INDEPENDENT INQUIRY
CHILD SEXUAL ABUSE

The Internet

Investigation Report

March 2020

2020

The Internet

Investigation Report
March 2020

A report of the Inquiry Panel
Professor Alexis Jay OBE
Professor Sir Malcolm Evans KCMG OBE
Ivor Frank
Drusilla Sharpling CBE

Any enquiries related to this publication should be sent to us at contact@iicsa.org.uk or Freepost IICSA INDEPENDENT INQUIRY.

This publication is available at https://www.iicsa.org.uk/reports

CCS0220114914 03/20

Printed on paper containing 75% recycled-fibre content minimum.

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty’s Stationery Office.

Contents

Executive Summary

This investigation focusses on the growing problem of online-facilitated child sexual abuse. The increase in access to and use of the internet has brought undeniable benefits to society. It has also enabled a section of society to misuse the internet to distribute indecent images of children; groom and manipulate children in order to commit sexual acts on them; and live stream the sexual abuse of children from around the world.

The harm done to children and their families is incalculable. We heard evidence from victims and their families about the devastating and long-term impact that this abuse has on them. Those affected live in fear that images of them being sexually abused remain available on the internet. Parents described their children being groomed as "*any parent's nightmare*".[1]

Scale of online-facilitated child sexual abuse

There are millions of indecent images of children in circulation worldwide. The word 'indecent' describes a spectrum of offending, some of which reaches unprecedented levels of depravity and includes the rape and torture of babies and toddlers. Although the dark web often hosts images of the most deviant kind, the vast majority of sites that host indecent images of children are available on the open web and potentially accessible to a worldwide audience.

In 2015, BT found that "*the average number of attempts to retrieve the CSA image was 36,738 every 24 hours*".[2] Extrapolate that data across all the internet service providers, and the number of attempts to access indecent images of children per day is alarmingly high.

Several police forces reported a rise in offences of online grooming. According to the National Society for the Prevention of Cruelty to Children (NSPCC), between April and September 2018, police recorded more than 10 grooming offences a day. Facebook, Instagram and Snapchat are frequently named as the most common platforms where grooming takes place.

It is wrong to assume that the live streaming of child sexual abuse does not involve children from the UK. The Internet Watch Foundation (IWF) frequently encounters images of live streams which involve children from Western backgrounds, the majority of whom are girls aged between seven and 13 years old. The sums paid to watch and in some cases direct the abuse are trivial, sometimes costing little more than one pound, thereby offering encouragement to would-be offenders to engage in child sexual abuse on a significant scale.

The true scale of offending and the number of children who have been victims of online-facilitated child sexual abuse is likely to be far higher than the number of reported offences.

The volume of online child sexual abuse and exploitation offences referred to law enforcement undoubtedly "*represents a broader societal failure to protect vulnerable children*".[3]

[1] MCF000007_009
[2] Kevin Brown 17 May 2019 20/5-7; 'CSA' means child sexual abuse.
[3] OHY002229_004-005

This investigation examined the response of law enforcement, industry and government to online-facilitated child sexual abuse by considering the response to three types of offending: indecent images of children offences; the grooming of a child; and live streaming of child sexual abuse.

Indecent images of children

There have been significant efforts by internet companies to detect indecent images of children on their platforms and services. The development of PhotoDNA in 2009 greatly increased the ability of internet companies to detect known (ie previously identified) child sexual abuse imagery. Other technological developments now exist to identify newly created or previously unidentified indecent images and videos.

The IWF has made remarkable progress in removing child sexual abuse material from web addresses that are hosted in the UK. When the IWF was set up in 1996, the UK hosted 18 percent of the worldwide total of online child sexual abuse imagery. By 2018, the figure was 0.04 percent.

The increase in detection and the removal of indecent images is important but this does not address the issue of ease of access to this imagery. It is still possible to access indecent images of a child from common search engines in only "*three clicks*".[4] The internet companies must do more to pre-screen material before it is uploaded to their platforms and systems. The Inquiry considers that preventing a user from accessing child sexual abuse material is a vital and necessary step in the fight against possession and distribution of indecent images of children.

Online grooming

There has been a rapid escalation in the number of children being groomed on the internet and, in particular, on social media platforms. Most internet companies either prohibit or discourage children under 13 years old from accessing their platforms or services.

However, we repeatedly heard evidence that children under 13 easily gained access to their services and that under 13-year-olds, especially girls, are at significant risk of being groomed. The internet companies failed to demonstrate that they were fully aware of the scale of underage use. The lack of a comprehensive plan from industry and government to combat this problem should be urgently addressed.

The Inquiry heard that collaboration between industry, law enforcement and government has resulted in a number of technological developments that help detect grooming. However, the Inquiry is not confident that internet companies are doing all they could to tackle online grooming on their platforms. More needs to be done than simply deploying existing technologies, many of which will not work where communication is encrypted. Encryption poses a real risk to the ability of law enforcement to detect and investigate online-facilitated child sexual abuse.

[4] NCA000376_003

Live streaming of child sexual abuse

The institutional response to live streaming is not as well developed as the responses to the grooming of children and the possession and distribution of indecent images of children. The ability of industry and law enforcement to detect child sexual abuse that is being live streamed is difficult given the real-time nature of the broadcast. The use of human moderators to monitor live streams is therefore a key feature of the response. We are unconvinced that internet companies fully understand the scale of the problem of live streaming on their platforms such that they can properly assess whether they employ sufficient numbers of moderators to detect such offending.

The response of industry and government

We repeatedly heard evidence from industry witnesses that their respective companies were committed to trying to prevent online-facilitated child sexual abuse. Industry's response was, at times, reactive and seemingly motivated by the desire to avoid reputational damage caused by adverse media reporting. Transparency reports published by the internet companies provide only part of the picture and there is a lack of guidance and regulation setting out the information that must be provided.

The government response includes the introduction in September 2020 of compulsory education in both primary and secondary schools that will help teach children about the need to stay safe online. The government also published its *Online Harms White Paper* aimed at tackling a wide range of online harms, including the threat of online child sexual abuse and exploitation. The Queen's Speech in December 2019 included reference to the introduction of legislation to establish a new regulatory framework. The Online Harms proposals are wide-ranging but the timetable for implementation of this legislation is unclear. The prospective interim code of practice in respect of child sexual abuse and exploitation offers a very real opportunity to make children in the UK safer online. We therefore unhesitatingly recommend that the interim code is published without further delay.

This recommendation, along with the Inquiry's other recommendations, aims to encourage greater collaboration between industry, law enforcement and government to put in place a strengthened and more rigorous regime to address the harm caused by online-facilitated child sexual abuse.

Recent cases

Operation 'C'[5]

In 2016, a local secondary school reported to West Midlands Police that there were images on the internet of one of their male pupils performing oral sex on another male. The police identified a social media account that was being used to distribute the images and a physical address linked to that account. The address was searched. A man in his 20s handed himself in to police. In his police interview, the offender admitted that he had set up a fake social media account posing as a female. He accepted that he had exchanged messages with the victim, including exchanging indecent images, which led to the meeting where he captured the victim performing oral sex on him. He denied setting up any other fake profiles and said he had only ever spoken to one other person using his fake account.

When West Midlands Police analysed his computer, they found a number of other fake female profiles and a large number of indecent images of young men. The offender followed a consistent pattern whereby he would befriend the victim using his fake female social media profile, encourage them to send indecent images to him and then use those images to blackmail them into meeting him and performing sexual acts. The police identified 45 victims. The offender pleaded guilty to 32 offences and was sentenced to 22 years' imprisonment.

Case 1

In 2017, Gwent Police received intelligence that a suspect was actively sharing files containing indecent images of children. Police obtained a search warrant, seized a number of devices from the address and arrested the suspect. During a police interview, he admitted downloading indecent images of children and in due course pleaded guilty to indecent image offences involving possessing a total of 158 indecent images of children. He was sentenced to a 12-month suspended sentence.

As part of their public protection duties, the police conducted a number of safeguarding assessments and spoke to members of his family. As a result, two victims, both aged under 13, reported that they had been sexually abused by the offender. In respect of the sexual contact offences, he was sentenced to 10 years' imprisonment.[6]

Richard Huckle

In 2016, Richard Huckle was sentenced to life imprisonment and was ordered to serve a minimum of 25 years for 71 offences of child sexual abuse.[7] Huckle was a UK national who pleaded guilty to sexually abusing 22 children in Malaysia and one in Cambodia. His victims were 13 years old or younger and included a baby estimated to be six months old. He captured images of this abuse and posted it online on the dark web, advertising this material

[5] OHY003315_021-022

[6] OHY003305_009-010

[7] NCA000163_052-053

for sale. When arrested, his computer devices were encrypted.[8] Once the encryption was broken, police found that Huckle had kept a scorecard awarding points per victim depending on the nature and seriousness of the sexual act he committed.[9]

Mathew Law

In December 2018, Mathew Law was sentenced to 15 years' imprisonment[10] for his role in a conspiracy to rape a seven-month-old baby.[11] Law was part of a 'paedophile gang', who communicated with each other privately using encrypted communication methods and the dark web. Other members of this network received sentences ranging from two to 24 years' imprisonment.

Law was convicted earlier, in 1999, of possessing and distributing indecent images of children and received a sentence of 15 months' imprisonment.

[8] Encryption is the process of converting information or data into a code that makes it unreadable to unauthorised parties.
[9] On 13 October 2019, Huckle was found dead in his prison cell. Another inmate has since been charged with his murder.
[10] The Court also extended Law's period spent on licence by five years.
[11] https://www.theguardian.com/uk-news/2018/dec/20/paedophile-gang-member-mathew-law-jailed-for-20-years

Part A

Introduction

Introduction

A.1: The background to the investigation

1. There are an estimated 14 million children under the age of 18 in the United Kingdom. Millions of those children regularly use the internet and enjoy the benefits of easy access to information and near instantaneous communication that the internet provides. At the same time, those children are potentially being exposed to perpetrators who commit online-facilitated sexual offences.

2. In 2018, Ofcom reported that:[12]

- more than half of three and four-year-olds spent nearly nine hours a week online, and 19 percent had access to their own tablet;
- 93 percent of eight to 11-year-olds spent about 13½ hours a week online, 35 percent had their own smartphone and 47 percent had their own tablet; and
- 99 percent of 12 to 15-year-olds spent 20½ hours online per week, 50 percent had their own tablet and 83 percent had their own smartphone.

3. The internet has created opportunities for sexual offending against children. It enables perpetrators to view images of a child being sexually abused (also referred to as indecent images of children). The number of indecent images in circulation is in the many millions.

4. The internet is also used to groom children. Grooming includes building a relationship with a child in order to gain their trust for the purposes of sexual abuse or exploitation. This can include forcing, manipulating or enticing a child to engage in sexual activity, either with themselves or with other children. These acts are then often live streamed and images taken of the footage. The move from establishing online contact with a child to meeting them in person and physically sexually abusing them can happen quickly.[13]

5. The Inquiry's Rapid Evidence Assessment (REA)[14] *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation* indicates that perpetrators are predominantly men from white or European backgrounds, with online offenders "*less likely to have criminal backgrounds, previous convictions or prior anti-social histories than contact offenders*".[15] In 2015, the National Society for the Prevention of Cruelty to Children (NSPCC) estimated that over half a million men had viewed indecent images of children.[16] UK law enforcement estimated that, in 2016, there may have been as many as 100,000 people in the UK involved in the downloading and sharing of child sexual abuse images.[17]

[12] Ofcom, *Children and parents: Media use and attitudes report 2018* p3

[13] Rapid Evidence Assessment: *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation* p45; INQ004149_006

[14] A Rapid Evidence Assessment (REA) is a review which gives an overview of the amount and quality of evidence on a particular topic as comprehensively as possible within a set timetable.

[15] Rapid Evidence Assessment: *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation* p10

[16] NCA000207_019

[17] NCA000163_019

6. It would be wrong to assume, however, that online-facilitated child sexual abuse is an exclusively male phenomenon. For example:

- In 2009, nursery worker Vanessa George pleaded guilty to a number of sexual offences against children and making, possessing and distributing indecent images. The images of the abuse she committed were sent to two other offenders whom she had met on Facebook.[18]
- More recently, in August 2019, Jodie Little was jailed for 12 years and four months for sexually abusing a boy and a girl both aged under 13. She recorded the abuse and sold it on the internet.[19]

7. Child sexual abuse imagery has become ever more depraved and the victims ever younger. From April 2018 to March 2019, police in England, Wales and Northern Ireland recorded 7,618 sexual offences against children aged between four and eight years old.[20] Law enforcement frequently encounter images of babies and toddlers being raped by adult males and children being sexually tortured.

8. The growing scale of child sexual abuse, including access to the most horrific and depraved indecent images, is facilitated by the internet. The offending is such that online child sexual abuse and exploitation is recognised by the UK government to be "*a national security threat*",[21] with reports about the volume, severity and complexity of the online threat being made to the National Security Council.[22]

9. It is against this background that the Independent Inquiry into Child Sexual Abuse has examined the institutional responses to online-facilitated child sexual abuse.

A.2: Scope of the investigation

10. As set out in the definition of scope,[23] this investigation examined the nature and extent of the use of the internet to facilitate child sexual abuse, including by sharing indecent images of children, viewing or directing the abuse of children via online streaming or video conferencing, and grooming or otherwise coordinating contact offences against children. It also considered the experiences of victims and survivors of child sexual abuse facilitated by the internet, and the adequacy of the response of government, law enforcement and the internet industry to child sexual abuse facilitated by the internet.

11. The Inquiry is aware that the protection of those using the internet is an area of ongoing and constant development. For example, in the Queen's Speech in December 2019, the government re-stated its commitment to progressing the Online Harms Bill. We therefore anticipate returning to these issues in the Inquiry's final report.

12. For the purposes of this investigation, the Inquiry adopted a broad definition of 'industry'. We therefore include in industry:

- the internet service providers (ISPs) and communication service providers (CSPs) such as BT;

[18] https://www.bbc.co.uk/news/uk-england-devon-11682161
[19] https://www.bbc.co.uk/news/uk-england-leeds-49499781
[20] https://www.nspcc.org.uk/what-we-do/news-opinion/thousands-sexual-offences-young-children/
[21] Christian Papaleontiou 22 May 2019 14/16-17
[22] The National Security Council is a weekly forum in which government ministers meet to discuss national security. The meeting is chaired by the Prime Minister.
[23] https://www.iicsa.org.uk/investigations/child-sexual-abuse-facilitated-by-the-internet?tab=scope

- software companies such as Microsoft;
- social media platforms such as Facebook;
- providers of search engines such as Google; and
- those who provide email and messaging services and cloud storage such as Apple.

13. Some companies provide more than one service; for example, Google's services include Google Chrome (web browser), Gmail (email service), YouTube (video-sharing website), and Google Drive (online storage for storing and sharing digital files).

14. When examining the institutional responses to online-facilitated child sexual abuse, the Inquiry identified three types of offending in relation to which the response could most easily be identified and understood.

14.1. Indecent images of children: An indecent image of a child is a photograph or pseudo-photograph[24] of a child under the age of 18 that is deemed to be indecent. An indecent image is likely to show a child in a sexual pose; the child may be clothed or in varying states of undress or naked. It may include the child being involved in penetrative and non-penetrative sexual activity. There are criminal offences for those who download, possess and distribute such imagery (under the Protection of Children Act 1978 and the Criminal Justice Act 1988). 'First-generation imagery' is a child sexual abuse image taken by an adult that has not previously been recorded by law enforcement or industry as indecent. A naked or partially naked image of a child taken by the child himself/herself is known as 'self-generated imagery'.

14.2. Grooming of a child: Grooming is the process by which a perpetrator 'prepares' a child for sexual abuse. In terms of criminal offences it can involve the adult sending a sexual message to a child (section 15A, the Sexual Offences Act 2003) or arranging to meet a child following such communication (section 15, the Sexual Offences Act 2003).

14.3. Live streaming of child sexual abuse: Live streaming is the broadcasting of real-time, live footage of a child being sexually abused over the internet. Whilst there is no specific criminal offence of 'live streaming', an offender who films an act of child sexual abuse can be prosecuted for 'creating' an indecent film (under section 1, the Protection of Children Act 1978).

15. While this report separately analyses the institutional response to these three forms of abuse, these types of harm are not always independent of each other and there can be considerable overlap. For example, there is evidence that grooming can lead to a child being asked to take indecent images of themselves or to sexual acts being video recorded. Often those perpetrators who come before the criminal courts for child sexual abuse contact offences are found to be in possession of indecent images of children.

16. The majority of websites that host indecent images of children are accessed via the open web.[25] However, the Inquiry also heard evidence about offending that takes place on the dark web (or dark net). This is part of the world wide web that is only accessible by means of specialist software and cannot be accessed through well-known search engines. The dark web is often used to host forums in which images and ideas can be exchanged

[24] A pseudo-photograph is an image, often created on a computer, which looks like a real photograph.
[25] Keith Niven 24 January 2018 4/9-12

amongst people with an interest in sexually abusing children. At any one time, the dark web is home to approximately 30,000 live sites, just under half of which are considered to contain criminal content, including but not limited to child sexual abuse and exploitation content.

A.3: Research

17. In addition to material gathered as part of the investigation and the evidence heard in the public hearings, the Inquiry also commissioned four pieces of research:

- an REA *Quantifying the Extent of Online-facilitated Child Sexual Abuse*;[26]
- an REA *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation*;[27]
- an REA *Characteristics and Vulnerabilities of Victims of Online-facilitated Child Sexual Abuse and Exploitation*;[28] and
- University of Bedfordshire Research Report *Learning about online sexual harm*.[29]

18. In general terms, the research concluded that girls are more likely to be victims of reported, online-facilitated child sexual abuse. Characteristics such as having a learning disability or coming from a home where there has been physical or sexual abuse can make children more vulnerable to online-facilitated child sexual abuse.[30] The children involved in the University of Bedfordshire Research 'Learning about online sexual harm' emphasised the importance of children being educated about online sexual harm at primary school, before they start using social media or other online forums.[31]

A.4: Procedure adopted by the Inquiry

19. The procedure adopted by the Inquiry is set out in Annex 1 to this report. Core participant status was granted under Rule 5 of the Inquiry Rules 2006 to three victims of online-facilitated child sexual abuse and five institutions and other interested parties.

20. The Inquiry separated its examination of the institutional responses to online-facilitated child sexual abuse into two phases. The phase one hearing was held in January 2018 and examined the response of law enforcement. In preparation for that hearing, the Inquiry requested data which resulted in figures relating to 2016/17 being provided. The Inquiry subsequently requested data relating to 2018/19 and, where available, this report refers to the more recent figures. The phase two hearing was held in May 2019 and focussed on the response of industry and the government. The Inquiry held several preliminary hearings in advance of the two substantive public hearings, which heard evidence over 14 days.

[26] Rapid Evidence Assessment: *Quantifying the Extent of Online-facilitated Child Sexual Abuse*

[27] Rapid Evidence Assessment: *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation*

[28] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation*

[29] *Learning about online sexual harm*

[30] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation* p9

[31] *Learning about online sexual harm* p6

21. The Inquiry received evidence from a number of sources. It heard accounts given by complainant core participants and other family members who had been directly affected by online-facilitated child sexual abuse. Those accounts provided the Inquiry with the distressing detail of the sexual abuse they or their loved ones suffered and the devastating effects of such abuse.

22. On behalf of law enforcement, the Inquiry heard from the National Crime Agency (NCA) and the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations. We also heard from witnesses representing a selection of the police forces in England and Wales, including those covering the least populated areas (such as Cumbria) through to those covering the most populated areas (such as Greater Manchester Police and the Metropolitan Police Service (MPS)).

23. The Inquiry heard evidence from a number of the companies which are responsible for provision of access to the internet and/or which provide social media platforms or other services, including Facebook, Apple, Google, Microsoft and BT. On behalf of the government, the Inquiry heard from the Home Office. Additionally the Inquiry heard from a number of non-governmental organisations (NGOs) and charities, including from the Marie Collins Foundation, the NSPCC, the Internet Watch Foundation (IWF), and John Carr OBE (a consultant and adviser on online safety and security).

A.5: Closed sessions

24. In addition to hearing evidence in open public sessions, the Inquiry held a number of private or 'closed' sessions. The closed sessions enabled the Inquiry to consider evidence that was relevant to the investigation but which had been assessed as being too sensitive to put into the public domain. Section 19 of the Inquiries Act 2005 sets out the legal framework for restricting public access to the hearing and to certain specified documents by the issuing of restriction orders.

25. The restriction orders[32] relate predominantly to sensitive detection techniques deployed by law enforcement and industry. To reveal those techniques would compromise the ability of the police and industry to detect online-facilitated child sexual abuse.

26. Following the conclusion of the closed sessions, the transcripts of those sessions were reviewed to ensure that only that material which was covered by the restriction orders was withheld from publication. Where the evidence given was not covered by a restriction order, the Inquiry published those additional parts of the transcript.[33]

27. The Inquiry has not prepared a closed part of this report. This report, including our conclusions and recommendations, takes into account all the evidence heard in both the open and closed sessions.

[32] https://www.iicsa.org.uk/investigations/child-sexual-abuse-facilitated-by-the-internet?tab=docs
[33] Extracts of evidence from closed sessions on 14 May 2019, 15 May 2019, 16 May 2019 and 21 May 2019

A.6: Terminology

28. There are a number of ways in which law enforcement, industry and government describe child sexual abuse and exploitation. Witnesses have referred to 'CSA' (child sexual abuse), 'CSAM' (child sexual abuse material), 'CSAE' (child sexual abuse and exploitation), 'CSE' (child sexual exploitation) and 'CSEA' (child sexual exploitation and abuse). Often these terms are used interchangeably.

29. In addition to the phrase 'indecent images of children', reference has occasionally been made to 'child pornography'. The Inquiry does not use this phrase. Indecent images of children are not pornography. They are a form of child sexual abuse and are illegal.

References

30. References in the footnotes of this report such as 'INQ000993' are to documents that have been adduced in evidence or published on the Inquiry website. A reference such as 'Chief Constable Simon Bailey 20 May 2019 102/23' is to the witness, the date he or she gave evidence, and the page and line reference within the relevant transcript.

Part B

Context

Context

B.1: Online-facilitated child sexual abuse

1. The government's *Serious and Organised Crime Strategy 2018* described the nature and scale of online-facilitated child sexual abuse:

> *"Any child can be a victim of abuse or exploitation … The exploitation of children online is becoming easier and more extreme. All ages are affected, from babies and toddlers through to older teenagers. Child sex offenders are becoming more sophisticated, using social media, image and file sharing sites, gaming sites and dating sites to groom potential victims. In response to law enforcement efforts to apprehend them, they are using encryption, anonymisation and destruction measures on the dark web and the open internet. Live-streamed abuse is a growing threat and children's own use of self-broadcast live-streaming applications are being exploited by offenders."*[34]

Scale

2. The magnitude of the scale and growth of online-facilitated child sexual abuse is significant.

2.1. A 2015 report by the National Society for the Prevention of Cruelty to Children (NSPCC) estimated that:

> *"there may be between 450,000 and 590,000 males aged 18–89 in the UK who have at some point viewed and used child sexual abuse images"*.[35]

2.2. In 2016/17, police forces in England and Wales[36] recorded 5,653 incidents of sexual crimes against children where there was an online element to the crime.[37] In 2017/18, the figure had grown to 8,525 offences.[38]

2.3. On 3 September 2018, a joint operation by the National Crime Agency (NCA) and local police forces in the UK resulted in the arrest of 131 suspects for offences relating to indecent images of children.[39] The scale of these arrests was not unusual. Mr Robert Jones, Director of Threat Leadership for the NCA, characterised it as just "*a week in the life of national policing and its work with the NCA*".[40]

2.4. Since 2016, approximately 400 to 450 people are arrested in the UK each month for offences of online-facilitated child sexual abuse.[41]

[34] HOM003253_016
[35] NCA000207_019
[36] In 2017, the NSPCC sent the 43 police forces across England and Wales a freedom of information (FOI) request asking for the number of sexual offences against under 18-year-olds that had a cyber-flag attached to them between 1 April 2016 and 31 March 2017. A total of 39 police forces responded.
[37] Rapid Evidence Assessment: *Quantifying the Extent of Online-facilitated Child Sexual Abuse* p13
[38] https://learning.nspcc.org.uk/media/1747/how-safe-are-our-children-2019.pdf p19
[39] Robert Jones 20 May 2019 16/10-19
[40] Robert Jones 20 May 2019 16/23-24
[41] Simon Bailey 20 May 2019 104/7-11

2.5. The Inquiry's Rapid Evidence Assessment (REA) *Quantifying the Extent of Online-facilitated Child Sexual Abuse* states:

> *"Although no study identified in this REA examined the proportion of adults holding online sexualised conversations with young people in England and Wales, it is unlikely that figures would be below the lowest estimate of 1 in 10 adults."*[42]

3. As the government's recent *Online Harms White Paper* (April 2019) observed, "*The sheer scale of CSEA online is horrifying*".[43]

Severity

4. As the scale of offending grows, so does the severity of the abuse. Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, told us that the police were seeing "*an exponential increase in reports of abuse*" but also that "*levels of depravity that are – if they could get worse, are getting worse. We are seeing babies being subjects of sexual abuse*".[44]

5. In its 2018 Annual Report, the Internet Watch Foundation (IWF)[45] said that where it detected child sexual abuse imagery of younger children, "*it is more likely to show the most severe forms of abuse, including rape and sexual torture*".[46] In 2018, Matthew Falder, aged 29, was convicted of offences that included using the internet to encourage the rape of a two-year-old child and offences against a newborn baby.[47] In another recent case, an offender uploaded videos on to a site on the dark web showing his abuse of children aged three and five years old.[48] The Home Office told us about one site on the dark web that required its subscribers to upload 20 first-generation images, or a two-minute video of infant or toddler abuse, each month.[49]

Demand

6. We asked the Home Office what the government was doing to gain a better understanding of what was driving the growing demand for child sexual abuse. Mr Christian Papaleontiou, Head of the Home Office's Tackling Exploitation and Abuse Unit, told us that there were:

> *"different models of and motivations for child sexual abuse and exploitation. Some of it will be sexual interest in children, some of it … where it is almost pure sadism … Equally, we will know … about the issue of the whole interaction between the power and authority on one hand and vulnerability."*[50]

[42] Rapid Evidence Assessment: *Quantifying the Extent of Online-facilitated Child Sexual Abuse* p14
[43] INQ004232_016
[44] Simon Bailey 20 May 2019 113/19-23
[45] The IWF is an independent not-for-profit organisation which aims to remove child sexual abuse images and videos from the internet and to minimise the availability of such material.
[46] INQ004283_028
[47] https://www.theguardian.com/technology/2018/feb/19/dark-web-paedophile-matthew-falder-jailed-for-32-years
[48] Robert Jones 20 May 2019 22/16-23/12
[49] HOM003247_010
[50] Christian Papaleontiou 22 May 2019 86/22-87/7

7. He agreed that there needed to be "*a much more sophisticated understanding*"[51] of the reasons why perpetrators committed child sexual abuse and explained that the Home Office had provided £7.5 million to fund the Centre of Expertise on Child Sexual Abuse. He told us that one aspect of the Centre's work was to look at "*typologies of child sexual abuse*" to help understand "*how you can take different approaches to different sorts of offenders*".[52]

B.2: Victims and survivors

Research

8. Research commissioned by the Inquiry concludes that girls are more likely to be victims of reported online-facilitated child sexual abuse.[53] The research also suggests that the 11 to 14 years age group may be most vulnerable to online-facilitated child sexual abuse.[54]

9. These findings are supported by other evidence.

9.1. In May 2018, research published by the IWF found that the majority of images and videos of live-streamed child sexual abuse analysed by the IWF depicted children assessed as being between 11 and 13 years old.[55] In 2019 (January to April), 81 percent of self-generated content on which the IWF took action was of children aged 11 to 13, predominantly girls.[56] Ms Susie Hargreaves OBE, Chief Executive of the IWF, told us:

> "*we are extremely worried about girls, young girls, 11 to 13, in their bedroom with a camera-enabled device and an internet connection*".[57]

9.2. The Inquiry heard similar evidence from police forces. Kent Police reported that victims of online-facilitated child sexual abuse were predominantly between 11 and 15 years old and 84 percent were female.[58] Norfolk Constabulary reported that 81 percent of victims were between 12 and 15 years old and (excluding victims of indecent image offences) 89 percent were female.[59] West Midlands Police agreed that those aged 13 to 15 years were by far the largest group of victims.[60]

10. Research also shows that adverse childhood experiences, such as physical or sexual abuse and exposure to parental conflict, make children more vulnerable to abuse online.[61] Above-average internet use increases vulnerability when this interacts with other characteristics such as having a disability or low self-esteem.[62]

[51] Christian Papaleontiou 22 May 2019 87/8-9

[52] Christian Papaleontiou 22 May 2019 87/15-18

[53] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation* p9

[54] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation* p10. The REA states that this may be because adolescents are more often sampled in research studies, and studies involving children under 11 years old are rare.

[55] IWF000010_011

[56] Susie Hargreaves 17 May 2019 134/18-135/3

[57] Susie Hargreaves 17 May 2019 135/4-6

[58] OHY003413_006

[59] OHY003312_017

[60] OHY003315_015

[61] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation* p9

[62] Rapid Evidence Assessment: *Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation* p9

The experience of victims and survivors

11. The Inquiry heard from IN-A3. When she was approximately 15 years old, IN-A3 worked part-time at a local bed & breakfast. Over time, the owner, Laurence Glynn (a man in his 60s), started to groom her and one of the other girls who worked there. He made inappropriate comments about her figure, bought her clothes and took her out to dinner. He took photographs of her sitting down in positions where her underwear could be seen. He sent her inappropriate messages on Facebook and Twitter. He showed her photos of young children which IN-A3 described as "*the most disturbing thing I've ever seen in my life*".[63] She told us that on one occasion Glynn sexually assaulted her. IN-A3 described the devastating effect the abuse had on her. She "*went a bit off the rails*", struggled, and still struggles, to sleep, and has an "*awful feeling*" of worrying that pictures of her may be circulating online.[64]

12. The Inquiry also heard from Ms Lorin LaFave.[65] On 17 February 2014, Ms LaFave's 14-year-old son, Breck, was brutally murdered by Lewis Daynes, then aged 18. In 2013, Breck had met Daynes in an online gaming community set up by Daynes. Daynes began to manipulate Breck and sought to distance Breck from his family. Ms LaFave tried to protect her son and in December 2013 she called Surrey Police and reported that she thought her son was being groomed for sex by an older man. She expected that the police would check any police records on Daynes but in fact nothing was done and the call log was closed. A subsequent Independent Police Complaints Commission[66] (IPCC) report concluded that, based on the information provided by Ms LaFave, the call handler should have "*taken more action*" and sought guidance on how to deal with callers expressing concerns about grooming.[67] Had the call handler checked Daynes' police national computer record, it would have revealed that when Daynes was 15 he had been accused of sexually assaulting a 15-year-old boy. This information should have prompted the police to investigate Ms LaFave's concerns.

13. On 16 February 2014, unbeknown to his parents, Breck visited Daynes. The next day, Daynes stabbed Breck to death. Daynes then destroyed his telephones and computer equipment by submerging the devices in a sink filled with water. The police found paraphernalia suggesting that the murder had been sexually motivated. Ms LaFave described that when she was told that Breck had been murdered she "*fell to the floor and could not stop screaming, this was what I tried so hard to prevent*".[68] In January 2015, Daynes was sentenced to life imprisonment with a minimum term of 25 years.

B.3: The institutions and organisations

14. In this investigation, the Inquiry considered the role of institutions and organisations such as government, law enforcement, industry, charities and non-governmental organisations (NGOs).

[63] IN-A3 13 May 2019 64/6-7
[64] IN-A3 13 May 2019 84/7-85/24
[65] Lorin LaFave 22 January 2018 57/12-111/16
[66] In January 2018, under the Police and Crime Act 2017, the Independent Police Complaints Commission (IPCC) was replaced by the Independent Office for Police Conduct (IOPC).
[67] INQ001032_012-013
[68] INQ001037_008

Government

15. The Home Office is the lead government department responsible for policy relating to online-facilitated child sexual abuse.[69] Its Tackling Exploitation and Abuse Unit engages with law enforcement, the intelligence agencies and industry; coordinates international cooperation to combat this abuse; identifies ways to address child sexual exploitation; and manages policy regarding the support of victims. The unit also works with other Home Office teams such as the team responsible for the Child Abuse Image Database (CAID).[70] In addition, the Home Office is responsible for making decisions on funding over and above the core budgets allocated to the NCA and the police.

16. Other government departments are involved in aspects of the response to child sexual abuse and exploitation.

> **16.1.** The Department for Education is responsible for educating children about online safety. From September 2020, relationships education will be compulsory in primary schools in England, and relationships and sex education compulsory in secondary schools.[71] Draft guidance for these subjects includes material on online safety and, more generally, healthy relationships, boundaries and respect for others.[72]
>
> **16.2.** The Ministry of Justice is responsible for the criminal law relating to acts of child sexual abuse (both contact offences and offences facilitated by the internet) and for the wider criminal justice system.
>
> **16.3.** The Department for Digital, Culture, Media & Sport (DCMS) is responsible for digital issues. In October 2017, DCMS launched its Internet Safety Strategy consultation looking at various aspects of online safety (but not illegal harms such as child sexual abuse and exploitation). At the conclusion of the consultation process, DCMS and the Home Office published the *Online Harms White Paper* (April 2019) which specifically included the government's proposals for combating online-facilitated child sexual abuse. These proposals are considered in more detail in Part F of this report.

Law enforcement

The National Crime Agency

17. The National Crime Agency (NCA) leads and coordinates UK law enforcement's response to serious and organised crime. The response to online-facilitated child sexual abuse is the particular responsibility of the Child Exploitation and Online Protection Centre (CEOP), a command of the NCA. According to 2018/19 figures, the CEOP command now has 278 staff as well as 43 secondees from children's charities and industry. Its budget for 2018/19 was £17.97 million.[73]

18. In addition to carrying out investigations, apprehending offenders and identifying and safeguarding victims, the NCA responds to public reports made via the 'ClickCEOP' button on the homepage of the NCA and CEOP websites. ClickCEOP is an online reporting tool which enables anyone to make a report of online sexual abuse directly to the NCA.

[69] HOM003247_002
[70] The Child Abuse Image Database (CAID) is a single secure database of illegal images of children.
[71] HOM003247_042
[72] HOM003273
[73] NCA000370_003

19. The NCA also receives reports from the National Center for Missing & Exploited Children (NCMEC), a non-profit private organisation established in the US in 1984. Electronic service providers (ESPs) based in the US are obliged under US law to make a report to NCMEC when they become aware of child sexual abuse material on their networks. Where the report relates to the UK,[74] NCMEC sends the report to the NCA. The NCA responds to the most serious reports itself and passes others on to local police forces.

20. The NCA also delivers an education programme known as 'Thinkuknow'.[75] The Thinkuknow website provides educational resources – including films, cartoons and lesson plans – for children, their parents and teachers to stay safe on the internet. The material is tailored to children depending on their age. The NCA also trains ambassadors to deliver the programme in schools. The NCA estimates that in 2016/17 the programme reached about 5.9 million children in the UK.[76] Between April 2017 and March 2019, Thinkuknow resources were downloaded over 81,000 times.[77]

Local police forces

21. Much of the operational work against online-facilitated child sexual abuse is carried out by the 43 police forces in England and Wales. In 2015, the Home Secretary designated child sexual exploitation and abuse as a threat of national importance, putting it on the same footing as terrorism.[78] According to Chief Constable Bailey, the impact of this was to make "*very clear*" to chief constables and police and crime commissioners of the need for an effective and adequately resourced response.[79]

22. There is an agreed plan in place for how local forces will work with the NCA and regionally with one another through regional organised crime units (ROCUs). The foundation of this plan is the '4Ps' approach of the Serious and Organised Crime Strategy:[80]

- 'Pursue': pursuing offenders through the criminal justice system;
- 'Prevent': preventing offending and reoffending while tackling threats from offenders and potential offenders;
- 'Protect': seeking to increase the resilience of systems and infrastructure; and
- 'Prepare': ensuring that those affected by serious and organised crime have the support they need.

23. The overall performance of police forces in pursuing online offenders is monitored by the Online Pursue Board, chaired by Chief Constable Bailey.

24. The Inquiry heard evidence from a range of police forces of different sizes across England and Wales: Kent Police, West Midlands Police, Avon and Somerset Constabulary, the Metropolitan Police Service, Greater Manchester Police, Norfolk Constabulary, Cumbria Constabulary and Gwent Police. While there are differences in the ways that forces structure and finance their responses to this type of offending, there are two key common features. First, the most serious or complex cases are typically tackled by a specialist unit. Second, over the last few years, all the forces have responded to the increasing scale of

[74] See Part C of this report.
[75] NCA000163_061
[76] Keith Niven 24 January 2018 41/20-22
[77] NCA000370_004
[78] OHY002224_007-008
[79] Simon Bailey 24 January 2018 80/8-14
[80] NCA000163_033

offending by dedicating more resources – financial, technical and human – to their efforts. For example, in 2015/16, Avon and Somerset Constabulary increased funding for its Internet Child Abuse Team (ICAT) by 18 percent.[81] In 2016/17, further funding enabled the ICAT to expand from seven to 16 staff and the number of data forensic investigators dedicated exclusively to ICAT cases increased from one part-time investigator to three full-time investigators.

25. Within the UK, law enforcement investigations into online-facilitated child sexual abuse will usually involve the use of investigatory powers to identify offenders and acquire communications data.[82] Communications data is the "*who, where, when and how of a communication but not the content*" of the communication.[83] Communications data would include, for example, the billing data showing the dates and times of messages and calls between telephones but not the content of any text message.

26. In the context of online-facilitated child sexual abuse investigations, much of the data is held by companies based in the US. Prior to October 2019, the acquisition of content data (eg the words in a text message or a social media post) held by companies overseas involved a process under a mutual legal assistance treaty (MLAT).[84] The MLAT process was described as cumbersome and lengthy, with the average time for UK law enforcement to get information from overseas companies being over a year.[85] However, on 3 October 2019, the Home Secretary signed a UK–US bilateral data access agreement allowing UK law enforcement to request communications content and data directly from US-based communications service providers.[86] It is envisaged that the new agreement will mean that data can be accessed in weeks, if not days.[87]

27. Once a perpetrator has been identified and arrested, there are a number of key criminal offences:

- possessing and distributing indecent images of children;[88]
- arranging or facilitating the commission of a child sexual offence;[89]
- causing or inciting a child to engage in sexual activity or causing a child to watch a sexual act;[90] and
- meeting a child following sexual grooming and the offence of engaging in sexual communication with a child, introduced in April 2017.[91]

28. In many cases where an offender is being sentenced for sexual offences, including those facilitated by the internet, the courts can impose a sexual harm prevention order. This can, for instance, place limitations on, and enable the monitoring of, the offender's use of the internet. Failure to comply with such an order is a criminal offence. The number of such orders has increased substantially, from 1,114 in 2006/07 to 5,551 in 2017/18.[92]

[81] OHY003388_002
[82] The powers are contained in the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016
[83] HOM003247_024
[84] Robert Jones 20 May 2019 77/4-15
[85] Christian Papaleontiou 22 May 2019 56/12-18
[86] https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement
[87] Christian Papaleontiou 22 May 2019 57/13-16
[88] For example: section 1 of the Protection of Children Act 1978, section 160 of the Criminal Justice Act 1988 and section 62 of the Coroners and Justice Act 2009
[89] Section 14 of the Sexual Offences Act 2003
[90] Sections 10 and 12 of the Sexual Offences Act 2003
[91] Sections 15-15A of the Sexual Offences Act 2003
[92] Ministry of Justice, *Multi-Agency Public Protection Arrangements – Annual Report 2017/2018* p14

Industry

29. The Inquiry heard evidence from a variety of companies that provide products and services capable of being used to enable or facilitate online child sexual abuse. Other than Kik (a messaging application founded in Canada), all of these companies have a very large presence in the UK. BT Group is the largest internet service provider in the UK.[93] Microsoft has almost 5,000 UK employees.[94] Facebook has approximately 40 million users in the UK and 2,300 full-time employees.[95] Apple does not keep specific data on the number of UK users of Apple products but estimates the number to be in the "*millions and millions*" and has 6,500 UK employees.[96] Google estimates that there are tens of millions of users in the UK of some of its products and has over 4,000 employees in the UK.[97]

Internet Watch Foundation

30. The Internet Watch Foundation (IWF) was established in 1996. Its objective is "*eliminating child sexual abuse wherever it occurs in the world*" and it plays a key role in detecting and removing child sexual abuse images from the internet.[98] From five founding members, the IWF now has 148 members, including internet service providers and social media companies such as Google, Microsoft, Apple, Facebook and BT.[99] It is a UK registered charity and is funded primarily (90 percent) by its members, with the remaining 10 percent coming from the European Commission.[100]

31. The IWF operates a hotline for the public to report potentially criminal online content and, since 2014, has also proactively carried out searches for such content. Its members are provided with various tools and blocking lists designed to prevent access to illegal content. It issues 'takedown notices' to UK internet service providers requiring them to remove child sexual abuse content.

32. In its first year of operation (1996), the IWF processed 1,291 reports of potentially criminal content.[101] At that time, the UK hosted 18 percent of the world's known child sexual abuse material.[102] By 2018, the IWF processed nearly 230,000 reports and the UK hosted 0.04 percent of such content.[103] By way of comparison, in 2018, the Netherlands hosted 47 percent of this material and 12 percent was hosted in the US.[104]

Other organisations

33. There are a number of third sector (voluntary and community) organisations that play a role in tackling online-facilitated child sexual abuse.

> **33.1.** The Marie Collins Foundation, established in 2011, is a charity set up to address the recovery needs of children who suffer sexual abuse and exploitation online. It offers support services to children and their families and provides training to professionals.

[93] Kevin Brown 17 May 2019 3/11-18
[94] Hugh Milward 15 May 2019 73/16-74/1
[95] Julie de Bailliencourt 14 May 2019 21/19 and 22/11-13
[96] Melissa Polinsky 15 May 2019 6/17-7/1
[97] Kristie Canegallo 16 May 2019 39/8-19
[98] IWF000020_001-005
[99] Susie Hargreaves 17 May 2019 57/15; IWF000020_003
[100] IWF000020_005
[101] IWF000020_001
[102] IWF000020_001
[103] Susie Hargreaves 17 May 2019 101/1-3
[104] INQ004283_021

33.2. The Children's Charities' Coalition on Internet Safety (known as CHIS), established in 1999, is made up of 11 UK children's charities. It lobbies government and industry to improve the safety of children online.

33.3. Mr Tony Stower, Head of Child Safety Online at the NSPCC, told us about the organisation's campaigns, research, and support for parents and children affected by this kind of abuse.[105]

33.4. The Lucy Faithfull Foundation (LFF) is a charity dedicated to preventing child sexual abuse. It runs a helpline called 'Stop it Now!' for adults worried about their own behaviour.[106] In January 2018, Chief Constable Bailey told us that such was the demand for help from the LFF that between April 2016 and March 2017 *"only 21 per cent of callers"*[107] managed to get through to the helpline when they first called. In March 2019, the Home Office announced £600,000 in funding to the LFF to increase the capacity of the helpline.[108]

Collaborative efforts

34. There are also a number of international forums set up to enable institutions and organisations to collaborate with one another.

34.1. The Virtual Global Taskforce was established in 2003 as a collaboration between international law enforcement agencies and industry.[109] The NCA is a member. An example of the taskforce's recent work is a project, led by the UK, focussed on engaging key technology companies to enhance child safety on their platforms.

34.2. The Technology Coalition, established in 2006, brings together international technology companies to collaborate in the response to online abuse.[110] It works to identify and promote technology solutions to child sexual abuse material with the aim of eradicating online child sexual exploitation.

34.3. In 2014 the WePROTECT Global Alliance was established as a forum to improve the global response to online-facilitated child sexual abuse.[111] The alliance has 85 member countries, 20 industry members and 25 leading third sector organisations.[112] In 2018, it issued a global threat assessment to provide a better understanding of the worldwide threat of online child sexual exploitation and abuse and set out what countries need to do at a national level to tackle such abuse and to provide support for victims.[113] The Home Office provides £1–2 million per year in funding for the WePROTECT Global Alliance secretariat.[114]

[105] Tony Stower 22 May 2019 140/18 to 141/13
[106] Simon Bailey 24 January 2018 139/6-18
[107] Simon Bailey 24 January 2018 140/8-10
[108] https://www.gov.uk/government/news/funding-boost-for-child-sexual-abuse-prevention-helpline-following-jump-in-contacts
[109] NCA000163_066
[110] GOO000001_010
[111] Christian Papaleontiou 22 May 2019 27/7-17
[112] Christian Papaleontiou 22 May 2019 26/25-27/3
[113] Christian Papaleontiou 22 May 2019 27/10-13
[114] Christian Papaleontiou 22 May 2019 26/21-24

34.4. In June 2018 the UK ratified the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as the Lanzarote Convention.[115] The Convention sets standards for the response to sexual offences against children. The Lanzarote Committee, established to implement the Convention, will help member states to cooperate in preventing and combating such abuse.

[115] HOM003247_043

Part C

Indecent images of children

Indecent images of children

C.1: Introduction

1. The precise number of indecent images of children in circulation worldwide is not known but is believed to be in the many millions. In the US alone, the National Center for Missing & Exploited Children (NCMEC) database contains 47.2 million unique images and 14.6 million unique videos which include indecent images of children and images taken prior to the abuse occurring.[116]

2. Images encountered by law enforcement span a spectrum of offending, including images of children in sexualised poses, the rape of young children and babies, penetration of small children and infants with objects, as well as children being tied up and subjected to physically painful sexual assaults.

3. The harm inflicted does not end once the image has been taken. In its recent annual report, the Internet Watch Foundation (IWF) recounted the abuse of a young girl called Olivia.[117] In 2013, eight-year-old Olivia was rescued by police. For five years she had been raped and tortured. Images and videos were taken of this abuse. Her abuser was imprisoned. However, the images remained online. Over a three-month period,[118] the IWF encountered images of Olivia's abuse online (including on commercial websites) on average five times a day.

4. This repeat victimisation is a constant worry for victims who were either groomed into taking photos of themselves or who had photos taken of them while they were being sexually assaulted. IN-A1, who was groomed online, said she "*remains worried about where the images of her and her brother are*".[119] Another victim, IN-A3, told us:

> "*you don't know where these images will end up … and that is an awful feeling, thinking that paedophiles can just look online and get whatever they want … it's scary*".[120]

C.2: Detection of images

5. There are different ways in which indecent images of children are detected by law enforcement and industry. The methods of detection vary depending on whether the image has previously been identified as an indecent image of a child (known image) or whether it is an image that has not previously been recorded by law enforcement or industry (unknown material) – often first-generation or self-generated imagery.

[116] NCA000370_004

[117] INQ004283_011

[118] Imagery was monitored between September and November 2018 on each working day (IWF000022_002).

[119] IN-A1 13 May 2019 101/14-15

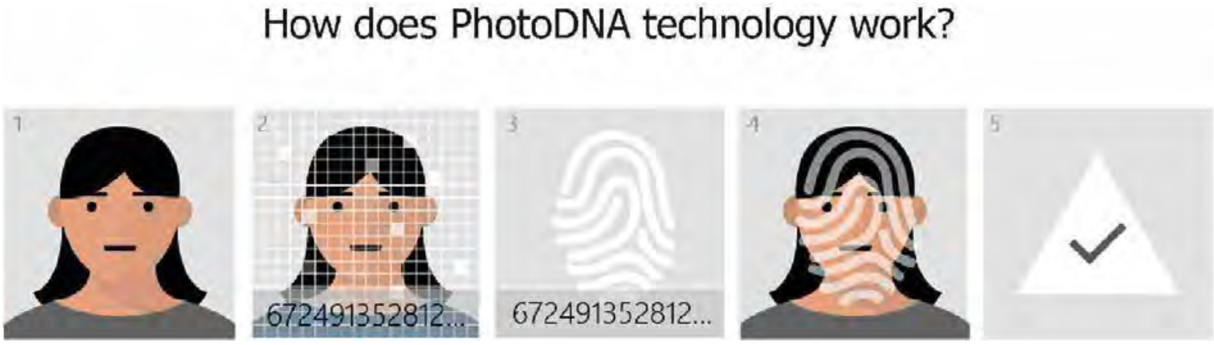
[120] IN-A3 13 May 2019 85/20-86/1

Known child sexual abuse material

6. The sheer scale of child sexual abuse imagery is such that in order to detect this material industry and law enforcement are reliant on software and machine learning.[121]

PhotoDNA

7. In 2009 Microsoft developed technology called PhotoDNA. The company "*didn't want to be a platform of choice for abusers*"[122] and so developed PhotoDNA to assist in finding and removing known images of child sexual abuse on the internet. PhotoDNA creates a unique digital signature (known as a hash) of an image which is then compared against signatures (or hashes) of other photos to find copies of the same image.



Microsoft's PhotoDNA

Source: MIC000012_003[123]

8. Mr Hugh Milward, Senior Director for Corporate, Legal and External Affairs for Microsoft UK, described the process:

> *"You can take an image and scan it and it effectively turns that image into a string of numbers. Then you can compare that string of numbers with other strings of numbers and if the strings of numbers is similar or the same, then you can reach a conclusion with very great accuracy that the image is the same or similar."*[124]

PhotoDNA therefore enables a child sexual abuse image to be identified even if, for example, the colour of the image has been altered, or the image has been cropped.

9. Microsoft makes approximately 5,800 referrals each month to NCMEC globally across all types of child sexual abuse and exploitation.[125] Mr Milward said that most of those reports related to the finding of indecent images on the web. He did not know how many of those referrals related to the UK. When asked why such analysis was not undertaken, he explained:

> *"we think about the way in which we're tackling this in every country, and we want to make a difference in every country. So breaking it down for the UK … it doesn't help us in the fight that we're making".*[126]

[121] Machine learning is an application of artificial intelligence that focusses on teaching computers how to learn from data without the need to be programmed for specific tasks.
[122] Hugh Milward 15 May 2019 100/3-4
[123] https://www.microsoft.com/en-us/photodna
[124] Hugh Milward 15 May 2019 100/21-101/3
[125] Hugh Milward 15 May 2019 109/7-12
[126] Hugh Milward 15 May 2019 112/16-21

10. Mr Milward said that one way of ascertaining the number of reports relating to the UK was to look at the number of accounts closed where child sexual abuse material had been found.

> "*So I have the figure for several years and they do vary between, you know, 98 in one year, 400 in another year, 244 in another year, 312 in another year.*"[127]

11. In addition to using PhotoDNA to detect child sexual abuse imagery across its own products and services, Microsoft made this technology available to other companies in the industry and to NCMEC.[128] More than 155 organisations now use PhotoDNA.

11.1. Facebook has been using PhotoDNA since 2011.[129] When asked what happens when an individual attempts to upload a known child sexual abuse image, Ms Julie de Bailliencourt, Facebook's Senior Manager for the Global Operations Team,[130] told us that in order to:

> "*compare the digital fingerprint of the new photos versus the hashes*[131] *that we have in our databank, we need to have sufficient information to make this match and conclude that the person uploaded this particular photo*".[132]

In practice this means that the abuse image is available to be viewed until such time as the image is removed. Ms de Bailliencourt said that on average an image was removed in "*a few minutes*" but added that she had seen the image being removed "*seconds after the upload*".[133]

11.2. Kik (a Canadian messaging application) started using PhotoDNA in 2015.[134] Kik has also developed 'SafePhoto' which is software used to "*detect, report, and ultimately delete known images of child exploitation on the Kik platform*".[135]

11.3. Google referred to PhotoDNA as the "*industry standard*".[136] In addition to using PhotoDNA, Google has designed its own "*proprietary technology*"[137] to search for indecent images of children. Developed around 10 years ago, Google takes the hashes from NCMEC and re-hashes that image.[138] Google uses the re-hash to scan for the image across Google's products and services. Google considers that this technology has led to improved accuracy in identifying child abuse images. Ms Kristie Canegallo, Vice President and Global Lead for Trust and Safety at Google, explained that Google has not shared this technology with other companies because "*it is tailored to our products. So I'm not sure whether others would find similar benefits*".[139]

[127] Hugh Milward 16 May 2019 3/3-5
[128] NCMEC was established in the US in 1984 as a non-profit private organisation. Its aim is to provide a coordinated national response to problems relating to missing and exploited children.
[129] Julie de Bailliencourt 14 May 2019 21/9-12
[130] Ms de Bailliencourt's role changed in April 2019; Julie de Bailliencourt 14 May 2019 19/24-25
[131] A hash is a unique digital signature of an image.
[132] Julie de Bailliencourt 14 May 2019 76/3-7
[133] Julie de Bailliencourt 14 May 2019 76/15-18
[134] Michael Roberts 17 May 2019 49/21
[135] KIK000009_002
[136] Kristie Canegallo 16 May 2019 88/22
[137] Kristie Canegallo 16 May 2019 88/9-10
[138] Kristie Canegallo 16 May 2019 88/2-4
[139] Kristie Canegallo 16 May 2019 89/6-8

12. In 2012, Microsoft donated PhotoDNA to law enforcement worldwide.[140] In 2015, Microsoft also made PhotoDNA available on its cloud services,[141] which enables smaller organisations who use cloud services to ensure that their platform is not used to upload and store such imagery.

13. Once the image has been hashed, the hash is inputted into the IWF or NCMEC hash database.[142] The IWF's database is known as the hash list. The hash list is compiled from hashes that are generated for each image that the IWF confirms contains child sexual abuse imagery. The hash list can then be used to search for duplicate images online so that the images can be removed. It can also be used by IWF members to stop those images being shared and uploaded. In the event that the IWF receives a report of an image already contained within the hash list, the analyst does not need to re-review the image and can move straight to ascertaining where that image is hosted and getting the image removed. By May 2019, the IWF's hash list contained approximately 378,000 unique hashes.[143] By December 2019, this number had grown to over 420,000 unique hashes.[144]

14. The NCMEC database is similar to the IWF hash list but contains a significantly higher number of unique hashes. In December 2019, the IWF entered into an agreement with NCMEC to allow its hashes to be shared with NCMEC thereby increasing the pool of known child sexual abuse imagery that can be detected.[145]

PhotoDNA for Video

15. Child sexual abuse content is often hidden amongst otherwise innocuous video footage. As a consequence, where a suspected child sexual abuse video is reported to the IWF, an IWF analyst is required to watch the entire video to ascertain whether the video contains child sexual abuse material. This can be a time-consuming process.

16. In 2018, PhotoDNA for Video was developed. PhotoDNA for Video breaks down a video into key frames and hashes those frames. Those hashes can then be compared and matched with hashes of known child sexual abuse images.[146]

17. PhotoDNA for Video has therefore increased the IWF's ability to identify child sexual abuse content and quickly take appropriate action in relation to videos. PhotoDNA for Video has also been made available to other internet organisations and companies worldwide.

18. As more organisations deploy PhotoDNA and PhotoDNA for Video, more material will be hashed and the databases will become larger. This will enable more child sexual abuse material to be detected. In this sense, detection and prevention are linked.

19. Software such as PhotoDNA and Google's own re-hash technology are valuable tools to prevent the proliferation of indecent images and videos. Such tools should be used as widely as possible by every organisation and company whose platforms allow for the uploading, downloading and sharing of content. Collaboration between companies in developing future technologies is vital.

[140] MIC000026_011
[141] The cloud is a network of remote servers hosted on the internet to store, manage and process data.
[142] Hugh Milward 15 May 2019 102/11-12
[143] Susie Hargreaves 17 May 2019 112/25
[144] https://www.iwf.org.uk/news/landmark-data-sharing-agreement-to-help-safeguard-victims-of-sexual-abuse-imagery
[145] https://www.iwf.org.uk/news/landmark-data-sharing-agreement-to-help-safeguard-victims-of-sexual-abuse-imagery
[146] MIC000018_003

Web crawlers

20. Part of the technological response to the volume of indecent images of children has been through the development of web crawlers. In the context of this investigation, a web crawler is a computer programme that automatically searches for indecent images on the web.

21. In 2016, the Canadian Centre for Child Protection[147] launched Project Arachnid. Project Arachnid is a web crawler designed to discover child sexual abuse material on sites that have previously been reported to the Canadian CyberTipline[148] as hosting such material. Google assisted in providing funding and technical assistance to develop this tool. Once child sexual abuse material has been detected, the crawler automatically sends a notice to the provider hosting the content requesting that the image be taken down.[149]

22. In November 2017, the Home Office invested £600,000 to help expand Project Arachnid.[150] This funding increased the capacity of the crawler so that more web pages could be searched per second, resulting in more images being identified and removed. The investment also meant that NCMEC's hash database was added to the Project Arachnid database, enabling the crawler to identify a larger number of indecent images of children. The money enabled the development of technology for industry to proactively scan their networks to identify and remove such imagery. As at January 2019:

- the crawler processed an average of 8,000 images per second and peaked at 150,000 images per second;
- 1.6 million notices were sent to service providers with more than 4,000 notices issued per day; and
- 7.4 million images of child sexual abuse have been detected.[151]

23. Since the start of 2019, Project Arachnid has detected more than 5,500 pages on the dark web hosting child sexual abuse material. However, because the identity of the server is anonymised, notices requesting removal of the material cannot be sent.[152] Project Arachnid has also detected a large volume of child sexual abuse material related to prepubescent children that is made available on dark web forums but actually sits on open web sources in encrypted archives. By virtue of encryption, scanning techniques cannot detect the imagery.[153]

24. In late 2017, the IWF introduced its own web crawler. Ms Susie Hargreaves OBE, Chief Executive of the IWF, explained the IWF's crawler in this way:

> *"we start off with a web page, a URL of child sexual abuse, and you put it into your crawler, which is like a spider, and then it will take that web page and it will start crawling and looking for similar things. So it will go into that web page and it will go to the next level down, next level down, it will see a link and it will keep going and keep going. And*

[147] The Canadian Centre for Child Protection runs a CyberTipline that operates in a similar way to NCMEC's CyberTipline.
[148] An online tool to report indecent images of children and incidents of grooming and child sex-trafficking found on the internet.
[149] HOM003278_001
[150] HOM003247_021-022
[151] HOM003278_002-003
[152] CRS000031_031
[153] CRS000031_031-032

> *every time it finds something that might be suspected child sexual abuse, it will return that back to us. We can then match that against our hash list … so that, if we see immediate matches, we can take action accordingly.*"[154]

IWF analysts view the crawler's returns to ensure that the image is illegal under UK legislation and then request that the web page is removed.[155]

25. The IWF crawler therefore enables a large amount of material to be identified far more quickly than a human analyst could. By way of example, in 2017, the IWF processed 132,636 reports of child sexual abuse material from both the public and through proactive searching (both by the IWF analysts and, latterly, via the crawler). In 2018, that number had grown to 229,328 reports, the increase being accounted for, in part, due to the use of the crawler.[156]

26. Where the content is hosted in the UK, the IWF confirms with law enforcement that removal of the imagery would not prejudice any ongoing police investigations and then issues a 'Notice and Takedown'. In 2018, only 41 URLs[157] displaying child sexual abuse and exploitation imagery were hosted in the UK, a decrease from 274 URLs in 2017.[158] Of that content, 35 percent was removed in under an hour; 55 percent in one to two hours and 10 percent in two hours or more.[159] In 2018, the fastest time for compliance with a 'Notice and Takedown' was two minutes and 39 seconds.[160]

27. Where the content is hosted outside the UK, Ms Hargreaves explained that the IWF's response depended on whether the host country has an INHOPE registered hotline. INHOPE is a foundation that develops national hotlines to help deal with child sexual abuse material online.

> "*So if they have a hotline – so there are 52 hotlines in 48 countries – we send the content via the INHOPE database*".[161]

The host country's hotline is then responsible for processing the IWF's report in accordance with their national law. If the country has no hotline, then the IWF will pursue the matter through either the National Crime Agency (NCA) or any direct link to law enforcement in that host country.[162]

28. Technological innovations such as crawlers greatly increase the capacity to proactively detect known images of child sexual abuse. Project Arachnid and the IWF's crawler are excellent examples of how collaboration between governments and non-governmental organisations (NGOs), aided by technology, can bring about tangible results in detecting child sexual abuse and exploitation imagery.

29. In the UK, the IWF sits at the heart of the national response to combating the proliferation of indecent images of children. It is an organisation that deserves to be publically acknowledged as being a vital part of how, and why, comparatively little child sexual abuse material is hosted in the UK.

[154] Susie Hargreaves 17 May 2019 75/11-22
[155] The Project Arachnid crawler counts images for removal; the IWF crawler counts web pages for removal.
[156] IWF000021_002
[157] A 'URL' (uniform resource locator) is the address where a particular page or resource (eg images, sound files) can be found on the world wide web.
[158] INQ004283_035
[159] INQ004283_035
[160] IWF000022_002
[161] Susie Hargreaves 17 May 2019 97/9-11
[162] Susie Hargreaves 17 May 2019 97/24-98/4

Previously undetected child sexual abuse material

Technology

30. Technology, including machine learning (ie computer programmes that can access data and use it to learn for themselves), also assists in identifying child sexual abuse images that have not previously been hashed or are newly generated images.

31. In September 2018, Google launched new artificial intelligence technology[163] which detects images containing child nudity and images most likely to contain child sexual abuse content (whether previously detected or not). The technology prioritises the image for review and enables Google to remove the image, often before it has been viewed. Ms Canegallo said that Google thought this technology was "*a game changer*".[164] Google estimates that this technology will enable reviewers to take action on 700 percent[165] more child sexual abuse content than before. It is making this technology available to NGOs and other industry companies. Machine learning is also used to detect material on YouTube that violates YouTube's nudity and sexual content policy.

32. In October 2018, Facebook announced that it had developed a classifier (a computer programme that learns from data given to it to then identify similar data) to detect whether an image may contain child nudity. Where the classifier identifies this possibility, the image would be reviewed by its Community Operations team. Facebook "*is exploring*" how to make this technology available to NGOs and other internet companies.[166]

33. Advances in technology undoubtedly play an important role in detecting large volumes of potential child sexual abuse and exploitation content and alerting the internet companies to a previously unidentified child sexual abuse image. However, there remains a need to ensure that companies have a sufficient number of staff (often called moderators) to be able to conduct a review of any such material and take action including, where appropriate, referring the matter to law enforcement.

Notification to law enforcement

CyberTip reports

34. US law requires that electronic communications companies or companies that provide remote computing services to the public report child sexual abuse material (known as a CyberTip report) to NCMEC "*as soon as is reasonably practicable*".[167] This obligation exists whether an image is a known or previously undetected image. In 1998, NCMEC noticed an increase in the number of reports relating to online child sexual exploitation and so created the CyberTipline. This is an online tool which enables the public and industry to report indecent images of children and incidents of grooming and child sex-trafficking found on the internet.

35. The CyberTip report, made via the CyberTipline, must contain information about the suspected perpetrator such as an email address or IP address.[168] A single CyberTip report might contain thousands of images linked to a single account or thousands of IP addresses;

[163] GOO000039; Also referred to as the 'Content Safety API'.
[164] Kristie Canegallo 16 May 2019 78/21-22
[165] Kristie Canegallo 16 May 2019 93/4-18
[166] FBK000059_003
[167] Keith Niven 24 January 2018 60/18-61/3
[168] An IP (Internet Protocol) address is a number assigned to a device connected to a computer network.

the report might relate to a single person using multiple devices or relate to multiple suspects and victims. Reports to NCMEC have increased from approximately 110,000 reports in 2004 to over 18.4 million reports in 2018.[169]

36. NCMEC's systems analyse the CyberTip report to identify the location for the IP address and NCMEC make that information known to the appropriate law enforcement agency. Where the incident or offender is believed to be based in the UK, NCMEC sends a referral to the NCA and these referrals are downloaded daily.[170] Where the referral is urgent, there is an out-of-hours arrangement that enables the NCA to deal with the report.

37. The majority of reports received by the NCA come from NCMEC. As a result of the increase in detection and reporting of child sexual abuse material to NCMEC, there has been an increase in the volume of referrals to the NCA.[171]

Table 1 UK industry reports of child sexual abuse material

Year	*Number of UK industry reports of child sexual abuse material*
2009	*1,591*
2010	*6,130*
2011	*8,622*
2012	*10,384*
2013	*11,477*
2014	*12,303*
2015	*27,232*
2016	*43,072*
2017	*82,109*
2018	*113,948**

**This figure includes 46,1468* [corrected figure: 46,148] *non-actionable referrals sifted out by NCMEC prior to dissemination to UK, in 2018, NCMEC deployed analytical capability focusing on UK referrals. This followed an NCA grant to NCMEC. The non-actionable content has been included to ensure the comparison is like with like in respect of previous years.*

Source: NCA000363_010

38. Although there were nearly 114,000 reports in 2018, this does not mean there were nearly 114,000 offenders in the UK.[172] The figures in Table 1 include what are known as non-actionable referrals. Mr Robert Jones, Director of Threat Leadership for the NCA, explained that not all referrals will identify a criminal offence or offender. For example, some reports will contain information only (described as informational reports). In some cases it is not possible, based on the information provided by the service providers, to geolocate an IP address.[173] In other instances the IP address might lead to multiple users, which means that the precise identity of the perpetrator cannot be ascertained.

[169] NCA000363_010
[170] NCA000163_027
[171] NCA000363_010-011
[172] Robert Jones 20 May 2019 15/4-8
[173] Geolocation of an IP address is the process of identifying the location where the internet is being accessed, whether on a computer or a mobile device.

Action taken by UK law enforcement

39. Staff at the NCA's Referrals Bureau assess the CyberTip report to determine the nature of the offending and the identity or location of the perpetrator. They also ascertain whether there is ongoing risk and threat to a child. The results are graded, one to three. Grade one involves an immediate threat to the life of a child and such reports are prioritised and actioned *"as soon as is possible"*.[174] Grade two cases concern a serious crime against a child and are actioned *"as soon as possible, but in any case within two days"*.[175] Grade three referrals will be prioritised after grades one and two and are generally dealt with by local police forces based on geolocation.

40. Inevitably, the increased referrals to the NCA have led to an increase in the number of cases allocated to local policing.

> **40.1.** Kent Police received 50 referrals from the NCA in 2013. This increased in 2017 to 258 referrals – a 400 percent increase.[176]
>
> **40.2.** West Midlands Police provided the number of referrals from the NCA and the time taken in days by West Midlands Police to deal with such referrals:[177]

Table 2 **NCA referrals to West Midlands Police**

Year	No. of NCA referrals	Time taken to deal with referral		
		Average (days)	Shortest (days)	Longest (days)
2013	161	5	1	46
2018	433	20	1	174
2019 (Jan to May)	186	16	1	105

Child Abuse Image Database

41. When investigating child sexual abuse offences, and in particular online-facilitated offending, police routinely seize a suspect's digital devices, including any mobile phone, computer and tablet. These devices are then examined for the presence of indecent images of children.

42. The increase in NCA referrals, coupled with the increased reporting of sexual offences more generally, led to significant demands being placed on the police teams dealing with such allegations and to delays in examination of digital devices. For example, in December 2014, Greater Manchester Police encountered lengthy delays in having devices examined, as can be seen from Table 3.[178]

[174] Keith Niven 24 January 2018 26/12
[175] Keith Niven 24 January 2018 26/16-17
[176] OHY003413_009
[177] OHY003315_019; OHY008692_002
[178] OHY003286_009

Table 3 Digital device examinations backlog, Greater Manchester Police December 2014

Type of case	*Number of cases*	*Oldest case*
Standard computer examinations	*74*	*61 weeks*
Urgent computer examinations	*32*	*16 weeks*
Standard telephone examinations	*905*	*7 weeks*
Urgent telephone examinations	*10*	*2 weeks*

Source: OHY003286_009

43. In 2014 and 2015, in order to manage the delays in having devices analysed, Greater Manchester Police spent an additional £400,000 in outsourcing digital examinations of devices.[179]

44. Police and digital examination departments often found the same image on different devices and so in 2014 the Home Office announced it had created a "*single secure database of illegal images of children*",[180] known as the Child Abuse Image Database (CAID). All UK police forces and the NCA have access to CAID, which contains the images and hash values (the digital fingerprint) of indecent images.

45. When a device is seized from a suspect, police will use CAID to identify known indecent images of children. If the device contains previously unidentified images, those images are hashed, added to CAID and categorised into one of three categories:[181]

- Category A includes images involving penetrative sexual activity.
- Category B includes images involving non-penetrative sexual activity.
- Category C includes other indecent images that do not fall within categories A and B.

46. CAID records the results of the categorisation and produces a report on the number of hashed images in each category. The use of CAID therefore helps to reduce the demand on forensic services as, in future, police examiners no longer have to review that image. Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, said that CAID "*has made a really big difference in terms of the amount of hours that officers and members of staff have to view these most awful images*".[182] By January 2019, there were over 13 million child abuse images in CAID.[183]

47. Mr Christian Papaleontiou, Head of the Home Office's Tackling Exploitation and Abuse Unit, explained that the CAID Innovation Lab was working to enhance CAID over the course of 2019 and 2020 by developing:

- a new algorithm "*to identify known IIOC images within minutes*";[184]

[179] OHY003286_009
[180] HOM003247_017
[181] Current sentencing practice requires the image to be categorised in order that the Court may determine the seriousness of the offence: https://www.sentencingcouncil.org.uk/offences/crown-court/item/possession-of-indecent-photograph-of-child/
[182] Simon Bailey 24 January 2018 128/20-23
[183] HOM003247_019
[184] Christian Papaleontiou 22 May 2019 30/21; 'IIOC' means indecent images of children.

- "*an auto-categorisation of images using AI which is used to grade the severity of child sexual abuse material*";[185] and
- "*scene matching – again, using artificial intelligence and data analytics – which allows better identification of victims and the threat an offender may pose to children*".[186]

48. Although the IWF has access to CAID,[187] it is presently unable to run CAID hashes through its crawlers, thereby limiting the IWF's ability to proactively search the internet for known images of child sexual abuse. As Ms Hargreaves said, "*if we could, given that there are potentially 10 million images in CAID … we would be able to massively increase our ability to bring down content*".[188] We encourage resolution of this issue.

Sharing of indecent images of children between offenders

49. Prior to the formation of the NCA in 2013, the Child Exploitation and Online Protection Centre (CEOP) conducted a number of policing operations focussed on apprehending those individuals who downloaded and shared indecent images of children.

50. The first nationally coordinated approach between the NCA and local policing aimed at targeting those individuals sharing indecent images of children was conducted in 2014.[189] Operation Notarise "*had two main objectives: to rescue children from abuse and to identify previously unknown child sex offenders*".[190] As a result of Operation Notarise (which ran from April to December 2014), 787 arrests were made, 9,685 devices were seized, 518 children were safeguarded or protected, and 107 suspects who were registered sex offenders or who had a conviction or allegation for a contact child sexual abuse offence were identified.[191]

51. In February 2015, the then Deputy Director General of the NCA wrote to the then Chair of the NPCC, suggesting that there needed to be "*more improvement in relation to a nationally coordinated response in relation to online CSEA*".[192] As a result of that letter, the NCA and NPCC devised a response plan for national, regional and local policing to six identifiable online threats.[193] One of those threats was the growing number of individuals sharing indecent images of children.

52. Law enforcement proactively uses sensitive detection techniques to identify offenders who share indecent images of children. Once a perpetrator has been identified, the NCA and police use a prioritisation tool known as KIRAT[194] (Kent Internet Risk Assessment Tool) to identify those offenders who are more likely to commit contact sexual abuse. KIRAT assesses the offender as low, medium, high or very high risk. Perpetrators assessed as high and very high risk are investigated and arrested as a matter of priority.

53. Mr Keith Niven, Deputy Director Support to the NCA, told us that the current KIRAT tool was evaluated in 2015 and successfully identified the most dangerous offenders. Ninety-seven percent of contact offenders were assessed as 'very high' or 'high' risk and

[185] Christian Papaleontiou 22 May 2019 30/25-31/2
[186] Christian Papaleontiou 22 May 2019 31/10-13
[187] HOM003272_002
[188] Susie Hargreaves 17 May 2019 112/2-6
[189] Keith Niven 24 January 2018 13/3-11
[190] Keith Niven 24 January 2018 13/12-14
[191] Keith Niven 24 January 2018 13/15-21
[192] Keith Niven 24 January 2018 7/16-18
[193] NCA000164
[194] KIRAT is also used by the EU member states as well as Australia, New Zealand, Israel and Canada.

the overall correct prediction rate was 83.7 percent.[195] When asked about the percentage of cases where KIRAT did not accurately assess the risk of the offender committing contact abuse, Mr Niven stressed that KIRAT was not the sole way in which officers sought to prioritise the case:

