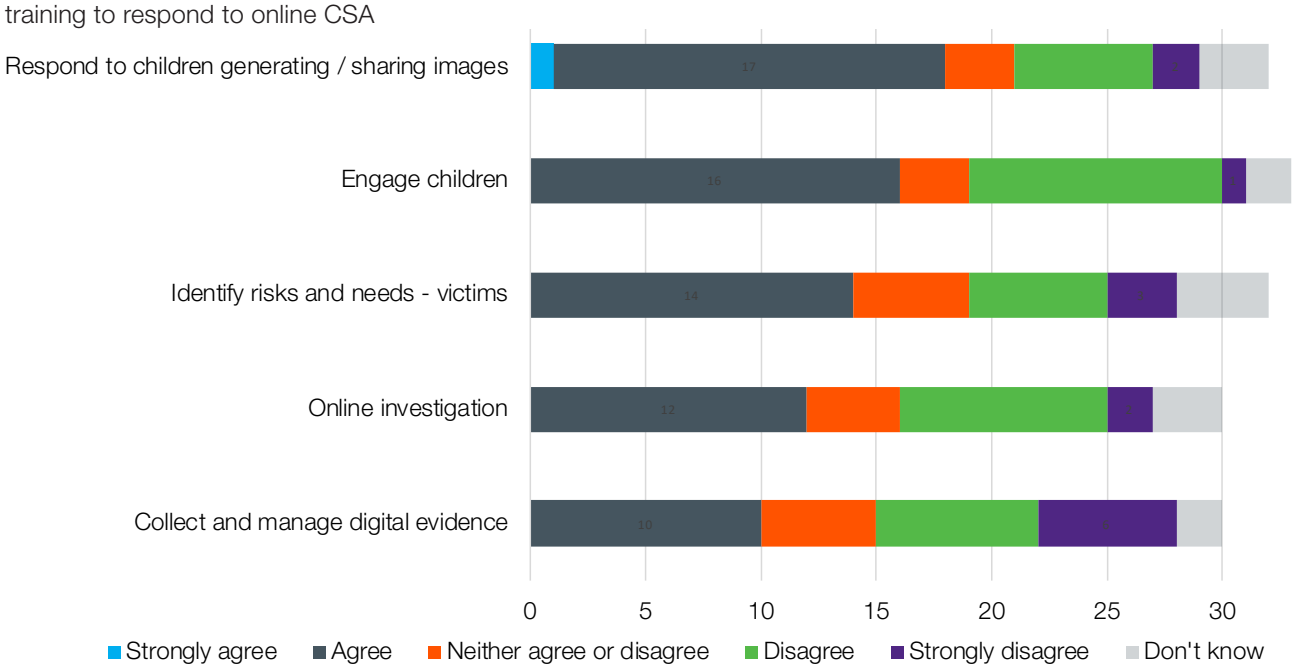
Figure 3.7 The percentage of staff in a dedicated online CSA role who had attended the specialist child investigation training course, by police force*



* Each bar represents an anonymised police force

61. A small proportion of officers were reportedly waiting to attend a course.

Figure 3.8 The perceptions of police strategic leads on whether officers in generalist teams receive sufficient training to respond to online CSA



When asked if they thought officers in generalist teams received sufficient training to respond to online CSA only a third (10 or 33 per cent) considered there was sufficient training in online investigation and 40 per cent (10) said there was adequate training for collecting and managing digital evidence (see Figure 3.8_). The main barrier is the absence of core digital skills training programmes for officers in non-specialist roles.

"Outside of specialist digital forensic or digital investigation training there are no digital training courses to assist front line officers and investigators to enable them to understand online activity and how to interpret digital evidence."

(Local police force – specialist online CSA investigation)

"The main improvement is to find the right level of training for the different areas which in many cases does not exist."

(Local police force – specialist online CSA investigation)

Some research found training was not always sufficient to build the confidence of practitioners,[62] especially in the general workforce for whom there is a challenge of embedding knowledge and skills in subjects that fall outside of the everyday. Some described technological solutions such as the Blue Light Digital app which can provide a reference point for officers when on the scene;

"it's like having the Digital Forensics and Cyber Crime Unit on your phone, providing advice on investigative strategies."

(Local police – specialist investigation team)

Digital Media Investigators are in essence specialists in cybercrime and in some police forces provide a central point of contact for practitioners in need of advice or guidance, but their role can vary in different police forces.

Law enforcement needs to adapt to the fast-moving digital environment and changes in hardware, software, the policies and functionality of each individual online platform, and wider social trends such as online spaces that are emerging or most popular. In this regard, changes in online markets and policies of communications providers influence patterns in offending and modus operandi which can erode effectiveness if the police are slow to adapt.

"Knowledge of new platforms, the changing world of social media and online platforms, it's so quick and fast-paced and law enforcement are going to have to keep up … It's like painting the Forth Bridge, you get good at something, then that becomes the old crime."

(NCA – Specialist practitioner)

62. This was a finding by overseas researchers interviewed for this research.

Consequently, structured training can strain to keep pace, especially for specialist officers working at the sharp end of the technological response for whom real-time knowledge and expertise is established in the course of their work or can only be sourced from experts outside of police, with a cost-implications for stretched budgets;

> *"the area is so new, the knowledge isn't there yet"*
>
> **(ROCU investigator)**

Many interviewees from specialist teams described an expectation that they would learn on the job, relying on informal knowledge exchange between peers as opposed to formal training. These more organic approaches to learning can be effective, particularly for specialists fully-immersed in this area of work, but can leave scope for inconsistency and mistakes and is contingent on having the requisite expertise within the team (a situation rendered more precarious by restricted tenure policies). Officers in a Regional Organised Crime Unit reported some limited informal sharing between units on a police online hub, but most was through informal connections with other teams.

> *'We do look at each other's work and see what each is doing and I have had emails before from other investigators'.*
>
> **(ROCU specialist online CSA investigation)**

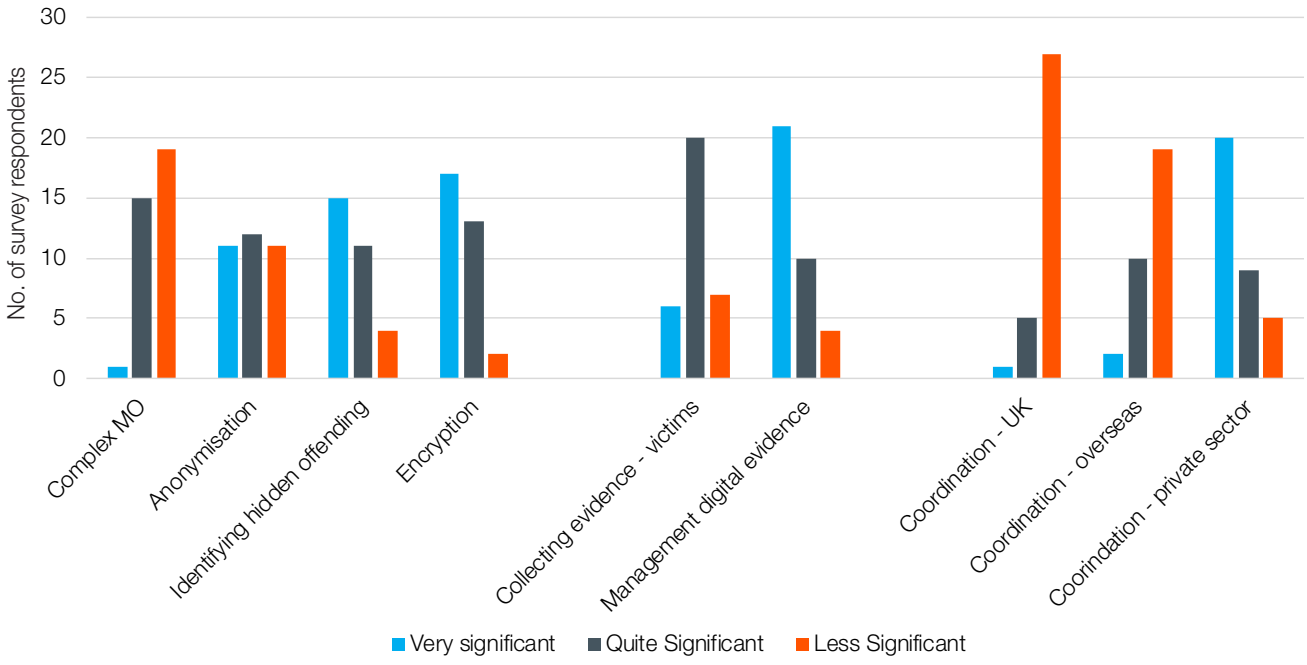
Technology constraints

The rapid technological developments for storing and sharing data in everyday life are not mirrored in the police technological infrastructure, meaning police systems are creaking under the pressure to collect, process and apply the vast amounts of data collected in the search for evidence and intelligence on offending and risk. A reliance on manual processes for managing information is no longer sustainable for effective and efficient policing, and law enforcement can only be as good as the technology in place to support it.

In our survey, internal processes for managing digital evidence were described as one of the most significant challenges in investigating online CSA, more so than other factors such as the innate complexity of offending or coordinating the response with partners (see Figure 3.9 below). 60 per cent (21) described management of digital evidence as a very significant challenge. 17 (52 per cent) of respondents mentioned technological enablers for offending such as encryption, 11 (32 per cent) raised anonymisation and 20 respondents (59 per cent) mentioned working with the private sector as another significant challenge.

> *"The ability to manage digital evidence across the piece is having a significant impact upon capability and capacity within the whole system."*
>
> **(Local police force – specialist online CSA investigation)**

Figure 3.9 The perceptions of lead online CSA investigators on the most significant challenges to criminal investigation



The lack of cohesion between police IT systems, including a lack of consistency in the way technology is adopted and barriers to networking the systems of different law enforcement agencies to facilitate seamless information exchange, is a long-standing challenge for UK policing, in large part due to the innately fragmented governance structures and funding arrangements across 43 local police jurisdictions (Crowhurst, 2017). These issues can impede day-to-day operations, organisational learning and the scope to innovate, and in the context of hidden and borderless offending, leaves sizeable blind-spots on offending and risk.

The global efforts by private sector companies, governments and law enforcement have propelled some advancements in online CSA. None more so than the PhotoDNA software developed by Microsoft which provides an international standard for indexing CSAM files, allowing data in different systems to be cross-referenced and for police and partners to complete automated searches of devices, databases and websites. In the UK, the Home Office has taken a coordinating role in pooling police intelligence into the national Child Abuse Image Database (CAID) which by 2019 contained 8.3 million unique indecent images of children,[63] and is used by all UK law enforcement to search for and categorise CSAM.

Data processing has become the essence of investigation for online CSA and the free-flow of intelligence data between agencies is necessary to quickly identify investigative and safeguarding opportunities. The ability to quickly cross-reference new with existing data helps to generate intelligence and increase the scope for police to become more proactive in their investigations. To illustrate, new CSAM may be discovered during a search at a local offender's address which depicts other undiscovered offenders who might be identified when cross-referenced with the data from CSAM on CAID. Information continuously emerges across different parts of the police network, and it needs to be pooled and refined in order to generate new intelligence and drive a more proactive response.

> *"… at the moment, people use our tools in a very reactive way, we've got this case and we will try to solve it … it doesn't require a man to search for [these links], it should just happen … I'm a hundred per cent sure that we are sat on data that would solve crimes, [data] that is not being used."*
>
> **(Private sector representative)**

Additionally, many images are duplicates that have been previously discovered and categorised in prior investigations, therefore cross-referencing with data in a database automates the processes of search and examination, expediting investigations and reducing the need to expose officers to harmful CSAM. Slower processes lead to fewer cases investigated:

> *"We need to be one step ahead … we need the right bloomin' networked computers. I just don't think we have the technological capability full-stop, to do things expeditiously."*
>
> **(NCA – Specialist investigator)**

The seamless exchange of information requires IT systems and networks with sufficient cohesion and the cracks are beginning to show in the current fragmented and rigid police infrastructure for adopting new technology. One police force described internal systems that held relevant data in silos and in addition, instead of real-time access to the national database (CAID), they received information through periodic updates shared by hard copy. Further, there are inconsistencies in the technological capabilities in different police force jurisdictions and real challenges for companies in the private sector to effectively interface with the many-headed governance structures in the police, especially when trying to introduce new products. The Home Office has taken some of the lead in determining a standard and procuring new technologies, for example through its accelerated capabilities environment, but there is no equivalent at the user end (i.e. the police).

> *"The CAID system in our force is antiquated, not plumbed in properly … which means our staff are being over-exposed to images they wouldn't need to see."*
>
> **(Local police force – specialist online CSA investigation)**

> *"Why is it that one force chooses to [use offender monitoring software] a bit, and another force doesn't use it at all? … [the company] stopped doing it because there wasn't the magnitude of interest."*
>
> **(Support services – specialist practitioner)**

On the frontline there is a gap between what practitioners recognise is needed and what is currently in place. Technology has the potential to create a more effective and efficient service by drawing useable intelligence from large volumes of data to identify, prioritise and target resources to the most serious and high-risk cases. Particular examples include software

63. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/childsexualabuseappendixtables

to identify and examine suspect devices (including remote storage accounts) at the crime scene or in forensic labs, to automate the process of categorising images, to cross-reference and draw links between data (for example linking images of the same victim through image recognition software), and to analyse and risk assess CSAM and online communications. The introduction of technology to bring more digital forensic capability to frontline practitioners represents a considerable step for streamlining processes of investigation.

> *"Digital forensic triage examinations at the scene of suspects has been ongoing in [our police force] for nearly one year. This allows police to ascertain the likely guilt of a suspect at the time of arrest and allow an effective risk assessment of that suspect once dealt with in police custody."*
>
> **(Local police force – specialist online CSA investigation)**

Some barriers arise from legacy IT systems that lack the processing power to manage the growing volumes of data, but also data protection concerns that create an understandable resistance to adopting more efficient networked systems that are considered more susceptible to a data breach. The absence of the right technology to analyse the data, and the staff with the requisite skills to apply it, stalls the processes of law enforcement and increases the likelihood that offending and victims are missed.

> *"The ability to triage/examine devices at scenes in an evidential format is in need for immediate improvement. Offenders are identified and action taken at an early stage and then there is a delay of months to years before the offender is convicted. If an evidential product was capable of being obtained on the day of arrest, then the suspect could be charged and in the court process in a matter of weeks. Equipment and training are required, this will require mass funding, due to the technology required and specialist training required."*
>
> **(Local police force – specialist online CSA investigation)**

> *'[To identify a suspect's connection to other offenders] unless you look for them, you don't really see them … there's only so far you can go to get through that volume of content … definitely no, we do not have the capacity and capability to deal with the volume and complexity of what's going on.'*
>
> **(NCA – Specialist investigator)**

The reality is that the current investment is grafted to the response as it is, one that has become overwhelmingly reactive due to the mounting pressures placed on investigation units to deal with the high volume of CSAM referrals and local safeguarding concerns. To illustrate, one force had developed a tool to automate the process of cleaning data from chat logs to identify potential victims or children at risk, reducing a process that could take weeks to a matter of minutes, but uptake from other forces was limited because of the pressure to sustain a reactive response to the high volume of CSAM referrals from the NCA:

> *"they're trying to keep their heads above water, just to get through the work they [already] have on."*
>
> **(Local police force – specialist online CSA investigation)**

Recommendation 8

Over the next decade the government should increase investment in the information technology required to keep pace with the changing threat of online child sexual abuse.

The challenge of moving from reactive to proactive investigation

The police response to online CSA, as with most other areas of crime, suffers from managing high volumes of incoming reports, which means that too much resource is dedicated to what is known as opposed to where most of the harm is. As one practitioner told us:

> *"My problem is volume. There may well be five people in the UK using VPN [or other technology] and they're really hiding their tracks, whereas at the same time I've got 300 people [to process and] I haven't got time … You've either got to do volume or you do complex criminality."*
>
> **(Local police force – specialist online CSA investigation)**

Many local online CSA investigators described a wide gap between the mission to protect children from harm and their experience, with only a small minority of CSAM investigations leading to offenders engaged in more serious sexual abuse or complex criminality and relatively few leading to the identification of other victims (such as those in "first-generation" CSAM). This is illustrated in the following comments from three separate police forces:

> *"We're dealing with the numpties who are getting caught, whereas the real high-risk offenders are operating on the dark web … the offenders dealt with by the NCA."*
>
> **(Local police force – specialist online CSA investigation)**

"We will talk about how many devices we will look at, we're looking for live abuse and don't find as much of it … we're really good at supporting victims but we don't identify many."

(Local police force – specialist online CSA investigation)

"[In] relying on an approach of just doing warrants until you find [the most serious offenders] is like going fishing with a golfclub."

(Local police force – specialist online CSA investigation)

Policies and protocols for law enforcement in the UK have set low risk thresholds, with an enforcement or safeguarding response much more readily levered than in some other jurisdictions; for example, practitioners stated police in Australia do not accept referrals of some lower category images and in the Netherlands, the police have more discretion to divert lower risk individuals for alternative intervention. These illustrate variable policies and protocols in response to risk. A consequence of the UK approach is that in addition to the burgeoning volume of crimes being identified, the police are left to address risk almost without limits, creating the demand for a response that is unsustainable and potentially failing to achieve the stated objectives of risk management (i.e. identifying and protecting children at risk of abuse). In seeking to address ever-present but invisible risk, the police have no choice but to deal with everything, limiting the scope to proactively seek out the "worst people".

Recommendation 9

The National Police Chiefs' Council and the National Crime Agency should review their approach to risk and proportionality in relation to CSAM offences. The aim should be to protect more children from harm by dedicating more investigative resource at proactively identifying serious offenders, in particular those involved in grooming and possessing first generation material.

Instead of just focusing on the reactive response to CSAM, there is widespread agreement that there should be a greater focus on proactive investigation of online CSA. The objectives of proactive investigations are to:

- *Investigate serious offenders*: the collection of intelligence can lead to the identification of offenders who cause or present the greatest risk of harm and/or adopt the most sophisticated methods to evade detection. It allows the police to direct criminal justice resources to the most persistent and harmful offenders.
- *Disrupt online offending*: the production and distribution of CSAM is facilitated by online websites that function within expansive online networks of people and communities that serve to proliferate CSAM. Targeting "upstream" suppliers and/or their connectivity to other offenders or communities brings the prospect of breaking distribution chains and reducing the capacity of others in the network to offend. Furthermore, effective law enforcement can impact on offenders' confidence in the technology and networks to protect them, increase the perceived risks and in this way deter offending. This includes reducing the number of co-offenders that engage with illicit networks.
- *Safeguard children*: the police work to an overarching harm reduction agenda that prioritises the protection of children from abuse. Many serious crimes go undetected, including the most severe CSAM often in concealed spaces such as the dark web, and collecting the intelligence can lead to the identification and protection of otherwise hidden victims. Similarly, monitoring online communications enables investigators to identify the preparatory acts or commission of abuse in real-time and stopping this abuse is core to the police mission.

However, there are a number of challenges that need to be addressed if we are to shift the effort in a more proactive direction.

First, law enforcement needs to be clear about what is meant by "serious offending". Practitioners explained to us that there can be a conflation between seriousness and complexity, when in reality the two are not necessarily linked. Most specialist resource in the NCA, in ROCUs and in the larger forces is targeted to pursue the offenders who cover their tracks, operating on the dark net and so on. And yet both the research evidence and our practitioner interviews indicate that the majority of contact abuse that crosses over into online offending is derived from criminal opportunities in offline settings (most commonly intra-familial), and so less rooted in elements such as complex co-offending structures or technical capability. Two NCA investigators stressed that the highest risk offenders were those on the web seeking to make contact with children, not necessarily the offenders and communities on the dark web.

"… there's a danger of people getting confused about what is high risk and what is hard-to-catch."

(NCA – Specialist investigator)

"It shouldn't be about how technically capable your suspect is, it should be about the damage they're doing."

(Overseas law enforcement – specialist practitioner)

Second, safeguarding is not always compatible with proactive investigation aimed at the hard-core groups at the centre of these criminal networks. This is because no law enforcement outcome such as detection or disruption of an online criminal network, can come at the expense of a child not safeguarded from contact abuse.

"[If we identify the threat of contact abuse] the investigation is blown out of the water, you'd have to go and safeguard that child … most other crimes don't have that same pressure and that does alter decision-making and reduces the time you can investigate because [you] can't risk a child getting harmed by that person."

(NCA – Specialist investigator)

Third, there is a need to ramp up investment in the digital investigative capability that is essential to undertaking proactive work. The police effort to suppress criminal networks is contingent on keeping pace with the evolving methods and counter-measures of perpetrators. The most sophisticated offenders monitor law enforcement activity and tactics, and online communities provide a platform to share methods to bypass the tactics in use by the police. One example was the increased vigilance in some communities to malware which the police had deployed as a "technical hack" to reveal the identity of users (Broadhurst, 2019). Other communities operate to stringent protocols mandating a user to perpetrate and evidence their sex crime to verify their intentions and mitigate the risk of infiltration. Some choose to operate from spaces that are simply out of sight and inaccessible to third parties, such as encrypted communication apps or file-lockers.

"They can make their way up [in terms of privileges] … to get into some sites, you have to produce your own abuse image. They did that I think, so no law enforcement could get in."

(NCA – Specialist investigator)

Some of the most harmful crimes require offenders to operate in open spaces, most notably to meet and sexually exploit children. Undercover investigations to detect grooming offenders require officers to credibly imitate the online profile of a child, a task that grows increasingly difficult as the digital footprint of children grows, with 24/7 access to internet-enabled devices and continuous posting of new files and messages on an array of platforms and apps (Martellozzo, 2015). The growing complexity of the task of operating in a context in which modus operandi, technology and social trends are subject to continuous change, threatens to erode the efficacy of proactive police tactics if they are slow to adapt.

The NCA, ROCUs and some larger local police forces deploy specialist investigators to patrol or operate undercover on social networking sites, chat rooms, forums and other communication platforms on the open and dark web. As with all proactive work, coverage is severely challenged, with officers policing spaces and people that span not just national but global jurisdictions, and added to this, investigators struggle to meaningfully direct their attentions to online spaces or accounts that present the greatest risks. The internet is not only sprawling but ever-changing with new platforms, apps and technology being introduced all the time and young people who continuously migrate to new spaces as global and local trends change.

"We get a threat assessment that's yearly, but it can change so quickly and most cops are of an age that we don't use the internet like that, how can I know what platforms are out there? … partner (organisations) are really well-suited to get this information, we're behind, on the back foot of what's current."

(ROCU specialist online CSA investigation)

"… understanding the nuance [is important] and being able to keep pace against the backdrop of a continuously evolving digital environment."

(Private sector representative)

Fourth, there are resource constraints and engaging in proactive work can both take officers away from dealing with cases that have been brought to their attention and can lead to new demands the resourcing implications of which are not predictable in advance.

"The ROCU is the source of local [undercover investigation] resources but they do not solely operate in our force area. If they increased their [investigative] capacity we would need more specialist investigation resource to manage the increased demand."

(Local police force – specialist online CSA investigation)

"I guarantee there will be links between the offenders. But machines will only take you so far … we would have to do something about that … We can't be held to account for the things we don't know, as soon as I've found that kid and nothing's been done, that's on me … If you go around lifting stones you've got to do something about it."

(NCA – Specialist practitioner)

The result is that police resources are not really configured to risk, but rather to known offending. To

Box 3.3 Proactive forms of investigation: network disruption

As an alternative to costly and protracted criminal investigation, the police can deploy interventions that are aimed to disrupt routines, lifestyles and networks in order to make it more difficult to perpetrate crimes, commonly in partnership with public or private sector organisations (Kirby and Penna, 2010).[64]

Undercover work deployed against serious and organised criminality in this space is focused on targeting organised criminal networks producing and distributing CSAM, by entering virtual chat rooms, joining communities, and setting up fake websites that purport to contain CSAM (UNODC, 2015).

There are ethical considerations to be made about engaging in authorised criminality (such as uploading CSAM) to develop the trust needed to infiltrate the criminal networks, using tactics and activity that need to remain secret to be effective. There are also the resultant gaps in scrutiny, not to mention the psychological toll on officers exposed to the highly distressing CSAM shared in these hidden communities (Vendius, 2015).

A number of well-publicised operations by US and Australian law enforcement involved taking over and operating the CSAM sites in order to identify suspects and children at risk, but these drew some controversy because the time required to collect the intelligence meant perpetuating these crimes and, in the process, revictimising the children depicted in the CSAM (Broadhurst, 2019). The imperative to safeguard children is not always compatible with the practical need to develop intelligence and investigate perpetrators.

The effectiveness of disruptive activity in tacking online networks is challenged by their intrinsic capacity to expand, shrink and reconfigure themselves (Martellozzo, 2015). The approaches to proactive disruption include:

- Surveillance: Specialist tools can be used to tap into and monitor publicly accessible activity on P2P file-exchange networks, a process that is analogous to police "walking their beat". To identify criminality, which in this context relates to tracing files and file exchanges that are known or suspected of being CSAM (Liberatore et al, 2010).
- Damage trust: Disruption may also involve compromising the trust and relationships between members of the network in order to break down cohesion and reduce their capacity to offend (Afilipoaie and Shortis, 2018; Soudijn and Zegers, 2012). Previous operations have also sought to establish fake websites to identify offenders seeking CSAM (Gillespie, 2008). These help to identify and investigate offenders and more broadly, can serve to disrupt offending by undermining people's confidence in the security of these networks.
- Disrupt connectivity: The transformative effect of online networks for distributing information means it has become very easy to click through the hyperlinks that connect to a multitude of sites providing access to CSAM. Some suggest it is the networks themselves, and the abundant criminal opportunities they afford which should inform disruptive intervention, focusing not just on specific sites of interest in isolation, but also accounting for sites (and linked offenders) which are most problematic in the context of the network (Joffres et al, 2011; Westlake and Frank, 2016). Software (i.e. webcrawlers) can be used to automate the detection of offending sites (using hash values and key words) and chart the linkages between them, to map out the network and assess the significance of individual sites in the "massive distribution chain" for CSAM (Joffres et al, 2011; Westlake and Frank, 2016). This highlights which sites are the "key players" that are most relied upon to either maintain connectivity and cohesion across networks or specific sites with the greatest volume of CSAM, with a view to targeting disruption to reduce the accessibility of CSAM.

The principles of disruption are in part transposed from social network analysis techniques to map out individuals, their functions and relationships, and focus intervention on those others in the network relied on to commit crime (Joffres et al, 2011). In a similar vein to the offline realm, the capacity for continual change in increasingly decentralised criminal markets and networks, requires the police to understand the short and long-term consequences of disruptive intervention (both intended and unintended), including effectiveness, displacement and any adverse effects (for example, see Innes and Sheptycki, 2004).

64. Disruption is an intelligence-led approach to enforcement that has links to situational prevention methods and is commonly targeted to inhibit offending of individuals suspected of involvement in serious and organised crime (Kirby and Penna, 2010).

illustrate, the police have considerable capabilities to patrol P2P networks and discover CSAM offending that is otherwise unknown, but there is widespread reluctance across police forces to use this capability. In interviews, some officers said that their forces had chosen not to adopt this proactive method and in others it was only used if they had spare capacity, depending on the scale of demand from known offending (i.e. crimes reported by industry). In essence, the police feel more able to make difficult prioritisation decisions about crimes and victims that have yet to be discovered.

In our survey some strategic leads expressed concerns over the amount of resources available to specialist teams in order to effectively tackle the demand from CSAM suspects; over half (17, or 52 per cent) considered they had insufficient resources. Often this is reflective of the high volume of demand that is continuously being referred by NCMEC. However, more respondents highlighted insufficient resources in local police teams (23 or 72 per cent) and half (19 or 52 per cent) cited a lack of resource in local investigation teams.

Box 3.4 Proactive forms of investigation: identifying groomers

The UK was one of the first countries to create the offence of sexual grooming and in doing so, criminalised the "preparatory" behaviours for committing sexual abuse crimes (Gillespie, 2004; Vendius, 2015). The subjective intention to groom and exploit a child is the main factor in legal decision-making, not whether the case involved a real child (i.e. a tangible victim). This grants considerable flexibility to the police to proactively tackle online CSA, including the ability for officers to work undercover in online spaces. This tactic takes one of two principal forms; taking over the account of a child who has reported grooming by an offender that has suggested they physically meet or going undercover to operate fictional online accounts to pose as a child to create the opportunity for prospective offenders to commit crime. (Sorell, 2017).

One of the main benefits in targeting online grooming is the prospect to pre-empt and prevent serious sex crimes such as rape or sexual assault (Craven et al, 2007; Sorell, 2017). However, robust identification of individuals with these intentions is a challenge, firstly because of inherent under-reporting by victims who are being groomed, and secondly, the challenge for undercover investigators in interpreting a suspect's intentions from their online communication and behaviour. Online offenders are diverse in their motivations and many are sexual fantasists with no real intentions of enacting the ideas they communicate (Taylor and Quayle, 2003). Undercover investigations are regulated by the Regulation of Investigatory Powers Act (2000) with controls to ensure an agent does not incite offending that would not otherwise have been perpetrated (i.e. legal entrapment).

In targeting finite resources, the police must try to focus their efforts on the highest risk suspects among the many who seem prepared to engage in sexual communications with young people, with high priority accorded to those who seek to arrange a physical meeting with the fictitious child.

> *"Anyone can say anything online [and a challenge] in trying to decipher who's the real risk, a lot of people are fantasists."*
>
> **(NCA – Specialist practitioner)**

> *"It's like shooting fish in a barrel, there's so many of them … you wouldn't have to be on a platform very long before you see some of this taking place … [if there are children you can communicate with on a forum] you can guarantee offending is taking place."*
>
> **(NCA – Specialist practitioner)**

Interviewees described challenges in completing robust assessments of anonymous offenders known only through their digital account, with very few contextual details to determine their risk other than the social cues from the online interaction. This requires considerable skill, time and prioritisation is reduced to two categories; the blue-light cases where there is an imminent safeguarding risk to an identified child and "the rest". In one area law enforcement had invested in linguistics research with the aim of developing tools to automate assessment of online communications, to help them move away from the "volume" and to focus their attention on the most serious offenders motivated to perpetrate contact abuse.

> *"… we're blind to most of the stuff they're doing … they might be talking to 900 other people, at the point of engagement, [our assessment] is basically about what they're saying."*
>
> **(ROCU specialist online CSA investigation)**

Preventing suspect self-harm and providing support for the families of suspects

Many CSAM suspects have had little or no prior contact with the police, having led otherwise law-abiding lives that can include a regular family life. The sudden arrival of law enforcement can have considerable consequences for the health and welfare of suspects. To illustrate, nearly a quarter of all online CSA offenders identified in one police force were flagged by police to have experienced mental or physical health difficulties (23 per cent) and 15 per cent as at risk of suicide.[65] Nationally, there were 250 suspect deaths recorded as the outcome for CSAM investigations in 2014-18, 0.5 per cent of all recorded outcomes during this period. While the reason for these deaths is not recorded, to provide some context, for offenders of all crimes in 2014-15 there was a total of 67 "apparent suicides" following police custody, a quarter of whom (17) had been arrested for an indecent image offence.[66]

Some practitioners were keenly aware of the risks, with one from a large urban force estimating that there were at least two suicide attempts each month. At the time of the survey, the NCA had recently begun to collate statistics on suicides from each police force, though different police forces varied in their approach to collating these figures; some had no specific processes to account for suicides among online CSA suspects, and others maintained a separate database to monitor these outcomes.

An arrest can also have a significant impact on the suspects' own family, most of whom will have been unaware of their offending.

> *"… because also we turn [the family's] lives upside down when we come banging through the door."*
>
> **(NCA – Specialist investigator)**

In addition to the confusion and uncertainty, the unexpected arrest of a parent has the potential to cause trauma to the suspects' children. And regardless of the eventual criminal justice verdict, a public outing threatens to permanently tarnish suspects' and their family's standing and relationships in the community. For these reasons, the specialist investigation teams gauge the success of an executed warrant by their ability to "get in and get out … and [to] be as sensitive as possible". This includes conducting the arrest without uniform and in unmarked cars and making a discreet entrance into the property to avoid raising the awareness in the wider community.

The initial period of detention provides police with the opportunity to assess the risk and support needs of a suspect during what was described as the initial 48-hour 'flashpoint' period. There is systematic assessment, monitoring and support from officers and health professionals working in custody, through the process of arrest, police interview and detention in custody. However, many suspects will be quickly released back into the community under investigation which can leave them in a "suspended state of limbo" for several years. The comprehensiveness of support varied by police force, ranging from a signpost to the national support helpline, to more extended support provision once the suspect was released back into the community.

The primary enforcement role of the police places limits on their effectiveness to support suspects, therefore third-party organisations fill an important gap. The Lucy Faithfull Foundation is a specialist national helpline that is signposted for all CSAM suspects, though has a cost implication for the suspect which may mean that not all can access this service. In our survey, individual police forces variously referenced additional organisations that included local statutory support services such as social services or youth offending teams, GPs and other helplines such as the Samaritans and local charities.

> *"Provision of Lucy Faithfull Foundation details to suspects along with details of other organisations that may assist the suspect should they feel anxiety. A 'pathway' is being developed in unison with the criminal justice liaison mental health team to support offenders through the investigation and judicial process. Periodic contact from the officer … with the suspect, to enquire over welfare matters and update on the progress of investigations."*
>
> **(Local police force – online CSA strategic lead)**

For children deemed to be at risk of abuse by the offender they will be referred to the local children's services, but otherwise the availability of support for the partners and children of suspects was patchy. In many areas the support was limited to an exchange with the police at the point of arrest. Families may have questions pertaining to the nature of the offence, the risks the suspect poses to them and others, the criminal justice processes and may themselves require emotional or practical support. One police force, in partnership with the Lucy Faithfull Foundation, had created materials to provide relevant information for families and to signpost available support services.

65. A high proportion (86, 86%) of those flagged with a suicide risk were also recorded as having experienced physical or mental health issues.

66. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655203/deaths-in-police-custody-review-international-evidence-horr95-tables.ods

"Support for families of offenders is not something that [we] currently provide beyond brief advice offered at point of contact with families, usually at initial arrest stage."

(Local police force – online CSA strategic lead)

"[We] have recently designed a 'Family Pack' for partners of [CSAM] offenders which provides information on what has happened and signposts to services that may be able to support them."

(ROCU specialist online CSA practitioner)

Recommendation 10

We recommend that police forces collate robust statistics on suicides and attempted suicides linked to CSAM suspects and national statistics should be published annually by the National Police Chiefs' Council. Appropriate support services should be engaged to minimise the risk of suicide among this group.

Recommendation 11

The National Police Chiefs' Council should commission research to understand the gaps in emotional support for families affected by the arrest of an online CSA suspect. This should provide the basis for greater support for these family members.

Online vigilantism

Vigilantism encompasses a spectrum of activity, ranging from a lone individual engaging in a single enforcement act, to more organised, group-based activity that is sustained over time. Theories to explain the emergence of vigilantism across different contexts describe collective mobilisation following an emotive reaction to a crime or behaviour that poses an acute threat to the core values, standards or identity shared by a community, accompanied by a lack of confidence that criminal justice will provide the desired response (Asif and Weenink, 2019; Silke, 2001). In addition, strong identification with the victim(s) is suggested to be an important driver of vigilante activity. Child sexual abuse is one of the most reviled crimes across the world and has in the past sparked various outbreaks of vigilante violence, sometimes involving aggressive protests from morally outraged parents following a sex crime in the community (Silke, 2001).

It has become commonplace for users individually or collectively to take an active role in governing the behaviour of others to maintain order in online communities (Wall and Williams, 2007). This behaviour can take the form of "digital vigilantism" in which users and groups engage in collective action to tackle all manner of social or legal infringements that cause offence or moral outrage (Trottier, 2015).

A widespread moral consensus on online sex grooming and abuse has fostered a vehement collective response, with the emergence of multiple online vigilante groups taking up arms to tackle online child abuse, often with the support of many online followers. These groups impersonate a child or young person to engage and "bait" individuals online who seek sexual activity with a child or young person.

The motivations and methods of the different groups are diverse, with some who restrict their actions to information gathering and making referrals to the police (adopting more closely the role of activist), and others with the primary motivation to mete out their own form of punishment. This commonly takes the form of public exposure online or by arranging to meet in-person and engaging in a public confrontation that is broadcast over social media; violence can ensue but punishment is primarily centred on this extreme form of "privacy violation" in which an individual is exposed and publicly branded with the highly stigmatised label of "paedophile" (Trottier, 2015). In some cases, this action changes in an instant that person's standing within their personal relationships and community.

The opportunities and challenges presented by online vigilantism

Unlike many conventional forms of vigilantism, these online "stings" are legal so long as groups do not engage in accompanying criminal behaviours such as violence, threats or harassment. And the criminalisation of preparatory behaviours like grooming has increased the scope for members of civil society to play an active role in identifying and detecting online criminals. In targeting otherwise hidden crimes, referrals from these groups make up a substantial proportion of the crime recorded by the police. In 2017, 29 police forces reported 150 online grooming suspects had been charged following identification and referral by a vigilante group, and nearly half (47 per cent) of charges for meeting a child following sexual grooming had used evidence provided by these groups.[67]

In dealing with these proliferating but hidden crimes that outstrip the police capacity to respond, multiple practitioners recognised the value in vigilantes unearthing serious criminals they might not otherwise

67. https://www.bbc.co.uk/news/uk-england-43634585

reach. Several highlighted incidents in which a suspect was brought to their attention who transpired to have sexually abused local children.

> *"There are benefits [to vigilante groups], mainly the volume of offenders willing to engage in sexual online chat and meet a child after is massive, and beyond the scope and capacity of the proactive police teams to identify all and investigate."*
>
> **(Local police force – online CSA strategic lead)**

This scale of public activism might be viewed as a positive example of citizenship in which individuals in the community are taking responsibility for protecting children and preventing crime. There are multiple contexts in which the public are encouraged to actively participate and support the police efforts to identify risks and prevent crime in communities. Notable examples are Neighbourhood Watch and Crimestoppers. However, in these contexts enforcement and punishment are implemented at the discretion of police, which is not the case for much of online vigilantism:

> *"There would be benefits if the OCAGs [online child abuse activist group] referred their information as intelligence to the police for assessment and development without taking action. It is the action and live streaming which undermines what they are out to achieve."*
>
> *"It's fraught with danger. I get why they're doing it and they're very good sometimes in what they do. Evidentially it's a nightmare and they sometimes go and meet them without telling us, they don't think about the destruction of the evidence and sometimes just go there to beat them up."*
>
> **(NCA – Specialist investigator)**

There are three areas where online vigilante groups pose a challenge for law enforcement.

First, they can make it difficult to secure a criminal justice outcome. These groups play an active role in establishing the context and criminal opportunity during the online exchange, opportunities that might otherwise never have arisen, and so there can be a thin line between drawing out a motivated sex offender and creating one. The techniques mimic those employed by covert policing, but operate without training or knowledge of legal protocols, so often provide evidence that is inadmissible in a court due to the use of strategies that amount to entrapment.

Moreover, following the initial referral to the police many groups do not engage further in the formal criminal justice process; for example, refusing to give statements or hand over their devices or other digital evidence. This leaves a fragmented evidential-trail that is difficult and resource-intensive for the police to piece together and can ultimately preclude prosecution.

> *"In my experience [online vigilante groups] have little, if any, experience or knowledge of evidential requirements – they regularly refuse to provide supporting evidence and understandably this leads to CPS declining charges."*
>
> **(Local police force – online CSA strategic lead)**
>
> *"On the whole, they offer poor evidential continuity, and are often not transparent in how the initial engagement with a suspect occurred. Decoys often disengage quickly after a 'sting' and become reluctant or unwilling to fill evidential gaps identified by police or CPS."*
>
> **(Local police force – online CSA strategic lead)**

The disengagement of groups during formal investigation indicates that for many of these groups a criminal justice outcome is secondary to meting out their own form of punishment. This informal enforcement is imposed without an audit trail, which puts them outside of any accountability structures and subverts the fundamental principles of due process and fair treatment in the criminal justice system. Furthermore, these interventions are targeted based on hidden (and potentially dubious) personal agendas, instead of one oriented to public service or public good.

> *"They like the celebrity of it … if we said 'come on then, be a volunteer or a special', they wouldn't be interested in it because they wouldn't be getting the support from the public … they don't do anything without posting it on Facebook."*
>
> **(ROCU specialist online CSA practitioner)**

Second, these groups are not targeting offenders based on proper risk assessment and so their activity can distort the work of the police. The police target their resources primarily to safeguarding need, and so direct investigations to online offenders who present the greatest risk to a real child. The activities of vigilante groups are (understandably) not bound by the same logic and are relatively arbitrary in how they are targeted, with a principle focus to punish anyone who displays a willingness to engage. The intrinsic risk and seriousness of an individual who displays a sexual interest in children compels the police to respond, however in many cases the police investigation does not reveal involvement in other forms of abuse. Some practitioners considered that referrals from these groups diverted police resources away from the highest risk offenders and children in need of safeguarding.

"The majority of persons identified by [vigilante groups], albeit there are notable exceptions, are not found to otherwise have a sexual interest in children following investigation. The incidents cause community tension, investigative difficulty and are a distraction from the rising demand of other more significant sources of online CSE [child sexual exploitation] demand."

(Local police force – online CSA strategic lead)

Finally, these groups can cause all sorts of harms that the police then have to manage. The indiscriminate approach of many groups commonly ensnares the less vigilant, some of whom are considered themselves vulnerable, with multiple practitioners describing a pattern of referrals with learning disabilities or other mental health difficulties. Furthermore, practitioners described a margin of error in which vigilante groups can identify and confront the wrong person. This long tail of collateral damage to suspects, their families, communities or the wrongly accused, needs to be managed by police, increasing demand for safeguarding (for example, the provision of safe houses), public reassurance and law enforcement in the event there are crimes perpetrated by the group or other community members.

"… the propensity for [vigilantes] to 'expose' suspected perpetrators on social media platforms presents the police with significant safeguarding challenges in respect of that perpetrator and their family. This invariably places further demand on resources … [and] the risk of self-harm among perpetrators is naturally increased when their image or identity is publicly exposed."

(Local police force – online CSA strategic lead)

"They seem like they're doing the right things [but] they have the suspect very exposed and we're left to pick up the pieces for safeguarding that person."

(Local police force – specialist online CSA investigation)

Responding to online vigilante groups

The government and law enforcement need to strike a balance, with any display of support serving to empower and legitimise these groups while undermining their own position and authority. However, outright opposition risks denting the confidence and support of many in the public who are supportive of these groups, something that strained law enforcement agencies cannot afford to lose.

"Public support for these groups is significant and police cannot afford to be seen as protecting perpetrators. This is a challenging balance to strike."

(Local police force – online CSA strategic lead)

The first responders to these incidents are commonly frontline investigators or uniformed officers, often falling outside of the remit of specialist teams, and most operate to principles in the national guidance produced by the NPCC; broadly to provide a response to their reports but otherwise to not actively engage or endorse online vigilante groups.

"The safeguarding of children and young people is a priority for [the police force] and the PCC … [and] to date [we] have always responded positively to information provided by members of the public including [vigilante groups] and that will not change. The activity of [the groups] will always be at their own discretion and we do not task nor [share] intelligence with [these groups]."

(Local police force – online CSA strategic lead)

These principles help maintain a status quo, but do not deal with the challenges nor embrace the opportunities these groups may offer, and there may be scope to harness this activity by trying to channel it into more collaborative and constructive intervention.

"There may be benefits in extending our reach by developing relationships with [vigilante groups] as we need to consider opportunities to move with the times in relation to Police Service Volunteers and extending the skills and capabilities of Special Constables into more diverse and specialist areas of policing. The challenges, however, are the current lack of regulation, capacity to manage volunteers in this way and the capacity of existing investigation teams to manage an inevitable increase in demand."

(Local police force – online CSA strategic lead)

Recommendation 12

We recommend that the police continue to use evidence produced by online citizen groups where appropriate but that they should also make available structured guidance for those who wish to work lawfully and cooperatively, to limit the potential for harm.

Configuring law enforcement systems to risk and harm

This section has shown that CSAM offending creates a high volume of demand on law enforcement resources. In part, this reflects systems that take a uniform approach to managing all local suspects and relatedly, the challenges in identifying which cases represent the greatest risk of contact abuse. Added to that, there is a high volume of offenders causing considerable harm within online spaces, such as sexual communications offences, online exploitation and the proliferation of CSAM. Investigations of these online crimes commonly span UK and global jurisdictions and involve some of the most technically sophisticated offenders but can fall through the cracks of law enforcement that is (understandably) preoccupied with cases that present the greatest risk of contact abuse. These two challenges to the current system will now be discussed in turn.

Managing CSAM Offenders

In managing CSAM offenders, risk is central to the law enforcement discourse. Consequently, the demand on policing is only partially reflective of tangible crime, much of which (in relative terms) is low harm, and to some extent is manufactured through processes of risk assessment. In this way, the scale of demand on law enforcement is the product of risk tolerance (which in the UK is comparatively low) as represented in assessments for interpreting crime and intelligence data (e.g. KIRAT).

Criminal investigation is an essential component to identifying and addressing serious sex offending and safeguarding victims and children at risk, though many investigations do not reveal additional offending. Regardless, a second objective is risk management in all cases, to prevent offenders from repeat offending or progressing to more serious crime. There are questions over the alignment of current criminal justice systems to the task of managing low harm CSAM cases.

- First, many convicted offenders do not receive a custodial sentence so remain in the community.
- Second, there are challenges in resourcing and practically implementing active offender management for low risk CSAM offenders (see Chapter 5).
- Third, there is considerable reliance on offenders' voluntary engagement with support services to address unhealthy attitudes or behaviours (see prevention chapter).
- Fourth, the evidence indicates that many CSAM offenders follow a distinctive pathway that does not lead to more serious sex crimes, and further, the shock of being subject to a criminal justice intervention is for many a sharp deterrent from further offending. Studies show low recidivism rates for CSAM offenders with no prior convictions, with 2 per cent subsequently convicted of a contact sexual offence and 5 per cent an internet-based offence (Seto and Eke, 2015). This is supported by a recent UK-based study which found 2.7 per cent of convicted CSAM offenders committed a subsequent contact abuse offence (Elliott et al, 2019).

It is clear that these risks need to be addressed but greater gains and efficiencies might come from an increased emphasis on education, support and health interventions for the purpose of risk management. In this regard we endorse the recommendations of Justice (2019) which proposed a "conditional diversion" scheme in which low risk offenders (i.e. CSAM-only offenders with no relevant offence history) are diverted from the criminal justice system to a "psychoeducational programme". The key outcomes of the scheme are to:

- Clarify and make consistent what is in reality, already a community-based response to CSAM offenders.
- Focus the attentions of criminal investigation teams on the identification of serious offenders.
- Reduce the risk of reoffending by capitalising on a 'teachable moment' following arrest (Justice, 2019).
- The potential to reduce the high risk of suicide among this group of offenders (see 'Preventing suspect self-harm' above (page 58)).

Recommendation 13

A criminal investigation remains essential in each CSAM case to identify those in which there is a risk of more serious sexual abuse. Where none is discovered however the police should be able to issue a conditional caution with the following provisions:

- As a minimum, the offenders should be mandated to attend an educational course at their own expense. The course would communicate the harms from these crimes, address criminogenic attitudes, give information on the law and signpost additional services if needed.
- Compliance to these conditions would be monitored and criminal sanctions imposed in the event of a breach.
- Appropriate safeguarding controls should be in place. Each offender would remain on police systems to monitor and assess their risk in the community, and their participation in the scheme could be revealed via enhanced Disclosure and Barring Service (DBS) checks so that they could never work in a role involving contact with children.

This scheme should be trialled in the first instance and would be subject to a full evaluation.

Tackling online offending

Online offending such as sexual communications, exploitation and image-sharing are perpetrated in increasing volumes and can cause high harm to victims or through the proliferation of CSAM. A key challenge lies in identifying online offenders that are the most serious. Most protocols assess the risk of contact sexual abuse and much less has been done to index and compare the harms of online offending (for example, the use of threats or blackmail to coerce victims or involvement in establishing image-sharing communities). The lack of knowledge, tools and techniques to assess online harms mean it is difficult to meaningfully target resources at the right cases. Furthermore, there is currently no law enforcement unit that has the specific remit to address serious *online* offending.

Specialist investigation units in the NCA, ROCUs and a small number of police forces are tasked with investigating serious sexual abuse. However, their remit is differentiated from local teams more by the complexity of the investigatory processes rather than the seriousness of the crime (for example, capabilities to undertake online surveillance or collaborate with international law enforcement), because they share the same overriding agenda with local teams which is to disrupt contact sexual abuse. This has created a gap in law enforcement activity to target the most serious *online* offending.

There are intrinsic barriers to investigating cybercrime that are exacerbated by the capability deficit across the workforce, but especially among generalist officers who currently have responsibility for responding to local victims of online abuse. A consequence is that local officers commonly emphasise other forms of intervention such as protective advice over criminal investigation. There is also much online offending that is not reported but in the absence of the risk of contact abuse, fall short of thresholds for proactive investigation. More is needed to pursue and disrupt the most serious online CSA offending, to increase the rate of detection and deter offending that is currently perpetrated in high volumes.

Recommendation 14

The National Crime Agency and the National Police Chiefs' Council should jointly develop a more robust framework for understanding online harm, including for example an index which could guide practitioners to focus on the highest risk online offenders.

Recommendation 15

The National Crime Agency should establish a new specialist investigation team, that operates in parallel with existing units, but with a specific remit to target, investigate and disrupt offenders who are causing the most serious online harm. The remit of this team would be to investigate online abuse or exploitation reported by victims in the UK, and also cases detected (but not pursued) in the proactive investigations of existing teams. This team should also develop its own capabilities to proactively investigate and disrupt online offenders and networks, working in collaboration with overseas law enforcement agencies.

3.5 SUMMARY

This chapter has described in detail the structures, resources and systems for investigating online CSA offending in England and Wales. In doing so it has revealed the gaps between current provision and what is needed. This includes specialist teams with sufficient capacity to drive proactive investigations to address the most serious criminality and risk; generalist officers with the confidence and capability to effectively respond to reported crime; and technology to collect and refine the huge volumes of data to produce criminal evidence and essential intelligence to uncover serious crimes and identify children at risk.

As with all cybercrime, there is a dislocation of offender, victim and information (including criminal evidence and intelligence data), meaning an investigation that starts in one place commonly diffuses into other jurisdictions and sectors in the UK or globally. A cohesive networked response is vital for effective and efficient investigation and safeguarding. This not only affects the outcomes but also the decisions made along the way. Different bodies work to different priorities and standards, but practitioners need to be sure that other police forces or statutory bodies will be responsive to referrals so as to mitigate against wasted effort. This situation is exacerbated in the context of global law enforcement and technology firms working to divergent legal frameworks, policies and priorities. The adoption of shared priorities and common standards for risk assessment and case prioritisation needs to be an ambition.

The demand on the police in terms of recorded CSAM offences increased by 121 per cent between 2015 and 2018. And despite the diversity of offending and risk, public policies remain singularly focused on reactive law enforcement. There is a growing strain on the police to respond to such high volumes of high-risk crime, which constrains capacity to uncover and target hidden perpetrators engaged in the most serious on and offline abuse. Moreover, many CSAM investigations do not identify additional offending, so many offenders who are convicted do not receive a prison sentence. This is indicative of a burgeoning volume of so-called “low hanging fruit” offenders who are detected on mainstream social media platforms. There is a need to consider ways to diversify public policies and interventions to ensure that law enforcement is focused on addressing the most serious offenders and protecting children at greatest risk.

Finally, enforcement in this area has some added complexities. Firstly, the acute risk of suicide among suspects following an arrest, and the needs of family members to understand and process such a significant event. The effectiveness of law enforcement must in part reflect the support provided to mitigate the risk and harm that arise from the intervention. Secondly, online vigilantism is likely to remain a permanent part of this field, given the limitations on the capacity and capability of law enforcement to proactively detect and disrupt offenders and the opportunities for citizen-led investigation created by the internet. The approach and outcome of the interventions is highly variable across different groups. Regardless, they operate far outside the controlled systems and procedures of the police, and there is a need to provide greater guidance to groups who wish to work lawfully and cooperatively to limit the potential for harm.

4. VICTIM CARE AND SAFEGUARDING

In this chapter we explore the service provided to victims of online CSA both by the police and by partner organisations. First, we describe the needs of online CSA victims as identified in existing research. Second, we set out how victim support and safeguarding are delivered and by whom. Third, we set out those areas where victim support falls short and make recommendations for change.

4.1 THE NEEDS AND EXPECTATIONS OF ONLINE CHILD SEXUAL ABUSE VICTIMS

It would be a mistake to assume that the main thing victims want is a positive criminal justice outcome, with the perpetrator taken to court, found guilty and sentenced. While such an outcome is important for many, victims also want timely and accurate provision of information by the police and the provision of services and support that they can draw on if needed (Wedlock and Tapley, 2016).

Importantly research has found that victims want to know that the harm they have experienced has been validated by the police, that they have been believed and respected. The police are a potent symbol of national authority and as such their acceptance of a victim's story plays an important part in giving victims a sense that they are not alone, that they have been listened to and that society at large recognises what they have been through (Elliot et al, 2014).

Meeting the needs and expectations of children and young people can require specialist skills and processes but their expectations are broadly similar to other victims. They want clear communication, including general information on procedures and their rights. They want to be kept informed on the progress of their investigation, they want officers to be sensitive to their needs at the point of disclosure, including confidentiality and discretion, and they want to be able to access support where they want it (Beckett et al, 2015; Hamilton-Giachritsis, 2017). A key outcome is that victims feel safer after their interaction with police than they did before.

In responding to online CSA, the police have been found to lack an understanding of the risks that online offenders present to victims, to have failed to appreciate the seriousness and harm that it causes and to have missed opportunities to follow investigatory leads to support at-risk children (HMIC, 2015). Research with victims has identified inconsistency in the response, with some officers described as supportive whereas others were perceived as overly formal or unable to recognise the seriousness of the crimes (Hamilton-Giachritsis et al, 2017). Furthermore, victims of online CSA can feel blamed for what has happened, and that they have contributed to their own victimisation, echoing previous misconceptions of street-based CSA where practitioners were unable to recognise the signs of exploitation and abuse when they were presented with evidence of them.

4.2 HOW VICTIM SUPPORT AND SAFEGUARDING ARE DELIVERED

Across all police forces there is a bifurcation in the response, with specialist investigation teams generally responding to offender-related intelligence and crime reports while generalist local policing teams respond to victim-related reports:

- Specialist investigations teams will respond to reports regarding volume CSAM offenders received from NCMEC and will handle safeguarding in relation to any children with whom the offender may have regular contact (for example, as in the case of a suspect whose occupation involves contact with children).
- Local police teams will respond to any crime or intelligence reports regarding victims who live in their force area, who will deal with this alongside their other general duties.

Reports regarding local victims can sometimes lead to local or external criminal investigation (depending on the presence and location of a perpetrator) but they are often much more focused on the child, both in terms of risk and vulnerability to current or future abuse and addressing their own deviant behaviour such

as in sharing self-generated sexual imagery. Risk and vulnerability are assessed not only from the victim's point of view but also through interpreting behaviour, context and relationships. This calls for techniques, capability and interventions that are distinct from the work to tackle local adult offenders, a point made clear by one local strategic lead; *"[it's] a whole different, tricky area of business that really"*.

Table 4.1 provides a breakdown of the types of victims of different types of CSA offences included in recorded crime over an 18-month period in a single police force. It provides an illustration of the nature of local police demand from online CSA:

- Obscene publications crimes are recorded in the highest volume, but only a minority of these involve a recorded victim (such as local "youth-produced" images and non-consensual sharing between peers).
- 36 per cent of the local police demand pertained to a local victim, most commonly online sexual activity or grooming offences.
- Females comprised the majority of locally recorded victims.

This indicates that local police forces face the highest levels of demand in relation to local adult CSAM offenders, but also highlights a much more varied set of offences that create demand for non-specialists in local police teams.

"I would say in my judgement many online CSAE incidents are dealt with by local police teams; [for example] parents reporting an offender sending sexual images to a child."

(ROCU specialist online CSA practitioner)

In our survey of police strategic leads for online CSA each was asked to assess the relative importance of different offence characteristics in steering support and safeguarding resources (see Figure 4.1). The vulnerability of the victim was considered the most important factor in steering the response (55 per cent of respondents). This was followed by the risk of perpetrating an offline offence or identifying a suspect with access to children in the community. The risk of an online offence or a suspect's online capabilities were the least influential in steering resources.

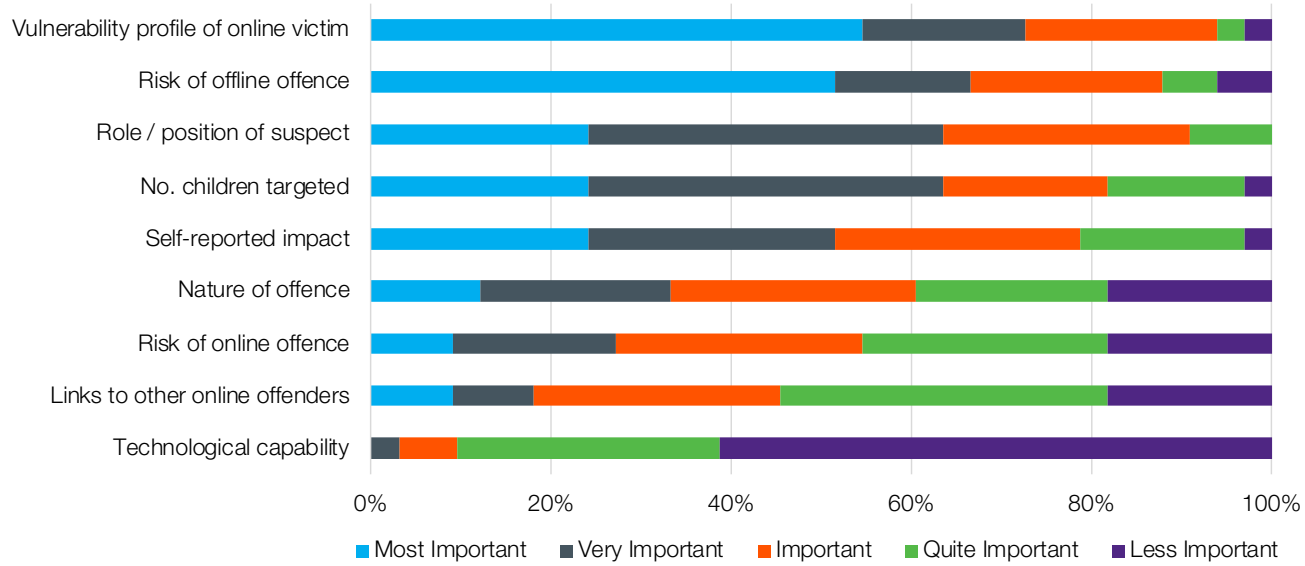
Table 4.1 A breakdown of the online CSA victims recorded by a single police force, April 2018 to September 2019

Offence group	Female	%	Male	%	State-based crime	%	Total
Obscene publication	75	5.9	14	1.1	1194	93.1	1283
Sexual activity inviolving a child	259	53.6	119	24.6	105	21.7	483
Sexual grooming	242	74.7	38	11.7	44	13.6	324
Other child sexual abuse	9	64.3	3	21.4	2	14.9	14
Grant total	585	27.8	174	8.3	1345	64	2104

* There was missing data for identifying the victim or gender in 47 recorded offences.

** The data reflect the number of recorded offences, not the number children who are vulnerable or at risk, which would need to account for repeat victimisation or victim-offender overlap in recorded crime (for example, a child suspect sharing sexual imagery may also be assessed as vulnerable), and also the variable number of at-risk children linked to each suspect.

Figure 4.1 The importance of different offence characteristics in the resourcing decisions for victim support and safeguarding



* The total number of respondents who answered each question varied.

4.3 AREAS FOR IMPROVEMENT IN THE POLICE AND PARTNER RESPONSE TO VICTIMS

Communication

Before taking the step to report a crime most victims make a decision as to whether police involvement is something they want, based on factors such as the degree of harm they have experienced, a desire to see an offender brought to justice or a need for protection or reassurance. However non-police practitioners observed that in the case of online CSA, this decision (commonly made by parents) could be distorted by ambiguity over what circumstances constitute a "police matter", whether it will do any good or whether it will lead to more harm.

While the impact of an offence can be acutely felt by victims and families, many parents opt to contact a helpline (which adopts the role of a *de facto* call screen for the police) for reasons that can include:

- A limited appreciation or understanding of online risk and harm, especially when contextualised by preconceived notions of all other (more "serious") police business.
- An inability to ascertain criminality from more subtle scenarios, such as when the child and suspect are close in age, or a sexual motive is inferred rather than made explicit in online communication.
- A lack of confidence that the complaint will be taken seriously, especially if they cannot provide tangible evidence.
- A lack of clarity about the scope to criminally investigate the crime (by virtue of being online) or what alternative support the police can provide.
- An unwillingness to expose an incident that is a source of shame, embarrassment or self-blame and worse still, to risk exposing themselves to more harm by incriminating their own child or incurring intervention from social services.

> *"I think the parents tend to think police don't deal with this. Police should do more to [let the] public know, raising awareness might lead to fewer problems. If police gave first hand, info explaining to people who [make] contact, what will happen next, it would be helpful for people to know."*
>
> **(Support services – specialist practitioner)**

Providing a supportive and empathetic response

The victim can experience trauma both in relation to an experience of abuse but also from having it exposed to their family and practitioners, with some victims feeling shame and placing the blame on themselves and in some cases, suffering the loss of what was an important relationship with the offender (for example, if they have been groomed). Recovery and resilience is considered more likely when the child is supported and

positive police engagement with both the victim and family can promote understanding, provide assurance that culpability lies with the perpetrator and help foster a supportive environment. From the perspective of reducing harm, managing this highly emotive situation in a way that is sensitive to the emotions and relationships of the child would seem to be the main priority. A child-led instead of an offender-led response, can also in turn improve law enforcement outcomes in facilitating eventual disclosure from victims which can take time and be hard-won.

> *"You've got to get into the psychological state of the child before you're going to get the proper evidence you need that will make sure that the justice is done."*
>
> **(Support services – specialist practitioner)**

At the point of reporting a crime a victim can have various expectations such as receiving a prompt initial response, assurance that contacting the police was the right thing to do, empathetic treatment from police officers and staff, that they will be taken seriously and any decision-making will be careful and considered, and clearly communicated.

Some practitioners highlighted a change in recent years, with police becoming more responsive and sensitive to victims' needs, but there remains inconsistency. The shortcomings can be procedural in nature, such as omitting to provide regular updates to victims and their families in the course of investigation, or the absence of a single designated officer to approach for information or support through the process. And in some cases, failings derive from the interpersonal style or a lack of understanding from the responding officer.

> *"We hear examples of both positive and negative experiences with the police. Young people have been positive about uniformed and non-uniformed officers, at other times the uniformed officers come across as frustrated or not understanding the issue or pressed for time, as though they don't have the time necessary to listen to the young person."*
>
> **(Support services – specialist practitioner)**

Recommendation 16

The College of Policing should review the training that is provided for generalist constables in providing support to victims of online CSA.

An improved understanding of risk and victims' needs in the online context

Our research highlighted gaps in police understanding of risk and victims' needs in relation to online CSA.

First, the absence of a physically present offender can cause the police and other practitioners to mistakenly assume the victim has greater control of the situation. The absence of an identifiable or physically present suspect naturally leads intervention to the areas a practitioner can influence, often the child and their behaviour. However, it risks signalling that blame rests with the child rather than the perpetrator and in doing so, this can exacerbate harm.

This also ignores critical contextual elements in the surrounding social, digital or physical spaces (for example, abusive on or offline norms between peers at school) that drive the abuse or harmful behaviour, and can inform effective intervention (Firmin et al, 2016). Failure or delay in identifying risk potentially leaves a child exposed to more abuse.

> *"[Victims will hear things like] 'block this person, just don't respond' … This is the right thing to do but if it is someone who has not told an adult and is being harassed [online], it's not easy for them to just ignore this because they're scared … they need that support network to help them with this."*
>
> **(NCA – Specialist practitioner)**

Second, in peer-to-peer cases involving young people close in age, practitioners can have difficulty in understanding unfamiliar behaviours or what is normal or acceptable in the modern digital context.

One regional strategic lead described an example of a group of approximately 30 children found to be regularly sharing sexual images with each other on a communications application, and expressed uncertainty in their interpretation of the harm or risk; "… *that's different isn't it? To sending images to your boyfriend, the need for social media followers … it could be trouble*."

There is a requirement for first responders to look beyond the reported offence or incident to ensure it does not lie on the surface of more serious harm and risk, by observing and understanding relevant social and contextual cues that might indicate harm (Clutton and Coles, 2007). The example in Box 4.1 provides an illustration of the challenges in assessing risk in an online context.

Box 4.1. Case study of the challenges of assessing risk in an online context

A helpline for children received a report from the mother of a 14-year-old daughter who had concerns about her 15-year-old friend who was sexually active and over two years had been messaging males online and was also producing and sending sexual images of herself (the age and identity of the male recipients was not known). The mothers concern had peaked when the girl claimed to have arranged to meet with one of the males, though it was never made clear if this meeting actually took place. The adviser perceived the main concern of the mother was to ensure safety of her own daughter, prompting her to report to the school and the helpline, and it was not clear whether the other girl's mother had known what was happening.

Contextual safeguarding is a model for intervening to address local situations, contexts and relationships in both private (for example, home) and public spaces (for example, schools or local hangouts) that foster exploitative sexual interactions and experiences. It is a framework for understanding and tailoring interventions to address situational drivers of exploitation, akin to traditional crime prevention techniques such as problem-oriented policing (Firmin et al, 2016).

The challenge with online CSA is that online digital settings are less within the reach of local practitioners and besides, are a much more fluid setting subject to continuous change (for example, new trends and platforms). In cases in which online and offline settings (and relationships more directly) intersect such as with school peers who engage online, there is scope to focus on the offline context. However, where these harmful contexts and relationships are more confined to a child's online setting, its application is less clear.

In our survey the majority of CSA leads reported sufficient training was provided for staff in specialist teams to be effective in engaging at-risk children or victims (32 or 91 per cent), identifying the risks and needs of victims (31 or 89 per cent) and in responding to reports of children producing and sharing sexual images with peers (31 or 91 per cent). However, they expressed less confidence in training provided to generalist practitioners with over a third considering it insufficient to effectively engage with at-risk children (12 or 36 per cent) and a quarter said it was inadequate for identifying the risks and needs of victims (9 or 28 per cent) or for responding to reports of self-produced sexual images (8or 25 per cent). This relative lack of specific training compared to specialist teams is unsurprising but needs to be considered in the context that much of the engagement local online victims have with police is with officers and staff in these generalist teams.

Recommendation 17

We recommend that the Home Office commissions research on how contextual safeguarding can be provided in an online context.

Greater clarity around the local police offer to victims of online Child Sexual Abuse

Police resources for responding to online CSA are driven more by localised opportunities for law enforcement than they are by victim support and safeguarding. This is reflected in the weight of investment channelled into specialist investigation of CSAM offenders, but also in the decision-making of generalist practitioners which can emphasise the police criminal justice role over support or protection.

> *"The children are not always safeguarded. The police are involved in the initial stages, what happens next is often left to the parents or the school … It is not fair on the children for police just to do the investigation. I do think it is the police's job to offer support, divert offending, offer services to victims. The police shouldn't just be an agency to dole out punishments. Their response should be victim focused to prevent further incidents. It is important to prevent reoffending because children become more vulnerable each time."*
>
> **(Support services – specialist practitioner)**

The absence of an enforcement opportunity introduces ambiguity for local officers regarding their remit with the victim. It is not clear what further role they have in delivering support and protection beyond immediate "safe and well" checks. This is complicated in the many cases in which the victims generated the images themselves and are therefore "on the wrong side of the law" and sometimes perceived as being blameworthy (see Box 4.2 for an example). As a result, the police can miss opportunities to intervene and provide support for children that might keep them safe.

Box 4.2 Case study to illustrate the complexities of handling peer-to-peer cases

A school reported to the police that a male student had shared a sexual image of a female student with another male student, who had gone on to show the image to others at the school. The female in the picture had produced the image and shared it with a male friend approximately a year prior to the crime report and was unclear how it had come to be in the possession of those reported by the school. Neither the female nor her family wished to submit a formal complaint. The police advised the female student of the law on sharing sexual images, explained the risks and advised her on future conduct. Similar advice was given to the male students who had been found in possession of the image. The image was deleted from their devices.

The role of partner organisations in support and safeguarding

The complexities of responding to child sexual abuse that occurs in local communities are tackled by multi-agency safeguarding partnerships comprised of police specialists (often public protection units), local authorities, health and education. These safeguarding hubs collectively produce robust risk and needs assessments, drawing on shared knowledge of the child's history and circumstance, before embarking on a joint investigation to arrest the perpetrator and safeguard the child. Practitioners in one police force highlighted the challenge for Multi-Agency Safeguarding hubs in accurately appraising risk, with heightened vigilance from frontline staff generating an increasing volume of referrals for at-risk children. The scope for a comprehensive partnership response to online CSA specifically is limited when the victim and offender reside in separate UK or national jurisdictions. And there are also limits in the safeguarding response from partner organisations for similar reasons to those in the police; interviewees highlighted less understanding of online harm and risk and in turn, limited prioritisation of resources from services under pressure and a lack of confidence, knowledge or techniques to effectively respond to an online victim.

> *"… the response should still be the same but there's still that lack of training among social workers and teachers. I still think they're really unclear on how to respond to it … there is such a remit of work that social services work with, [and online CSA] is not the same kind of priority as other types of work they have to deal with."*
>
> **(NCA – Specialist practitioner)**

The remit of social services in tackling online abuse remains ambiguous and priority continues to be weighted to tackling localised CSA cases (especially familial abuse). The inability to draw on the expertise of social services restricts the ability to assess needs and implement targeted safeguarding for local individuals or groups at risk. Additionally, it demands much more of the police in terms of applying the necessary "soft skills" when responding to these crimes. The response can be singularly determined by the capability of first responders (including in the police) to effectively appraise a situation and deliver an appropriate response, which can understandably lead to mixed results.

The absence of close partnership working between the different organisations creates a number of gaps. These include the absence of a common framework for making decisions which creates inconsistency but also erodes confidence in knowing under what circumstance to make a referral. The limited dialogue between organisations restricts the scope of practitioners from different organisations to learn what to expect from a partner organisation. For example, the police often represent the end-point for an identified risk or victim but those who referred cases to them were left with lingering uncertainty over what that means in terms of a response, the outcome and whether the referral was appropriate.

> *"It would help to know about the process so we could guide the parents, I get asked what will the police do and I don't know."*
>
> **Support services – specialist practitioner**

4.4 POLICING YOUTH-PRODUCED SEXUAL IMAGERY

The police approach to youth-produced sexual imagery

Current legislation for taking, making and sharing indecent images of children takes little account of the wide range of circumstances and motivations that drive these behaviours and the extent to which they are or not derived from abusive or exploitative situations. An approach which does not discriminate between offences on the basis of the underlying context and harm, obfuscates the line between offender and victim and raises the question about what does or does not constitute sexual abuse imagery (Leukfeldt et al, 2014). Moreover, the criminalisation of young people engaged in producing and sharing self-generated imagery has implications for trust and confidence in police and their partners, as a legitimate recourse, if young people experience harm and victimisation and require help in the future.

The ambivalence in weighing up the conflicting ends of law enforcement and child protection is experienced by policing across various western countries. There

are various lines to take that include; adopt a zero-tolerance approach and enforce the laws; decriminalise self-produced imagery (though this can introduce ambiguity for criminal prosecutors, especially in tackling image-sharing that occurs within an abusive context); or implement police discretion on the basis of a systematic screen or professional judgement, which leaves open the potential for inconsistent and biased responses (Leary, 2010).

In recent years, the police in England and Wales have taken the latter approach. This is to avoid unnecessary criminalisation of high volumes of children who break these laws due to the emergence of social and sexual "norms" such as sexting, and the likelihood that incompatibilities between youth behaviour and the law are poorly understood. One school liaison officer reported that *"young people have been shocked that the line from what is legal and illegal is very fine".*

The police have been empowered to tailor their response to the circumstance and avoid needless criminalisation and labelling of a child as a sex offender for being found in possession, sharing or generating sexual images of themselves or a peer (College of Policing, 2016). Cases that are diverted from criminal justice in this way are recorded as below, hereby referred to as "Outcome 21":

> *"Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the suspect is not in the public interest"*

This outcome is considered appropriate for cases in which there are no "aggravating factors"; including those for which the behaviour is considered non-abusive, where there is no evidence of exploitation or if cases do not involve "extensive or inappropriate sharing" or "persistent behaviour" from the child or young person (College of Policing, 2016). Regardless of the outcome, all images will be added to CAID and a crime record kept by police which, depending on the discretion of the police, is later disclosable in an enhanced criminal record check. In this regard, it can close off opportunities for entering certain types of employment (such as childcare) in later life.

The scale of youth produced sexual imagery as part of recorded crime

In 2018, Outcome 21 was the most frequent outcome recorded nationally by police for CSAM offences, constituting nearly a third of all recorded outcomes that year (see Table 2.2 in Chapter 2). The fact that the proportion of suspects in CSAM cases who are female has risen from 19 per cent in 2014 to 41 per cent in 2018 is indicative of the rise in the volume of self-generated images.

Box 4.3 Crime data from a local police force indicating the rising volumes of self-generated imagery in the case load.

Crime data from a single police force allowed for a more detailed profile of online CSA suspects. Nearly a third of all CSA offence suspects[68] were aged under 18 at the time the offence was reported (365 or 30 per cent), and nearly two thirds of these non-adult suspects were male (232 or 64 per cent). Overall, female offenders were a minority (174 or 16 per cent) but were over-represented among non-adult suspects (133 or 36 per cent); the most frequent age category among female offenders was 13 to 15 (80 or 46 per cent), whereas for males it was those aged 25 and over (681 or 65 per cent).

The majority of female suspects had perpetrated offences for possession, taking, making or sharing indecent images of children; out of a total of 174 online CSA suspects, 166 were linked to these offence types (95 per cent), over three quarters of whom were aged under 18 (128 or 77per cent) (see Table 4.2).

Table 4.2 The characteristics of suspects identified for possession, taking, making or sharing indecent images of children offences in a single UK police force, by age and gender.

Suspect age	Female	%	Male	%
Under 10	3	1.8	1	0.2
10 to 12	30	18.1	26	4
13 to 15	77	46.4	104	16
16 to 17	18	10.8	45	6.9
18 to 24	8	4.8	57	8.8
25 and over	30	18.1	417	64.2
Total	166		650	

* A suspect had not been identified for 993 recorded offences and in two cases the age or gender was not recorded.

68. This included obscene publication (specifically indecent images of children), sexual grooming, sexual activity and other sex abuse or exploitation offences recorded with a link to cybercrime.

Shortcomings in the legal framework

In an age in which social relationships are mediated through ubiquitous digital communications and media, youth produced sexual imagery as well as any malicious actions (such as "revenge pornography") can naturally manifest during the normal passages of youth and relationships, as young people go through a key developmental stage in their sexual, emotional and social lives (Hales, 2018; Osterday, 2016). It is the unprecedented scope for children and young people to digitally capture and share sexual images of themselves and others that draws the otherwise normal stages and trials of young lives into the realm of criminal justice.

The motivation or culpability of the "offender" in self-generating or sharing sexual images can bear little relationship to the consequences of their behavour (in terms of actual or perceived harm to others or themselves).

In the context of youth-produced imagery, criminal legislation performs a variety of functions; it gives powers to the police to tackle cases linked to sexual abuse or exploitation (notably that perpetrated by peers), it creates a more generalised deterrent to young people in producing and sharing sexual images, which serves to mitigate vulnerability and risk to the child themselves and stems the proliferation of CSAM offending opportunities for would-be online offenders.

However, there are a number of shortcomings:

- It is difficult to test the strength of the deterrent, but it is inevitably impeded by the gap in understanding of the law among young people.
- Youth-produced imagery can provide a window on to serious crime, but in the large majority of cases this is not the case.
- The introduction of a softer investigation outcome (i.e. Outcome 21) highlights the disconnect between criminal law and the operational emphasis on protecting children from abuse. In balancing these two goals there is scope for inconsistent interpretation depending on who is responding to or receiving the report; for example, while children and young people identified through industry intelligence are treated and recorded as "suspects", those who commit similar offences and seek advice or support from the third sector or the NCA[69] helplines are not referred to the local police.
- Practitioners interviewed described callers (especially parents) that were acutely aware of the victim-offender overlap, torn between the need for reassurance, protection and in some cases a response to an offender but equally, concerns over their own incrimination. The potential for existing legislation to delegitimise the police as a viable source of help or protection and deter victims or guardians from reporting crimes runs counter to the overriding objective to support and safeguard victims of online CSA.

"I had one 15-year-old girl ring up who said that she had voluntarily sent naked pictures to her boyfriend who then had shared them round the school. Her mum had told her not to phone the police as you might get in trouble, you should ring the NSPCC instead, the daughter was really sad. The mum didn't know what to do, she was fearful and crying. People know sharing indecent images of children is a crime even if you're a child; it makes them fear for their children's future, there is a strong sense of shame."

(Support services – specialist practitioner)

"Getting parents to contact police about harmful sexual behaviour online, it is harder to get them to contact police if their child is the perpetrator than [if they are not], we tell them that this is not about criminalising anyone it is about getting help."

(Support services – specialist practitioner)

The intention of the Sexual Offences Act 2003 was not the prosecution of two young people in "mutually agreed sexual activity" (Home Office, 2004), and the obscene publications laws as originally conceived in 1978 could not have foreseen the social and technological changes that have led to the proliferation of self-produced sexual imagery, nor was it intended to address such behaviour from young people. The introduction of amendments to the legislation that specify exemptions for young people aged 13 to17[70] engaged in consensual image-sharing, would focus law enforcement on tackling exploitation and abuse. Borrowing from previous research (Hales, 2018), the following behaviours might be exempted from criminal legislation for a child under 18:

a. *To take or make an"indecent" image of themselves in the first instance.*

69. Click CEOP is staffed by the NCA's 's child protection advisors who provide advice to anyone with concerns over online abuse or grooming online.

70. The Sexual Offences Act 2003 states that children under 13-years old cannot consent to sexual activity.

b. *To send it to someone if they want to, they are the subject, and the recipient has consented to receive it (unless the recipient is under 13).*

c. *To possess an indecent image of another child, if it was sent to them willingly and consensually by the subject (unless that child was under 13).*

Recommendation 18

There should be clearly defined exemptions to the Obscene Publications Act based on age and consent. This would move the emphasis away from law enforcement and towards education and awareness-raising in cases where children are sharing pictures of themselves with other children.

4.5 PROACTIVE SAFEGUARDING

Every report of online CSA constitutes a crime scene that can unearth victims and risk that either extend from, or are extraneous to the reported incident (for example, CSAM recovered from a local suspect's device may depict recent contact abuse by an unconnected sex offender). Proactive safeguarding techniques can identify hidden abuse by drawing on either the evidence collected in an online investigation or from the forensic examination of electronic devices and data collected during investigation. The digital evidence trail from a single investigation can produce a panoptic view on to a multitude of offences, offenders and victims, generating opportunities to instigate safeguarding locally or in any other UK or national jurisdiction.

"Cases with a large volume of victims require additional investigative resources in order to trace and safeguard the victims but also to identify quickly the level and scale of offending. These children identified are likely to be at risk [from] other paedophiles and as such will always be a priority."

(Local police force – online CSA strategic lead)

Table 4.3 below outlines the main sources of intelligence or evidence that can provide a sightline on to various threats, highlighting the scope to uncover serious and global safeguarding needs from a single local investigation.

Table 4.3 Local police techniques for uncovering victims and risk of CSA for the purposes of proactive safeguarding

Information source	Proactive safeguarding method
Intelligence – local child	Data collected through open-source investigation, intelligence-sharing between local agencies or onsite investigation: • Children at risk of grooming or contact abuse due to a local connection to a local CSAM offender (for example, a suspect whose occupation brings them into contact with children). • Children at risk of grooming or contact abuse identified when executing an arrest warrant (for example, children living at the address).
Digital intelligence or evidence – local /non-local child	Data collected from seized electronic devices or other investigation technique: • Victims of contact or online abuse depicted in CSAM. • Victims or children at risk of contact or online abuse revealed in chat logs or other online communication (either between online offenders or communication between victim and suspect).

Proactive safeguarding by means of interrogating digital evidence found in the possession of CSAM suspects is a relatively new strand of response, formalised in a UK strategy in 2015. Proactive victim identification adds a new layer of demand on policing and calls for a distinct set of investigative capabilities. Victim identification is a core strand of the operational response from the NCA,[71] principally focused on proactive safeguarding of victims identifiable from NCMEC referrals (particularly CSAM that depicts recent contact abuse) as well as from images and chat logs identified in the course of proactive investigation. In some cases, a victim can be identified or located using digital forensic analysis but otherwise through in-depth online investigation to reveal the location or identity of the people depicted in the image.[72]

The CAID intelligence database provides a shortcut by filtering CSAM data to draw out "first generation" (or previously unknown) images, that have not been the

71. https://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/inquiries/parliament-2017/policing-for-the-future-inquiry-17-19/publications/

72. For example, see - https://www.interpol.int/en/Crimes/Crimes-against-children/Victim-identification

subject of previous investigation. It is also inferred that they are more likely to contain recent or ongoing abuse.

Local officers highlighted a number of technical and systemic challenges to effective identification and safeguarding:

- The volume of data that is collected in the course of a single investigation and the restricted capacity to conduct timely forensic analysis, resulting in missed opportunities to safeguard children.
- The complexity and labour-intensive nature of investigations, meaning a single case can demand considerable time and resource to analyse the images or chat logs especially in cases where it is not possible to automate the analysis using forensic tools and/or the abuse took place in a non-local (so unfamiliar) setting.[73]
- The small number of "first generation" images or victims that are identified, relative to the overwhelming volume of data that is collected (some investigators suggested "new material" is more likely to be found in spaces such as the dark web).
- The capacity for some cases to spiral and for high volumes of children at risk to be identified, often dispersed across the UK or globally, with ambiguity over the local remit and responsibility but equally, presenting challenges in implementing a networked safeguarding response across jurisdictions.
- Challenges in reaching out to children if the online service provider is unable to attribute their online account or facilitate communication with the identified user.

The example below of an emerging practice identified the potential for an increased emphasis on proactive safeguarding but also the inherent limitations of a local approach to tackling vulnerability that is both UK-wide and global in scope.

Emerging practice: Dyfed Powys police force

The local specialist online CSA team identified a need to focus on more proactive investigation to uncover CSAM offenders who are perpetrating more serious offending and to identify more victims or children at risk. Closer examination of a "download" of evidence collected from a suspect's device, specifically the chat log histories on each device, unearthed additional crimes such as grooming, but also identified other children and young people for whom there was no explicit evidence of a crime but rather an online exchange ("purely chat") with the suspect. They initiated Operation On Your Side to address this identified vulnerability, with each child referred to the NSPCC which sent a message to offer support and provide information to raise awareness of the risks.

This is a localised initiative for addressing UK-wide vulnerability (it did not cover overseas children at risk) from a smaller police force which had capacity to engage in this proactive work. They developed bespoke software which sped up considerably the otherwise labour-intensive processes for analysing communications data, but they were limited to data collected in the course of their own investigations. And larger police forces which collected more data were not engaging with the initiative due to the strain of keeping up with the volume of referrals from the NCA. There were also challenges in engaging social media companies to get the permissions to be able to communicate with children identified as vulnerable.

Victim identification officers are in place across most local police forces. In our survey six police forces reported having no such dedicated resource, though some were assigned the role as a secondary duty. Moreover, the number of victim identification officers was between one or two, irrespective of the size of the police force, indicating capacity is particularly low in larger police forces (see Table 3.1 in Chapter 3). A local strategic lead expressed uncertainty over what the role should entail and highlighted the need for national guidance and others highlighted the need for standardisation, by introducing national training in this specialist area:

"Significantly more input on CAID and Victim ID from a national perspective. Both systems are what each individual UK force should be using on a daily basis, yet there remains a considerable training gap in both areas."

(Local police force – online CSA strategic lead)

One victim identification officer considered that his role was not sufficiently valued by colleagues and described challenges in managing the scale of work alongside other duties. Moreover, it relied on the processes of forensic investigators whose primary focus is criminal investigation (i.e. the CSAM suspect) and who are under considerable pressure to process high volumes of cases, each involving high volumes of data.

"[There is a need to] communicate to the force that it is a worthwhile role … I rely on the [forensic] examiners to identify the things we need and they might miss something … anything more than that [process], we haven't got the resources to take it too far."

(Local police force – specialist online CSA investigation)

73. To illustrate, one police force was compiling a database of school logos in use across the UK to be able to expedite identification of children from CSAM in the UK.

Besides following the procedural elements of the work, a definition of the specific skills and capabilities that are needed to engage effectively in victim identification work is lacking. Local officers in the UK described the limited training specific to this area. One senior stakeholder thought there was too little targeted recruitment for victim identification work despite the distinctive skills profile.:

> *"It's a very different skill-set, it's not traditional police investigation … you don't need to be a police officer, you need to know how to follow rabbit-holes … your traditional detective would probably not be very good at victim identification."*
> **(Overseas law enforcement – specialist practitioner)**

Recommendation 19

There is a need to consolidate victim identification capability, potentially using a hub and spoke model in which the National Crime Agency at the centre coordinates the activities of victim identification officers in local jurisdictions, with clear lines of accountability to the National Crime Agency for activity and outcomes.

Recommendation 20

As part of proactive safeguarding police forces should develop and embed the use of software to automate and speed up the triage process for identifying newly identified (or "first generation") images and to also identify files containing the same individuals using facial recognition software.

4.6 SUMMARY

This chapter has described the diverse and complex needs of victims of online CSA offences, and the commensurate challenges in assessing and tailoring interventions to the risks and needs of each victim. Victims do not just want a positive criminal justice outcome, they also want sensitive treatment by officers, timely information, support services where needed and recognition from the state of the harm they have experienced.

Much of the specialist resources for tackling online CSA within the police service are targeted at the investigation of identified suspects, whereas reports from victims and others in the local area are assigned to generalist frontline police officers. Consequently, the quality of the response to victims is reflective of the overall capabilities across the workforce in relation to digital investigation; harm and risk assessment; working with vulnerable victims and at-risk children and safeguarding. This complexity understandably produces an uneven response from generalist teams. Furthermore, the police and wider partner organisations need to establish and make clear the services they can offer to victims of online CSA. This would provide a clear set of expectations for victims, but also facilitate coherent partnership working, by delineating the role and remit of each organisation in supporting and protecting victims and children at risk.

More fundamentally, there is a lack of research into online harm and risk which is a barrier to implementing interventions that are informed by evidence.

The current law on CSAM was not written for the digital age and a high proportion of crimes within the scope of police intervention are perpetrated by children and young people themselves. It needs to be reformed to ensure law enforcement is focused on tackling abuse and exploitation, not intervening in the consensual and non-abusive sexual development of teenagers. Clearly defined exemptions based on age and consent are needed to move the emphasis away from policing and towards education and awareness-raising for young people on the risks and how they can be mitigated.

Finally, the global reach of the internet means that responsibility for the protection of victims and children is now global in scope. All CSAM and communications discovered by the police has the potential to become a virtual crime scene that could identify a child located anywhere in the world who remains at risk of abuse. This important work relies on a highly specialised set of capabilities, technological solutions to analyse increasing amounts of data and a clearly defined role and training requirement for those tasked with these investigations.

5. PREVENTING ONLINE CHILD SEXUAL ABUSE

So far, we have described the work that is undertaken to tackle abuse that has already taken place. However, it is clear from the volumes of incidents, particularly CSAM offences, that we can never "arrest our way" out of the problem of online CSA. The volumes of offending are simply too large. While both proactive and reactive investigation is vital in order to detect and disrupt offenders, and to safeguard children, the reality is that most online CSA offenders will not be identified by law enforcement. We therefore need to do much more to prevent online CSA in the first place.

The commitments and framing of the problem in the national CSA strategy (HM Government, 2021) provide a valuable steer to delivering a cross-government response to CSA, with a particular emphasis on prevention. In this chapter we explore what more can be done in the prevention space in relation to online CSA. First, we set out a conceptual framework for thinking about preventative actions targeted against online CSA. Second, we then look at the three main channels for preventative interventions and discuss what more could be done in each. These are: offender diversion and controls, education and awareness and online situational prevention.

5.1 A PREVENTION FRAMEWORK

The three widely used layers of crime prevention are primary, secondary and tertiary (Wortley et al, 2012; McCartan et al, 2018). Primary and secondary prevention relate to interventions which take place prior to an offence, whereas tertiary is a strategic response after an offence, principally to minimise the risk of re-victimisation or re-offending:

- **Primary**: universal approaches that take place prior to offending.
- **Secondary**: approaches targeted at "at risk" groups, which include prospective offenders and those deemed vulnerable to victimisation.
- **Tertiary**: a response to CSA at the time of offence or once it has taken place (for example, victim support or interventions/controls to manage convicted offenders).

In relation to online CSA, we can envisage all three layers of prevention operating in three different arenas. Drawing inspiration from a prevention typology developed by Smallbone and Wortley (2017), Table 5.1 outlines the main existing prevention strategies viewed from the perspective of the design of the digital environment (i.e. the situational context), the behaviours of offenders and children and young people and prospective guardians.

In our survey of CSA strategic leads, we asked about what more needed to be done to prevent online CSA. 89 per cent told us that education to influence the behaviours of local children was very important, more than for any other prevention strategy (see Figure 5.1). The reasons included a perception that children are entering into online spaces with limited supervision and engaging in risky sexual behaviours while displaying a lack of awareness or vigilance to the risks. 57 per cent believed education and awareness for adult guardians was very important.

> *"Many of the more prolific offenders are engaging with large numbers of children across a range of platforms. It is clear from these that children are prepared to engage in sexual communication and sexual acts without knowing who is at the other end of the communication or that their communication and videos are being captured. Education therefore remains a key component of raising awareness of the risks and driving down opportunities for offenders."*
>
> **(Local police force – online CSA strategic lead)**

51 per cent considered regulation of the technology industry to be very important and 37 per cent thought the same about improved controls and security on online platforms. A key area highlighted was the verification of identities and linked to this, more controlled access to online spaces to prevent offenders infiltrating young spaces online and also prevent children and young people from entering spaces that are not age-appropriate.

"This is an area which presents significant opportunities to drive down demand. Many of the platforms require little or no confirmation of identify etc. and increased controls and security could reduce the access to many platforms by children reducing the overall risk to them and reduce the number of offenders who scour such sights knowing that their true identify is unknown and is likely to remain so."

51 per cent considered that in of itself, criminal investigation was very important as a preventative strategy, presumably because of its deterrent effect as well as the ability to disrupt activity or to incapacitate an offender via a spell in custody.

Table 5.1 The three-layered prevention framework applied to online CSA

	Intervention layer		
	Primary	**Secondary**	**Tertiary**
Digital environment/ setting	Digital safe spaces for children. Technology that digitally shields children from online risk and harms (for example, URL blocking or applications that moderate online behaviour).[74]	Identify and block suspicious communications between users to prevent online exploitation. Block the purchase of abusive images.[75]	Block URLs containing CSAM. Removal of accounts or forums that facilitate viewing or sharing of abusive images. Removal of indecent images of children from URLs.
Offending	Public information campaigns to raise awareness of the law and related enforcement. Public information campaigns to promote support services.	Warning messages for those engaged in risky behaviour (e.g. pop-up message on a search engine to deter and signpost to help). Diversionary programmes for those considering offending (including therapeutic interventions and support lines). Referral to advice and support for children and young people displaying illegal or harmful sexual behaviour.	Intelligence gathering and related interventions, including tactics such as website or forum takedowns. Management of convicted offenders (for example, control orders imposed by the courts). Rehabilitative treatment programmes in the community or prisons.
Victims and vulnerability	Public information campaigns to raise awareness of the risks and appropriate protective measures (for children and young people or guardians). Educational programmes in online safety, healthy relationships and identifying the signs of grooming and exploitation.	Support for those affected or with concerns to seek help or advice (such as helplines). Referral to advice and support for children and young people displaying "risky" online behaviours. Education of others in a child's social network (such as parents, teachers and peers) to identify and act onrisk.[76]	Educating victims in online safety. Therapeutic intervention for victims. Removal of indecent images of children from URLs.*

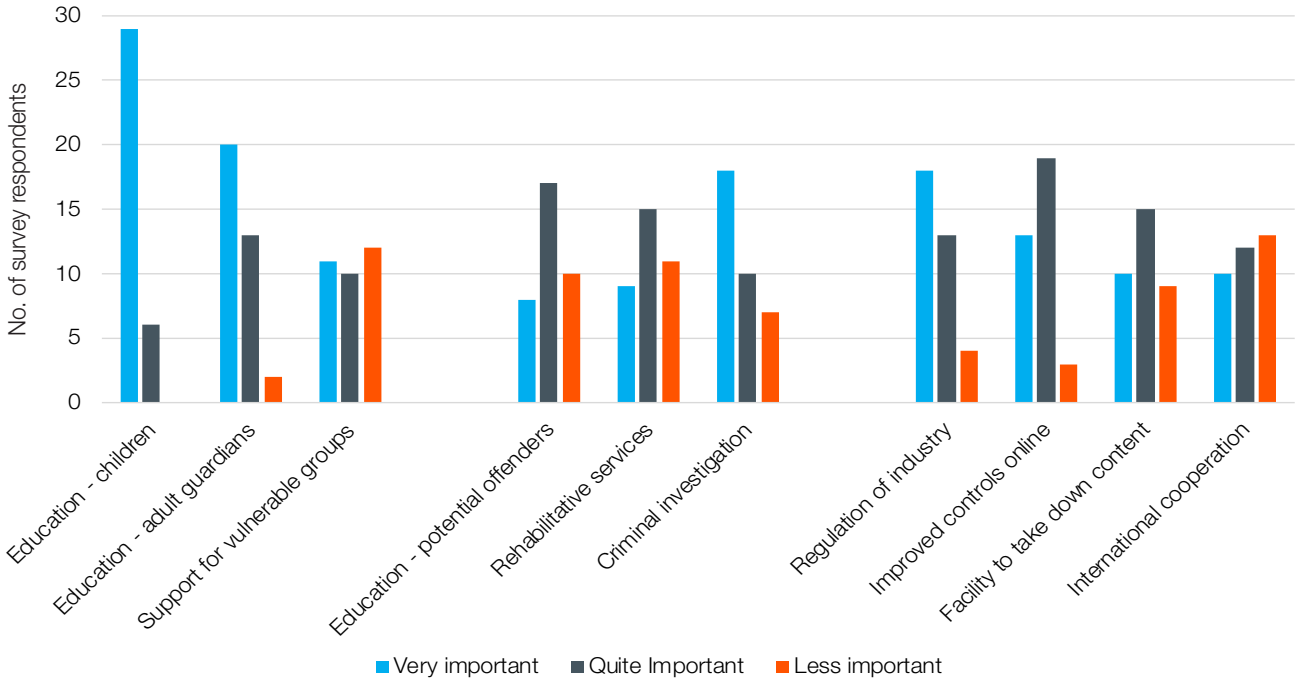
* Image takedown is included twice because it reduces the risk of revictimization of the child in the image (caused by repeated viewing) and also reduces the online opportunity to offend.

74. For example see https://blog.bit-guardian.com/best-app-to-control-kids-phone-in-2020/ or https://www.bbc.co.uk/news/technology-49726844

75. IWF services include identification of payment services and virtual currency wallets associated with CSAM. Alerts are distributed to related IWF member organisations https://www.iwf.org.uk/our-services

76. Those within a child or young person's social network are more likely to identify signs of harm prior to involvement of law enforcement. Awareness and prevention education of those in social networks (e.g. friends, family, teachers or healthcare workers) also known as 'bystanders', builds capability and enables recognition of suspicious behaviour earlier (Plummer and Klein, 2013).

Figure 5.1 Prevention strategies considered most important in the police for reducing local online CSA and exploitation



The following sections examine more closely the three methods of prevention highlighted above; offender diversion and controls, education and awareness for children and young people and online situational prevention to increase public safety. In each, the current and proposed strategies, the role of the police, and the challenges in coordination and implementation are discussed.

5.2 OFFENDER DIVERSION AND CONTROLS

Law enforcement forms an important component of crime prevention, not only in providing a visible deterrent but also in diverting offenders away from a pathway into more serious crimes. However, the practitioners we spoke to emphasised the need for a change of approach that supplements the work of specialist police investigators in pursuing these offenders, with a proper focus on trying to change offender behaviours.

> *"The scale is just frighteningly huge … there's so many people just interested in this stuff ... it's a social problem rather than a law enforcement problem."*
>
> **(NCA – Specialist investigator)**

> *'The biggest challenge to the UK is the fact that we don't consider it a national health problem, we see it as a crime … It's a more complex problem calling for a more complex response and at the moment we're hitting a digital problem with a fairly blunt hammer (i.e. law enforcement).'*
>
> **(Private sector representative)**

Offender diversion

The growing concerns over child sex offending in society do not always align with the reality on the ground, with police practitioners telling us of their frustrations at having to deal with high volumes of less serious offenders who are unlikely to pose a physical risk to children.

> *"… [they say things like] 'oh but it was just a fantasy, I wasn't doing anything' … a lot of these men are really stupid, it feels like a waste of my time when there are worse offenders out there."*
>
> **(Local police force – specialist online CSA investigation)**

The use of public messaging can help sharpen the deterrent and ensure public understanding of the legal position, to undo existing rationalisations or minimisations of behaviour, but also reach out to people experiencing sexually inappropriate thoughts and signpost them to support services and divert them from offending. Mass communications can be delivered to the public or targeted to individuals or spaces in which there is indicated risk.

Examples of how this can be done include:

Risky internet browsing: pop-up communications were implemented by internet search engines to respond to text that indicates a user is searching for CSAM. The message flags up the illegality of the behaviour and signposts the individual to support at

the Stop it Now! website[77] – this led to a thirteen-fold reduction in related searches[78] and in just over three years 20,644 clicked from these "splash pages" to the UK support site, though the proportion who engaged with support is not known (Justice, 2019). Some practitioners indicated the potential for more targeted diversionary communications on URLs in open and dark web spaces that are known to contain CSAM, for example posting support links and diversionary service information within known CSA forums.

Identified suspects: unlike those identified when browsing the internet, who have not yet (ostensibly at least) perpetrated an offence, most online communications companies react to an offence that has already occurred. For this reason, they refer to law enforcement rather than signpost support, presumably because any communication with the user may compromise a prospective investigation. However, many investigations do not reach a criminal justice outcome despite the digital intelligence received from NCMEC, showing that an image has been accessed or shared at an identified address as indicated by one specialist investigator; *"we know it's there, we can't prove it, [sometimes] we know it's that person*."

Hampshire Police developed "warning notices" issued in cases where an investigation fails, that "gives a little bit of guidance on how to conduct themselves on the internet, it's a shot across the bows [but] doesn't carry any bearing". There is controversy in an approach that sends warnings to people who have not been found guilty of a crime and further, are disclosable during subsequent DBS checks (placing limits on an individual's freedom to apply for certain jobs). A similar approach is taken by police in Germany but the emphasis was on providing support rather than issuing a warning. A message states: "we're not sure what you did but if you think you might need help then go here to get some help".

Mass communication: Police forces in Wales, in partnership with the Lucy Faithfull Foundation (an offender support service), introduced a public information campaign to raise awareness on the laws for accessing CSAM.

> *"I think there are offenders out there who want help but they don't know about Lucy Faithfull … It's not the police's role, but I don't think there's enough being done to help offenders, because they do need help."*
>
> **(ROCU specialist online CSA investigation)**

The challenge for the police is in targeting finite resource when reaching out to such a broad base of (predominantly male) offenders that are dispersed across all social, economic, demographic or geographic backgrounds. Police interviewees described political sensitivities in facilitating a response that emphasises support over law enforcement. This is because of the stigma, anxiety and a strident public narrative that is less mired in the real-world complexities and conflicting priorities faced by the police, and understandably presses for justice and safety assurances rather than looking to prevent abuse.

> *"We need to get rid of the anger, the outrage and the hatred and start taking a mature approach to dealing with them... I'm not saying that there's not people out there who don't need to be pursued, but a lot of them they want help, a lot them want effective [coping] strategies. I'd much rather see that than see a child get abused."*
>
> **(Overseas law enforcement – specialist practitioner)**

The work of charities like the Lucy Faithfull Foundation is central to diverting individuals from online offending, mostly by providing a helpline which allows a caller to remain anonymous while directing them to online self-help treatment programmes. The helpline provides an outlet for many who would otherwise have no-one else to discuss this matter with and has a focus on education and building personal coping skills to help them manage their own behaviour. As with other charities such as StopSO and the Safer Living Foundation, there is also scope to provide more intensive therapeutic intervention to those who need it, though an individual may need to forego their anonymity to access these services.

There is indication that these interventions have value in preventing future offending (Beier et al, 2015; Finkelhor, 2009; Mokros and Banse, 2019) though some are calling for more robust evaluation to support an expansion of these services (Justice, 2019). Currently the indications are that these charities are constrained in their resources, with the Lucy Faithfull Foundation reporting 6,000 calls missed in a recent three-year period (2016-19) due to a lack of capacity, and another charity (Circles of

77. This service is run by the Lucy Faithfull Foundation.

78. According to a 2018 Google blog, a partnership campaign launched with Lucy Faithfull in 2013, in 40 languages led to a significant decrease in CSA image search queries https://www.blog.google/technology/safety-security/continuing-fight-against-child-sexual-abuse-online/

Accountability) recently came to an end due to a lack of funding (Lucy Faithfull Foundation, 2019).

To a large extent, the Lucy Faithfull Foundation has become the de facto source of support and rehabilitation for the rising numbers of offenders identified and investigated by police. In every arrest the suspect is advised to call the helpline should they require emotional support or if they wish to address and change their behaviour.

Research has found it is not uncommon for offenders to consider seeking professional help[79] and a more proactive prevention strategy requires reaching out to people at an earlier stage, preferably before committing an offence. One barrier is publicity, ensuring that awareness is sufficiently widespread so those with a need can take the decision to access the service.

Examples from police forces have demonstrated the short-term effect of such awareness-raising; in Wales a public campaign led in the short-term to approximately a 40 per cent increase in people contacting the helpline.

The extent of voluntary engagement is very dependent on trust and confidence in a service that will not leave them exposed.

> *"There are people out there who know they have a problem and are looking for a way to interact with therapeutic service providers without being treated as a criminal."*
>
> **(Private sector representative)**

In Germany there are stringent laws in relation to CSAM offending, however public policy has prioritised a prevention strategy for treating individuals with a sexual interest in children or young people. An integral component is the Dunkelfeld service which offers support to individuals, many of whom have committed offences but have not been detected by law enforcement. Most commonly they have engaged with CSAM online, though a minority have perpetrated a contact offence. The focus seldom deviates from the treatment of the individuals, with strict confidentiality rules prohibiting practitioners from reporting to the police or other organisation, one that can only be breached when an individual discloses a real and imminent risk to a specific child. This encourages engagement with the service and facilitates more openness. In addition to therapy, practitioners are also able to prescribe suppressant medication to control the individual's behaviour (Beier et al, 2009).

Recommendation 21

The government should invest more in offender treatment services to tackle the behaviours of those who recognise they have problem and are willing to address it.

Prevent reoffending

The majority of CSAM offenders do not receive a custodial sentence and have no access to statutory educational or treatment programmes. Interviewees and the published evidence suggest that for many CSAM offenders, the experience of the police visit and arrest is itself a strong enough deterrent to inhibit the likelihood of future offending. A recent study in the UK found only 2.7 per cent of offenders convicted of a CSAM offence subsequently perpetrated a contact offence, while CSAM offenders with a prior contact abuse offence were three times more likely to be reconvicted for a sexual offence[80] (Elliott et al, 2019). This raises questions over the nature of support or intervention needed to manage CSAM-only offenders effectively and efficiently with such low recidivism rates and limited propensity to escalate to more serious sex crimes.

Organisations such as the Lucy Faithfull Foundation offer post-conviction support that is often paid for by the offender. The role of police and statutory partners post-conviction is to primarily implement control measures imposed by the courts to restrict behaviour and reduce opportunities to reoffend; certain restrictions may be placed on an offender's internet use as part of a Sexual Harm Prevention Order. Enforcing these restrictions introduces new challenges, requiring practitioners to monitor and supervise behaviour in online spaces that are more easily concealed. Effective detection of a breach requires a similar set of digital forensic techniques and powers as those needed for criminal investigation, such as analysis for searching and triaging devices or digital techniques to search for hidden devices or servers at their home.

The challenges include:

- Finite resource: proactive and specialist resources need to be conserved for the highest risk cases due to the high demands placed on offender management and digital forensic teams. This commonly relies on the strength of assessments made during periodic home visits often based on a suspect's behaviour or answers in interview.

79. In research looking at 254 members of the public who self-reported both a sexual interest in prepubescent children and having perpetrated a related offence, one in five (20 per cent, 52) reported they had considered seeking professional help, most commonly those who had engaged with "child pornography" (Dombert et al, 2016).

80. This comparison was between CSAM-only offenders – i.e. those with no prior conviction for any other type of sexual offence – and 'mixed' offenders with prior CSAM and contact sex abuse offences.

- Variable technical capability: we found variability across police teams in their technical capability, with some more reliant on analogue methods to assess digital risk due to limits on technical resource or capability.
- Digital monitoring: whereas community-based intelligence might flag breaches of offline restrictions, the same is not the case for online behaviour. Several police forces have trialled or introduced software which facilitates continuous remote monitoring of an offender's internet-use and even send communications to stem any suspicious online behaviours from the offender.

This patchy implementation of offender management introduces inconsistent coverage across different police forces, and currently there seems real potential for more motivated and technically sophisticated offenders (arguably those for whom the controls are most needed) to continue to offend despite the controls in place.

> *"At the moment there is differential practice, there needs to be consistency … why is it that one force chooses to do that, a bit, and another force doesn't use it at all?"*
>
> **(Support services – specialist practitioner)**

Practitioners highlighted the relative paucity of resources channelled into follow-up provision such as local offender support, treatment and management (including offender management, probation and prisons) that devalues the efforts of law enforcement in tackling online offenders.

> *"[There has been] massive investment in the front-end but that then it moves the bottle-neck further down … your digital forensics teams, the management of sexual or violent offender [MOSOVO] teams"*
>
> **(ROCU specialist online CSA investigation)**
>
> *"… it's pointless the police putting all these resources into investigation, if we're not going to put resources into managing them in the community."*
>
> **(Overseas law enforcement – specialist practitioner)**

Recommendation 22

The National Police Chiefs' Council should invest more in the technology required to monitor the activity of convicted online offenders and there should be stronger common standards in relation to the technical capabilities available across police forces.

5.3 EDUCATION AND AWARENESS

There are good reasons for thinking that many of the things that make a child vulnerable to offline abuse also make them vulnerable to online abuse (Livingstone, 2017). That said, the centrality of online spaces to the personal lives of children and young people has introduced new elements that contribute to vulnerability. In each if these areas there is an opportunity to do more work to educate children around how to stay safe online.

Social networks

Friendships are increasingly formed and developed in online spaces such as social media and gaming sites, rendering conventional notions of a "stranger" more ambiguous (Davidson et al, 2009). Research has highlighted widespread misapprehensions among children and young people about the true nature of online offending and exploitation which impairs ability to identify and avert risk (Smallbone and Wortley, 2017; Webster et al, 2012). One approach to tackling this issue is to develop the evidence and educate children on patterns in digital communications that signal risk,[81] as well as understanding techniques already in use by children and young people who are less vulnerable to grooming or abuse.

Access to technology and dangerous material

Internet-enabled devices that can be used to produce and share digital media are increasingly accessible to children and young people (Childwise, 2020) and there is evidence of evolving normative behaviours that conflict with values and laws in society. The Internet Watch Foundation found the vast majority (96 per cent) of CSAM identified from live streaming was filmed by the child on their own in a domestic setting

81. For example, the NSPCC translated research into grooming interactions into an online education package -https://learning.nspcc.org.uk/research-resources/2017/stop-time-online

82. To illustrate, a poll by the Home Office and Government Equalities Office found 84 per cent agreed it was acceptable to share a "nude pic" of their boyfriend or girlfriend without their permission, so long as it is just sent to friends.

(IWF, 2018). While some of this will be attributable to grooming and exploitation, these behaviours also derive from broader social trends including the sexualisation of youth in mainstream media, changed notions of socially acceptable behaviour including sharing sexual images of themselves or others (even when it is non-consensual[82]), and the reinforcement and validation sought in their digital interactions with others (Vannucci et al, 2020).

Youth education represents not only protection but also a diversion strategy, to help recognise harmful behaviour, signpost support, understand safe and healthy relationships and be aware of the legality of their actions. Many children and young people themselves recognise a need for greater education to help keep themselves safe online (HM Government, 2020). Some practitioners advocated a protective over prohibitive approach, such as teaching "safe sexting" techniques to mitigate the risks and harm, but such a policy is incompatible with the current legal system.

"… we need an honest conversation about how the kids are using the internet, the validation they get from strangers, and what puts them at risk."

(NCA – Specialist investigator)

"Look at what we have done as a society, with modelling and such, we are bringing children up in a totally sexualised society, so by the time they get online when their hormones are jangling and we're saying don't do it…there are double messages."

(Support services – specialist practitioner)

Impaired guardianship

Research indicates that children can be safer online when there is effective monitoring and protection from parents (Whittle et al, 2013; Wildsmith et al, 2013). There is a careful balance between giving children the freedom to thrive in an online environment, that brings immense opportunities, and imposing limits or restrictions to keep them safe (Livingstone, 2017). Children are most likely to turn to their parents for help when something goes wrong online (Ofcom, 2020) but monitoring is inherently difficult for parents or other guardians (such as teachers) due to the private nature of online spaces. Despite their central preventative role, we found there were concerns that many parents lacked sufficient knowledge of the technology, the sites inhabited by their children, the nature of the risks, prevention techniques and where to access information and support. Moreover, technology and online social trends continuously evolve and the challenge is in keeping abreast of these changes (both for parents and practitioners).[83]

"if parents don't know that an Instagram account should be private if you're a child, then we should be doing a national advertising campaign for every parent in the country. It has to come down to every parent at the end of the day."

(Local police force – specialist online CSA investigation)

Recommendation 23

The government should review the effectiveness of current work in relation to educating both children and parents about the risks of online CSA.

Work is already underway to educate children and parents about risks online. The NCA (and formerly CEOP) has led the way with the national ThinkUKnow campaign for children and young people, parents and practitioners. Added to this, online safety and healthy relationships recently became a core part of the school curriculum in England, in recognition of the integral role online spaces play in the lives of children and young people and a pressing need to address relevant risks (Department for Education, 2019).

In police forces, neighbourbood teams adopt a more localised and reactive role, either in response to a specific incident or problematic trend (for example, a school reports a sexting problem among their pupils). In many areas this is delivered by police staff involved in the Safer Schools Partnership in England[84] or the school beats initiative in Wales (see description below). The level of training specific to online CSA varies, with some generalist officers describing a lack of confidence in their own knowledge and understanding of online safety.

Merseyside Police introduced an initiative to train Police Community Support Officers as cyber champions with a role in providing support and safeguarding advice to children in schools, and victims of cybercrime (including online CSA). A key objective is to improve the quality of police engagement to build trust and confidence among children and young people who are often reluctant to engage with the police. Some have done this by addressing workforce capability, others suggest more digital engagement such as through social media to facilitate positive engagement.

83. To illustrate, the IWF highlighted an urgent need to educate parents and children about the risks of live-streaming services (IWF, 2018).

84. A joint education and policing initiative with a focus on early intervention to prevent crime and support victims of crime. Commonly it involves dedicated police staff working in designated school(s).

"… that's one thing we're lacking, we come across a lot of young people [presenting with these risks] but I wouldn't have a clue what to advise them"

(Local police force – generalist officer)

"… there is an emphasis on all officers to engage with communities in attempts to increase reporting amongst the victims of Child Sexual Exploitation, improving their confidence in the police response and to understand the issues that prevent vulnerable people to come forward. Additionally, [the aim is] to enhance officer knowledge, understanding and response to safeguarding and to recognise the increased risk of those who do not support a criminal prosecution."

(Local police force – specialist online CSA investigation)

Recommendation 24

The National Police Chiefs' Council and the College of Policing should review the training available for frontline police officers in providing preventative advice to children and parents in relation to online safety.

5.4 ONLINE SITUATIONAL PREVENTION

Online CSA incorporates a diversity of offending that is underpinned by a multitude of environmental drivers, motivations and behaviours; for example, whereas some offending is the result of a sustained sexual interest in children and may represent an extension of offline contact offending, some represents more opportunistic consumption by the "curious" on mainstream social media. Understanding how digital environments interact with online behaviour and drive offending helps inform situational prevention strategies to inhibit opportunities to commit crime, particularly for those who are less determined in their offending (Smallbone and Wortley, 2017).

One of the most robust theories of crime is that offending is the product of opportunities that arise in the course of day-to-day behaviours, activities and situations, with central factors being the presence of a motivated offender, a suitable target (i.e. victim) and the absence of a guardian (Cohen and Felson, 1979). Offenders are assumed to make a rational choice in committing a crime, balancing considerations over the amount of effort required, the level of reward to be had and the level of risk in offending, particularly from detection and punishment (Cornish and Clarke, 2003).

Further, provocations in the environment can foster offending; for example, ideas shared between peers which rationalise offending. There is also a need to address offender beliefs that excuse or minimise deviant behaviour such as by alerting people's conscience to the harm caused by their actions (Cornish and Clarke, 2003).

Applying situational crime prevention theory to online CSA

So how would one apply this thinking to the online situational environment to prevent online CSA?

Increase the effort required to offend: the internet has lowered the barriers of entry for motivated offenders, as well as opportunists, who might otherwise not have offended.

"It's so easy for people … look at how the numbers have grown, and I don't think that's the end of it [once caught], they'll come back."

(Local police force – specialist online CSA investigation)

"Kids will always find a way around these things but some of it is just too easy … let's not make it so easy to have access to these children."

(NCA – Specialist investigator)

Greater use of identity authentication would make it harder for groomers to access sites where children and young people are present.

Reduce the reward from offending: for many offenders the benefits are confined to experiences in online spaces, such as seeking sexual or other gratification from engaging with or collecting CSAM, networking with like-minded others or engaging in sexual communications with victims online. Prevention strategies need to consider how to reduce the benefits from engaging in these online activities; for example, in tackling online criminal forums there may be scope to engage in strategies to undermine the trust between members and thereby disrupt networks.

Increase the risk: the anonymity afforded by the internet changes human behaviour and heightens a propensity to offend in fundamental ways, in part because of offenders' confidence in the levels of online privacy and protection. In the case of the rising volumes of offenders identified on mainstream social media this confidence is misplaced (as evidenced by the burgeoning numbers of offenders referred by NCMEC). The perception that engaging in these behaviours is low risk has cultivated the conditions in which online CSA has become a volume crime. Communicating more

clearly the policing capability in this area may be one way of inhibiting online offending.

Tackling provocations: the internet provides near unlimited availability of pornography with mainstream sites hosting content (mostly from overseas) that sexualises young people (for example, "teen" or "barely legal") alongside all other content and search algorithms that direct and reinforce these interests through progressive links and pop-ups. This can result in users being directed to more extreme sites and content. This can lead to compulsive and escalating sexual fantasies and behaviours. For more determined offenders there is also the challenge in tackling the positive reinforcement received when networking with like-minded others in online forums, which can entrench and escalate offending.

> *"The majority, not all, get there from adult pornography use … otherwise they might not have gone there. [The internet] enables this bad behaviour to happen, it almost provokes this behaviour, not only facilitates it, there's a dynamism … there's all kinds of stuff [online] that you could never have imagined was even there."*
>
> **(Support services – specialist practitioner)**

As discussed above, pop up notifications warning browsers of the potential dangers may be one way of interrupting the cycle of escalation. Information about support services could also be provided more systematically in the parts of the internet where these offenders are likely to start out on a journey that could end with them viewing CSAM.

Removing excuses: the widespread availability of CSAM online and a perception among image offenders that their crimes are victimless, serves to attenuate the perceived harm of their actions and their own culpability. Some minimise their engagement with CSAM as "fantasy", not always recognising that the act of viewing the images means they have broken the law. Further, some perceive a moral grey area in relation to sexual communications, especially when the difference in age is small or uncertain, or they wrongfully construe a young person's behaviour as consent; one investigator believed that some "wouldn't even class themselves as a sex offender because [the young person] is 'up for it'."

> *"Online offences are the easiest to commit, people can commit in and might have some sort of internal rationalisation where they don't see it as committing an offence, because they have a distance between themselves and whatever they are looking at…and maybe they don't make the leap to it being real people suffering real things"*
>
> **(Local police force – generalist officer)**

Communications aimed at preventing online CSA should systematically combat these excuses and make clear the harms caused to children.

Technological solutions that could help to prevent online CSA

Identity authentication

Technology can be used to authenticate digital identities, including software applications which create digital passports and facial recognition software which can be used to verify the age of the user. The mainstream adoption of identity verification software holds considerable potential to mitigate online risk and harm. It enables the creation of safe spaces in which access rights can be readily monitored and controlled, separating users by age group; it can facilitate more informed choices from users by means of a trust-rating system to reflect the level of identity authentication completed by others on the platform; and it introduces a deterrent by being able to attribute online deviance to real-world identities, enabling a law enforcement response when appropriate.

Mandatory identity verification would be difficult to enforce, especially for websites run by non-UK companies (Burgess, 2019).[85] The greatest potential is in providing products and services for parents and children who are looking for these protections. There is an emerging market in social media and online communication products for children and young people that are designed and marketed under the principles of online safety, including more rigorous checks of user identities, restricted access permissions based on age, and more stringent terms and conditions that are proactively monitored and enforced. Introducing an industry "kitemark" on this basis to help guide consumer choice towards online spaces that offer assurances of safety has been suggested (Justice, 2019).

85. This is specifically in relation to the UK Porn Block, and thus only relates to porn site regulation https://www.wired.co.uk/article/uk-porn-ban-digital-economy-act

Surveillance

Many companies receive reports of online offending from users however, more timely and comprehensive coverage requires proactive surveillance to detect illicit content.[86] PhotoDNA is software that is widely used to apply a digital fingerprint to each indecent image of a child that has been detected, thereby enabling companies to complete automated searches for all known images. Industry-funded bodies such as the Internet Watch Foundation also play a key role in receiving reports, proactively searching images with a known digital signature and flagging CSAM to web companies to facilitate detection and removal; unlike specific platforms, they provide internet-wide coverage.

More recently, image recognition software has been developed by platforms to automate searches for otherwise unknown nude images or even more specifically, nude images of a child (Davis, 2018). Technology has been developed to detect recorded or live stream videos containing CSAM; one live streaming application designed for use by children used image recognition software to proactively monitor in real-time all video and image-sharing, but highlighted the need for a significant amount of human moderation resource due to the number of images flagged incorrectly and also the need to provide real-time intervention (for example, direct a young person to put their clothes back on).

A much greater technical challenge lies in the development of robust methods to proactively identify communications linked to the grooming or exploitation of children and young people. In part because of the widespread anonymity of users who are intermingled (for example, without knowing their age), but also the complexity of the task for moderators in collating and accurately interpreting risk signals from online communications.

The UK government with partners in the WeProtect Global Alliance and Microsoft recently developed software that conducts an automated search for specific key words and 'speech patterns' to identify potential grooming. The software has been made freely available to small and medium-sized technology companies.[87]

Challenges in designing out online child sexual abuse

There are a number of challenges in designing out online CSA through the kind of situational crime prevention measures described.

First, companies may resist measures that threaten consumer privacy and convenience. There is a clear trade-off here between safety and liberty that needs to be addressed by policymakers in the public interest.

Second, some of these measures require social media companies to increasingly moderate what people can say and do on their platforms. Proactive crime control strategies raise concerns over censorship and the right of these companies to decide. Clearly there can of course be no excuse for engaging in online CSA offences but as indicated earlier (in relation to suspected grooming and CSAM) the messy reality is that interpreting the abusive nature or legality of online content can become quite subjective, requiring extensive human moderation because the social and human context behind taking and sharing an image is what shapes the assessment of risk or criminality.

Third, there are data protection issues that complicate the sharing of information between policing and the private sector to prevent online CSA. For example, private sector representatives told us of the challenges in sharing the index of digital signatures (or hashes) for the millions of images in the UK government Child Abuse Image Database (CAID) which constitutes personal and highly sensitive data.

> *"… [the government] can't just ship a database of 12 million images to each company in the hope they will use it, that's not an acceptable use of that data."*
>
> **(Private sector representative)**

Access to the vast repository of hash files collected by law enforcement would facilitate proactive crime prevention and add legitimacy to industry efforts to police online spaces. Interviewees highlighted the need to develop new policies and technological solutions for separating the index reference (i.e. the hash) from the personal data, in order to permit a company's access without breaching data protection laws.

Fourth, technological developments across industry may make this work harder. In an age in which more and more personal information is stored and utilised in

86. For example, Facebook reports that 99 per cent of identified images are flagged before being reported by a user (Facebook Transparency Report, 2019).

87. https://www.gov.uk/government/news/new-ai-technique-to-block-online-child-grooming-launched -

online spaces, encryption technology introduces more enhanced data security to protect and users and give them confidence that their personal data is safe from abuse by illegitimate as well as legitimate industry or state actors.[88] The trade-off in bolstering data security is an erosion of capability to monitor and detect hidden crime. Not only does it reduce the real and perceived risk for offenders operating on the platform, in limiting the scope to detect and investigate offences, it relieves a company from the responsibility to monitor and act on offending.

Fifth, there is clearly a risk of displacement. A more hostile online environment creates barriers and risks, deterring opportunists and driving those most determined offenders "underground" to more secure and hidden online spaces or in the case of the dark web, spaces that are hard to reach for law enforcement and partners.

Finally, some interviewees speculated that the historic dominance of a small number of (principally US-based) online communications companies may be replaced by a more diverse and fragmented market, thereby increasing the scope to displace offending and create gaps in the coverage of crime prevention.

5.5 A SYSTEMIC APPROACH TO PREVENTION

The UK has in the past favoured self-regulation and joint working with internet service providers and wider industry over direct controls and regulations (Carr, 2017), but many consider that this approach is not working and the next step is to impose rules to govern the conduct of all companies providing online services in the UK.

The government has published the Online Safety Bill to introduce UK regulations to ensure internet companies to provide better protection for the public from a range of harms that include CSA (UK Parliament, 2022). The Bill intends to place a legal mandate on companies to take more responsibility and be more accountable for the safety of users on their platform. The plans would involve a set of national standards that would be regulated by Ofcom, with failure to comply leading to enforcement action; the proposed powers range from issuing fines, publicly exposing a company for failing to abide by regulations, direct action against senior members of a company or blocking the company from operating in the UK. There is some precedent to state-led regulation of the internet such as the introduction of an e-Safety commissioner in Australia with powers relating to an industry code of practice and the ability to issue formal requests for the removal of content, enforceable under a civil penalties scheme.[89]

The Online Safety Bill represents a welcome step in the right direction and brings real potential to stem the surge in online CSA and introduce much greater protections for children in the UK. Clearly its impact will need to be assessed following implementation. In its recent Strategic Review of Policing the Police Foundation called for the Bill to be built on as part of a step towards the creation of a more systemic approach to crime and harm prevention. This would encompass all industries whose goods or services introduce opportunities to perpetrate crime. This reach is especially important in the fast-moving technology sector that continuously creates new opportunities for criminal activity in online spaces. The aim of such an approach is to ensure there is clear accountability for crime prevention across government and new duties on the private sector. The Foundation has argued for a new national crime and harm prevention strategy that is genuinely cross governmental, a new national agency responsible for crime prevention (that would hold the responsibility for working with multi-national companies in an area like online CSA) and a new duty on private companies to prevent crime (The Police Foundation, 2022). All these measures would help to create a more systemic approach to the prevention of online CSA.

5.6 SUMMARY

This report has demonstrated that online CSA is perpetrated in such high volumes, that on its own law enforcement cannot be the answer. The growing volume of reported crimes and moreover, the high volume that go unreported, outstrip the capacity of the police to deliver a response equal to the scale of demand. This chapter has discussed the need for a much greater emphasis on prevention. This includes more education and awareness of the law and the available services to divert offenders (or would-be offenders) from these behaviours, more education of children and young people and frontline guardians to reduce vulnerabilities, and more use of targeted controls on digital environments to restrict offending. These different strands of intervention would suppress opportunities and close off entry-points to offending,

88. For example, see https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

89. https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions

with a view to diverting the least serious offenders, and drawing out the most motivated offenders for targeting by the police.

In the case of offenders, greater use could be made of targeted communications to deter offending in online spaces known to contain CSAM. There is a need to invest in technical capability and assets for monitoring offenders convicted of these offences, so that resources can be effectively directed towards risk and each police force operates to a common standard. Finally, greater investment in offender support and treatment services would expand capacity to respond to those reaching out for help. Furthermore, bolstered support services would provide credible, authoritative and well publicised information about the programmes available to guide people away from offending.

Education and awareness campaigns should aim to provide children with the knowledge to navigate the internet safely, through understanding the signs of grooming or exploitation. These campaigns should also target those young people who may be putting themselves at risk or posing a risk to others, by signposting them to support. Education must also help parents to provide effective guardianship in a changing online environment. Frontline police officers should receive more training in the advice they should be providing to children, parents and schools.

Finally, much more could be done to design out online CSA offending. Internet companies should be deploying the latest technologies for detecting online CSA on their sites but this varies considerably between companies because they have different levels of capability and operate from different countries that have established distinct public policies and laws. The Online Safety Bill is certainly a step in the right direction but it may need to be supplemented by reforms to ensure England and Wales take a more systemic approach to prevention at all levels, including a new duty on the private sector to prevent crime and a national agency with responsibility for crime and harm prevention.

6. CONCLUSION

It is time for a shift in our approach as a society to tackling online CSA. Its volume by far exceeds the capacity of law enforcement to respond, and reported online CSA continues to surge with the development of technology to detect these crimes and the introduction of more robust legislation to tackle these offenders.

More needs to be done to support the victims of online CSA, particularly the service they receive from the non-specialist local police teams who are generally responsible for engaging with them. Much more needs to be done to support the identification of victims depicted in CSAM so that they can be properly safeguarded. The law should be changed to avoid the criminalisation of the children and young people sharing images with each other and to support a consistent education-oriented approach.

Online CSA perpetrators are diverse in their behaviours, motivations and most importantly, the risk they pose to children. However, the response from the state to this volume crime has retained its focus on reactive criminal investigation by law enforcement agencies. The sheer volumes of non-first generation CSAM referrals mean that the police are unable to focus their resources on proactively going after the most serious offenders. In the face of demand that looks set to continue to rise, more sustainable strategies are needed, underpinned by the principles of overarching harm reduction.

This calls for crime control strategies that draw from a much wider set of organisations and sectors; to develop technological solutions to design out criminal opportunities, to raise awareness and deliver support to vulnerable children and young people, and to provide education and health interventions to divert would-be offenders away from criminality or prevent others from reoffending. There are undoubtedly serious and determined offenders for whom these strategies will never be enough, but the evidence indicates that a high proportion could be stopped at source or quickly diverted.

Doing more to prevent offending by the high volumes of low risk CSAM offenders would enable the police and the NCA to focus more resource on proactively going after the most serious offenders who pose the greatest risk to children.

REFERENCES

Alaggia, R., Collin-Vézina, D. and Lateef, R. (2017) Facilitators and Barriers to Child Sexual Abuse (CSA) Disclosures: A Research Update (2000–2016). *Trauma, Violence and Abuse* 20(2), pp.260-283.

Afilipoaie, A., and Shortis, P. (2018) *Crypto-Market Enforcement – New Strategy and Tactics*. Global Drug Policy Observatory.

American Psychiatric Association (APA) (2000) *Diagnostic and statistical manual of mental disorders DSM-IV-TR*. Washington DC: APA.

American Psychiatric Association (APA) (2013) *Diagnostic and statistical manual of mental disorders DSM-5.* Washington DC: APA.

Arthur, R. (2018) Consensual Teenage Sexting and Youth Criminal Records. *Criminal Law Review* 5, pp.381-387.

Asif, M. and Weenink, D. (2019) Vigilante rituals theory: A cultural explanation of vigilante violence. *European Journal of Criminology* 19(2), pp.163-182.

Babchishin, K.M., Hanson, R.K. and Hermann, C.A. (2011) The Characteristics of Online Sex Offenders: A Meta-Analysis. Sexual Abuse 23(1), pp. 92-123.

Babchishin, K.M., Hanson, R.K. and Van Zuylen, H. (2014) Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children. *Archives of Sexual Behaviour* 44*(1),* pp.45-66.

Bartlett, J. (2014) *The Dark Net*. New York: Melville House

Beckett, H., Warrington, C., Ackerley, E. and Allnock, D. (2015) *Children's voices research report. Children and young people's perspective on the police's role in safeguarding: A report for Her Majesty's Inspectorate of Constabularies*. Luton: University of Bedfordshire.

Beier, K., Neutze, J., Mundt, I. A., Ahlers, C. J., Goecker, D., Konrad and Schaefer, G.A (2009). Encouraging self-identified pedophiles and hebephiles to seek professional help: First results of the Prevention Project Dunkelfeld (PPD). *Child Abuse and Neglect*, 33(8), pp.545-549.

Beier, K.M., Grundmann, D., Kuhle, L.F., Scherner, G., Konrad, A. and Amelung, T. (2014) The German Dunkelfeld Project: A pilot study to prevent child sexual abuse and the use of child abusive images. *The Journal of Sexual Medicine* 12(2) pp.529–542.

Bourke, M. and Hernandez, A. (2008) The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. *Journal of Family Violence* 24(3), pp.183–191.

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014) Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology* 8(1), pp.1-20.

Broadhurst, R. G. (2019) Child Sex Abuse Images and Exploitation Materials, in R. Leukfeldt and T. Holt(eds) *Handbook of Cybercrime.* Abingdon: Routledge, (pp 310-336).

Brown, C. (2015) Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9(1), pp.55-119.

Burgess, M. (2019) Inside the messy collapse of the Uks unworkable porn block. *Wired,* [online] 23 October. Available at: <https://www.wired.co.uk/article/uk-porn-ban-digital-economy-act> [Accessed 16 June 2022].

Burns, C.M., Morley, J., Bradshaw, R. and Domene, J., (2008) The emotional impact on and coping strategies employed by police teams investigating internet child exploitation. *Traumatology* 14(2), pp.20-31.

Carr, J. (2017) A brief history of child safety online: Child abuse images on the internet. *In* J. Brown (eds) *Online Risk to Children: Impact, Protection and Prevention*. Chichester: NSPCC/Wiley.

CEOP (2013) *Threat Assessment of Child Sexual Exploitation and Abuse*. London: CEOP.

Chatterton, M. (2008) *Losing the detectives: Views from the frontline*. Surrey: Police Federation of England and Wales.

Childwise, (2020) *The Monitor Report 2020: Child's media use, purchasing, attitudes and activities*. Norwich: Childwise.

Clutton, S. and Coles, J. (2007) *Sexual exploitation risk assessment framework: A pilot study*. Ilford: Barnardos.

Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44(4), pp. 588-608.

College of Policing (2016) Briefing note: Police action in response to youth produced sexual imagery ('Sexting').

College of Policing (2019) *Supporting the wellbeing of Internet Child Abuse Teams (ICAT): Introduction and guidance*. Ryton on Dunsmore: College of Policing.

Cornish, D.B. and Clarke R.V. (2003) Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *In* M.J, Smith and D.B., Cornish DB (eds) T*heory for practice in situational crime prevention. Crime Prevention Studies no. 16*. Monsey, NY: Criminal Justice Press pp.41–96.

Coward, A. I., Gabriel, A. M., Schuler, A., and Prentky, R. A. (2009) Child internet victimization: Project development and preliminary results. Poster presented at the American Law Society Conference, San Antonia, Texas.

Craun, S.W., Bourke, M.L. and Coulson, F.N. (2015) The impact of internet crimes against children work on relationships with families and friends: An exploratory study. *Journal of Family Violence* 30(3), pp.393-402.

Craven, S., Brown, S. and Gilchrist, E. (2007) Current Responses to Sexual Grooming: Implication for Prevention. *The Howard Journal of Crime and Justice* 46(2), pp.60-71.

Crowhurst, L. (2017) *Reforming justice for the digital age*. London: The Police Foundation.

Crown Prosecution Service (CPS) (2019) *Violence Against Women and Girls Report 2018–19*. London: CPS.

Davidson, J., Martellozzo, E. and Lorenz, M., (2009) *Evaluation of CEOP ThinkUKnow internet safety programme and exploration of young people's internet safety knowledge*. London: Kingston University

Davidson, J. and Gottschalk, P. (2011) Characteristics of the internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies* 21(1), pp.23-36.

Davidson, J., DeMarco, J., Bifulco, A., Bogaerts, S., Caretti, V., Aiken, M., Cheevers, C., Corbari, E., Scally, M., Schilder, J., Schimmenti, A., Puccia, A. (2016) *Enhancing Police and Industry Practice: EU Child Online Safety Project*. London: Middlesex University.

Davis, A. (2018) New Technology to Fight Child Exploitation. *Meta*, [online] 24 October. Available at: <https://about.fb.com/news/2018/10/fighting-child-exploitation/> [Accessed 16 June 2022].

Department for Education (2017) *Child sexual exploitation: Definition and a guide for practitioners, local leaders and decision makers working to protect children from child sexual exploitation*. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591903/CSE_Guidance_Core_Document_13.02.2017.pdf> [Accessed 16 June 2022].

Dombert, B., Schmidt, A.F., Banse, R., Briken, P., Hoyer, J., Neutze, J. and Osterheider, M. (2016) How Common is Men's Self-Reported Sexual Interest in Prepubescent Children? *The Journal of Sex Research* 53(2) pp.214-223.

Elliott, I.A., Beech, A.R. and Mandeville-Norden, R. (2012) The psychological profiles of internet, contact, and mixed internet/contact sex offenders. *Sexual Abuse* 25(3).

Elliott, I., Thomas, S., and Ogloff, J. (2014) Procedural justice in victim-police interactions and victims' recovery from victimisation experiences. *Policing and Society* 24(5), pp: 588-601.

Elliott, I. A., Mandeville-Norden, R., Rakestrow-Dickens, J., and Beech, A. R. (2019) Reoffending rates in a U.K. community sample of individuals with convictions for indecent images of children. *Law and Human Behavior* 43(4), pp.369–382.

Europol (2019) *Internet organised crime threat assessment.* The Hague: Europol.

Europol (2020) *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*. The Hague: Europol.

Felson M (2003) The process of co-offending. *In*: M.J., Smith, D.B, Cornish (eds) *Theory for practice in situational crime prevention, vol 16*. Devon: Willan Publishing, pp 149–168.

Finkelhor, D. (1986) *A Sourcebook on Child Sexual Abuse*. London: Sage Publishing.

Finkelhor, D. (2009) The prevention of childhood sexual abuse. *The Future of Children* 19(2), pp.169-194.

Firmin, C., Warrington, C. and Pearce, J. (2016) Sexual Exploitation and Its Impact on Developing Sexualities and Sexual Relationships: The Need for Contextual Social Work Interventions. *The British Journal of Social Work* (2016) 46(8), pp.2318–2337.

Flood, M. (2009) The Harms of Pornography Exposure Among Children and Young People. *Child Abuse Review* 18(6) pp.384–400.

Franqueira, V. N. L., Bryce, J., Al Mutawa N. and Marrington, A. (2017) Investigation of Indecent Images of Children cases: Challenges and suggestions collected from the trenches, *Digital Investigation* 24, pp.95-105.

Gillespie, A.A. (2004) Tackling grooming. *The Police Journal* 77(3), pp.239-255.

Gillespie, A.A. (2008) Cyber-stings: Policing sex offences on the internet. The Police Journal 81(3), pp.181-183.

Hales, G. (2018) *A 'sexting' surge or a conceptual muddle? The challenges of analogue law and ambiguous crime recording*. London: The Police Foundation.

Halford, E., Dixon, A., Farrell, G., Malleson, N. and Tilley, N. (2020) Crime and coronavirus: social distancing, lockdown, and the mobility elasticity of crime. *Crime Science* 9(11), pp.1-12.

Hamilton-Giachritsis, C., Hanson, E., Whittle, H. and Beech, A. (2017) *("Everyone deserves to be happy and safe": A mixed methods study exploring how online and offline child sexual abuse impact young people and how professionals respond to it*. Available at: <https://learning.nspcc.org.uk/media/1123/impact-online-offline-child-sexual-abuse.pdf> [Accessed 16 June 2022].

HM Government (2018) *Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children*. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uplaods/attachment_data/file/779401/Working_Together_to_Safeguard-Children.pdf> [Accessed 16 June 2022].

HM Government (2020) *Online Harms White Paper*. Available at: <https://www.gov.uk/government/consultations/online-harms-white-paper/online harms-white-paper> [Accessed 16 June].

HM Government (2021) *Tackling Child Sexual Abuse Strategy*. Available at: <https://www.gov.uk/government/publications/tackling-child-sexual-abuse-strategy> [Accessed 16 June 2022].

HM Government (2022) Police recorded crime and outcomes: open data tables. Available at: <https://www.gov.uk/government/statistics/police-recorded-crime-open-data-tables> [Accessed 7 July 2022].HMIC (2015) *Online and on the Edge: Real risks in a virtual world. An inspection into how forces deal with the online sexual exploitation of children*. London: HMIC.

Home Affairs Committee (2018) *Policing for the future: Tenth Report of Session 2017–19, CP 62*.`London: HMSO. Home Affairs Committee (2020) *Oral evidence: Home Office preparedness for Covid-19 (Coronavirus), HC 232*. London: House of Commons.

Home Office (2004) *Children and Families: Safer from Sexual Crime. The Sexual Offences Act 2003*. London: Home Office.

Home Office (2010) Child Exploitation and Online Protection Centre (CEOP): The way forward. Available at: <https://www.gov.uk/government/publications/child-exploitation-and-online-protection-centre-the-way-forward> [Accessed 16 June 2022].

Howitt, D. and Sheldon, K. (2007) The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared. *Psychology, Crime, & Law*, 13(5), pp.469-486.

Hurley, R., Prusty, S., Soroush, H., Walls, R. J., Albrecht, J., Cecchet, E. (2013) Measurement and analysis of child pornography trafficking on P2P networks. *In Proceedings of the 22nd International Conference on World Wide Web*. Rio De Jeneiro, Brazil, 13-17 May, 2013. New York: ACM, pp. 631–642.

Independent Inquiry Child Sex Abuse (2020) *The internet: Investigation report*. Accessed at: <https://www.iicsa.org.uk/publications/investigation/internet/executive-summary> [Accessed 16 June 2022].

INHOPE Association (2019) *Annual report, 2018*. Amsterdam: INHOPE. Available at: <https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/39761566299-1591885517/2019.12.13_ih_annual_report_digital.pdf> [Accessed 16 June 2022].

INHOPE Association (2021) *Annual Report 2020*. Amsterdam: INHOPE. Available at: <https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf> [Accessed 16 June 2022].

Innes, M. and Sheptycki, J. (2004) From detection to disruption: Intelligence and the changing logic of police crime 1-24 control. *International Criminal Justice Review* 14(1), pp.1-24.

Internet Watch Foundation (2018) *The Annual Report: Once Upon a Year*. Available at: <https://www.iwf.org.uk/report/2018-annual-report> [Accessed 16 June 2022].

Internet Watch Foundation (2020) *The Annual report 2019: Zero Tolerance*. Available at: <https://www.iwf.org.uk/sites/default/files/reports/2020-04/IWF_Annual_Report_2020_Low-res-Digital_AW_6mb.pdf> [Accessed 16 June 2022].

Internet Watch Foundation (2022) *The Annual Report 2021*. Available at: <https://annualreport2021.iwf.org.uk/> [Accessed 16 June 2022].

Joffres, K., Bouchard, M., Frank, R. and Westlake, B.G. (2011) Strategies to Disrupt Online Child Pornography Networks. *European Intelligence and Security Informatics Conference, EISIC 2011*, Athens, Greece, September 12-14, 2011.

Justice (2019) *Prosecuting sexual offences*. London: Justice.

Kirby, S. and Penna, S. (2010) Policing mobile criminality: Towards a situational prevention approach to organised crime. *In* K.,Bullock, R.V.,Clarke and N.,Tilley (eds) *Situational prevention of organised crimes.* Cullopton: Willan.

Kleemans, E. and van de Bunt, H. (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(1), pp.19-36.

Kleemans, E. and de Poot, C. (2008) Criminal careers in organised crime and social opportunity structure. *European Journal of Criminology* 5(1), pp 69-98.

Kloess, J.A., Woodhams, J., Whittle, H., Grant, T. and Hamilton-Gilchrist, C.E. (2017) The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse* 31(2), pp.173-196.

Leary, M. G. (2010) Sexting or self-produced child pornography? The dialog continues – structured prosecutorial discretion within a multidisciplinary response. *Virginia Journal of Social Policy and the Law* 487, pp.566.

Leukfeldt, E.R., Jansen, J. and Stol, W.P. (2014) Child pornography, the Internet and juvenile suspects. *Journal of Social Welfare and Family Law* 36(1), pp.3-13.

Leukfeldt, E.R. and Yar, M. (2014) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior* 37(3) pp. 263–280.

Leukfeldt, R., Kleemans, E., Kruisbergen, E. and Roks, R. (2017) Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime Law and Social Change* 67(1) pp. 39-53.

Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2015) *The Implications of Economic Cybercrime for Policing*. London: City of London Corporation.

Long, M., Alison, L., Tejeiro, R., Hendricks, E. and Giles, S. (2016) KIRAT: Law Enforcement's Prioritization Tool for Investigating Indecent Image Offenders. *Psychology, Public Policy, and Law* 22(1), pp.12-21.

Liberatore, M., Erdely, R., Kerle, T., Levine, B.N. and Shields, C. (2010) Forensic investigation of peer-to-peer file sharing networks. *Digital Investigation* 7(1), pp.95-103.

Livingstone, S. (2017) Children and young people's lives online. *In* J. Brown (ed) *Online risk to Children: Impact, Protection and Prevention.* Chichester: Wiley.

The Lucy Faithfull Foundation (2019) *We're working to protect children: Annual Report & Financial Statements 2018/19*. Available at: <https://www.lucyfaithfull.org.uk/files/LFF_Annual_Report_2018_2019.pdf> [Accessed 16 June].

Martellozzo, E. (2015) Policing online child sexual abuse – the British experience. *European Journal of policing Studies*, 3 (1) pp. 32-52.

Martellozzo, E., Monaghan, A., Adler, J.R., Davidson, J., Leyva, R. and Horvath, M.A.H. (2016) *I wasn't sure it was normal to watch it*. London: NSPCC.

Martin. J. (2014) ("It's Just an Image, Right?": Practitioners' Understanding of Child Sexual Abuse Images Online and Effects on Victims. *Child & Youth Services* 35(2) pp.96–115.

Martin J. (2015): Conceptualizing the Harms Done to Children Made the Subjects of Sexual Abuse Images Online. *Child & Youth Services*. 36(4), pp.267-287.

May-Chahal, C. and Palmer, E. (2018) *Rapid Evidence Assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation*. Lancaster: Lancaster University.

McCartan, K.F., Merdian, H.L., Perkins, D.E. and Kettleborough, D. (2018) Ethics and Issues of Secondary Prevention Efforts in Child Sexual Abuse. *International Journal of Offender Therapy and Comparative Criminology*. 62(9), pp.2548-2566.

McGeeney, E. and Hanson, E. (2017) Digital Romance: *A research project exploring young people's use of technology in their romantic relationships and love lives*. London: CEOP.

McGuire, M. (2012) *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security.

McGuire, M. and Dowling, S. (2013) *Cyber crime: A review of the evidence. Research Report 75. Summary of key findings and implications*. London: Home Office.

McManus, M., Long, M.L., Laurence, A. and Almond, L. (2015) Factors associated with contact child sexual abuse in a sample of indecent image offenders. *Journal of Sexual Aggression*. 21(3), pp.368-384.Mokros, A. and Banse, R. (2019) The ("Dunkelfeld" Project for Self-Identified Pedophiles: A Reappraisal of its Effectiveness. *Journal of Sexual Medicine*. 16(5) pp.609-613.

Ministry of Justice (2012) Sexual Offences Guideline Consultation. Available at: <https://consult.justice/gov/uk/sentencing-council/indecent-images-children/supporting_documents/Guidelines_Indecent%20images%20of%20children.pdf> [Accessed 7 July 2022].

National Crime Agency (2018) Supplementary written evidence submitted by the National Crime Agency (NCA) (PFF0011). Available at: <http://data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Home%20Affairs/Policing%/20%for%20the%20future/written/82068.html> [Accessed 16 June 2022].

National Crime Agency (2019) *National strategic assessment of serious and organised crime*. London: NCA.

National Crime Agency (2020) *National strategic assessment of serious and organised crime*. London: NCA.

National Crime Agency (2021) *National strategic assessment of serious and organised crime*. London: NCA.

NSPCC (2016) *What should I do? NSPCC helplines: responding to children's and parents' concerns about sexual content online*. NSPCC [online]. Available at: <https://learning.nspcc.org.uk/research-resources/2016/what-should-i-do-nspcc-helplines-report-online-safety> [Accessed 16 June 2022].

NSPCC (2020) *The impact of the coronavirus pandemic on child welfare: online abuse*. London: NSPCC. Available at: <https://learning.nspcc.org.uk/research-resources/2020/coronavirus-insight-briefing-online-abuse> [Accessed 6 July 2022]

Nurse, J. and Bada, M. (2019) The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. *In* A. Attrill-Smith, C. Fullwood, M. Keep and D.J. Kuss (eds) *The Oxford Handbook of Cyberpsychology*. Oxford University Press.

Odinot, G., Verhoeven, M., Pool, R. and de Poot, C. (2017) *Organised Cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC.

Ofcom (2020) *Children and Parents: Media use and attitudes report 2019*. London: Ofcom. Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf> [Accessed 16 June 2022].

Office for National Statistics (ONS) (2020) Child sexual abuse in England and Wales: year ending March 2019. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/childsexualabuseinenglandandwales/yearendingmarch2019> [Accessed 16 June 2022].

Ogas, O., and Gaddam, S. (2012) *A billion wicked thoughts: What the internet tells us about sexual relationships*. New York, NY: Plume.

Ospina, M., Harstall, C. and Dennett, L. (2010) Sexual exploitation of children and youth over the internet: A Rapid Review of the Scientific Literature. Alberta: Institute of Health Economics.

Osterday, M. (2016) Protecting minors from themselves: Expanding revenge porn laws to protect the most vulnerable. *Indiana Law Review* 49(2),

Palmer, T. (2015) *Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people*. Ilford: Barnardo's.

The Police Foundation (2022) *A new mode of protection: Redesigning policing and public safety for the 21st century*. London: The Police Foundation.

Powell, M., Cassematis, P., Benson, M., Smallbone, S. and Wortley, R. (2015) Police officers' perceptions of their reactions to viewing internet child exploitation material. *Journal of Police and Criminal Psychology* 30(2), pp.103-111.

Plummer, C. and Klein, A., (2013) *Using policies to promote child sexual abuse prevention: What is working*. Harrisburg, PA: VAWnet

Quayle, E., and Taylor, M. (2002) Child pornography and the internet: Perpetuating a cycle of abuse. *Deviant Behavior* 23(4), pp.331–361.

Radford, L., Corral, S., Bradley, C., Fisher, H., Bassett, C., Howat, N. and Collishaw, S. (2011) *Child abuse and neglect in the UK today*. London: NSPCC.

Snell, E. (2016) Policing Cybercrime. *Computer Weekly*

Seto, M. (2010) Child pornography use and internet solicitation in the diagnosis of pedophilia. *Archives of Sexual Behavior* 39(3), pp.591–593.

Seto, M., Hanson, R.K. and Babchishin, K.M. (2011) Contact sexual offending by men with online sexual offenses. *Sexual Abuse* 23(1) pp.124.

Seto, M. C., and Eke, A. W. (2015) Predicting Recidivism Among Adult Male Child Pornography Offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and Human Behavior* 39(4), pp.416–429.

Seto, M., Buckman, C., Dwyer, G. and Quayle, E. (2018) *Production and active trading of child sexual exploitation images depicting identified victims* NCMEC & Thorn Research Report.

Silke, A. (2001) Dealing with vigilantism: Issues and lessons for the police. *The Police Journal: Theory, Practice and Principles* 74(2).

Skidmore, M., Goldstraw-White, J. and Gill, M. (2020) Understanding the police response to fraud: the challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management Volume* 40(5).

Smallbone, S. and Wortley, R. (2017) Preventing child sexual abuse online. In J. Brown (eds) *Online Risk to Children: Impact, Protection and Prevention*. Chichester: NSPCC/Wiley.

Sorell, T. (2017) Online Grooming and Preventive Justice. *Criminal Law and Philosophy* 11(4) pp.705–724.

Soudjin, M. and Zegers, B. (2012) Cybercrime and virtual offender convergence settings. *Trends in Organized Crime* 15(2-3), pp.111-129.

Steel, C.M.S. (2009) Child pornography in peer-to-peer networks. *Child Abuse& Neglect* 33(8), pp.560–568.

Suler, J. (2004) The Online Disinhibition Effect. *CyberPsychology & Behavior.* 7(3), pp.321-6.

Taylor, M., & Quayle, E. (2003) *Child pornography: An Internet crime.* Hove, UK: Brunner Routledge.

Tehrani, N., (2016) Extraversion, neuroticism and secondary trauma in internet child abuse investigators. *Occupational Medicine*, 66(5) pp.403-407.

Tener, D., Wolak, J. and Finkelhor, D. (2015) Typology of Offenders Who Use Online Communications to Commit Sex Crimes Against Minors. *Journal of Aggression, Maltreatment & Trauma* 24(3) pp.319–337.

Thibaut, F., Bradford, J.M.W., Briken, P., De La Barra, F., Häßler, F., Cosyns, P. and Cosyns, P. (2016) The World Federation of Societies of Biological Psychiatry (WFSBP) guidelines for the treatment of adolescent sexual offenders with paraphilic disorders. *World Journal of Biological Psychiatry* 17(1) pp.2–38.

Tremblay, P. (2006) Convergence settings for non-predatory "boy lovers". *Crime Prevention Studies* 19 pp.145-168.

Trottier, D. (2015) Digital Vigilantism as Weaponisation of Visibility. *Philosophy & Technology* 30(1) pp.55-72.

UK Parliament (2022) Online Safety Bill. Available at: <https://bills.parliament.uk/bills/3137/publications> [Accessed 16 June 2022].

United Nations Office on Drugs and Crime (2015) *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. New York: UNODC.

Vannucci, A., Simpson, E.G., Gagnon, S. and Ohannessian, C.M. (2020) Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence* 79, pp.258-274.

Vendius, T.T. (2015) Proactive Undercover Policing and Sexual Crimes against Children on the Internet. *The European Review of Organised Crime* 2(2), pp.6-24.

Wager, N., Armitage, R., Christmann, K., Gallagher, B., Ioannou, M., Parkinson, S., Reeves, C., Rogerson, M. and Synnott, J. (2018) *Rapid Evidence Assessment: Quantifying the Extent of Online-Facilitated Child Sexual Abuse*. Report for the Independent Inquiry into Child Sexual Abuse.

Wall, D. (2015) Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime* 2(2), pp.71-90.

Wall, D. and Williams, M. (2007) Policing diversity in the digital age: Maintaining order in virtual communities. Criminology and Criminal Justice 7(4), pp.391-415.

Webster, S., Davidson, J., & Bifulco, A. (2014) *Online offending behaviour and child victimisation: New findings and policy*. Basingstoke: Palgrave Macmillan.

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. and Craparo, G. (2012) *European online grooming project: Final report*.

Wedlock, E. and Tapley, J. (2016) *What works in supporting victims of crime: A rapid evidence assessment*. London: Victims' Commissioner.

Wells, M., Finkelhor, D., Wolak, J. and Mitchell, K.J. (2007) Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession. *Police Practice and Researc*h 8(3), pp.269-282.

Westlake, B. and Bouchard, M. (2016) Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research* 59 pp.23-36.

Whittle, H. C., Hamilton-Giachritsis, C., Beech, A. and Collings, G. (2013) A Review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior* 18(1), pp.62-70.

Whittle, H. C. and Hamilton-Giachritsis, C. (2017) Offender behaviour. In J. Brown (eds) *Online Risk to Children: Impact, Protection and Prevention*. Chichester: NSPCC/ Wiley.

Wildsmith E, Barry M, Manlove J, Vaughn B. (2013) Adolescent health highlight: Dating and sexual relationships. *Child Trend*s. Available at: <https://www.childtrends.org/publications/dating-and-sexual-relationships> Accessed: 16 June 2022.

Wolak, J., Finkelhor, D. and Mitchell, K.J. (2005) *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study*. Virginia: National Center for Missing and Exploited Children.

Wortley, R. and Smallbone, S. (2006) Introduction. *In* R. Wortley and S. Smallbone (eds) *Situational Prevention of Child Sexual Abuse* pp. 1–6. New York: Criminal Justice Press.

Wortley, R. (2012) Situational prevention of child abuse in the new technologies. *In* K. Ribisl & E. Quayle *Preventing Online Exploitation of Children*. London: Routledge.

Yip, M., Shadbolt, N., and Webber, C. (2012) *Structural analysis of online criminal social networks. IEEE International Conference on Intelligence and Security Informatics* (ISI), Arlington, US, 10-13 June 2012, pp.60–65.

Zonana, H. (2011) Sexual Disorders: New and Expanded Proposals for the DSM-5 - do We Need Them? Journal of the American Academy of Psychiatry and the Law. 39(2) pp.245-9.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank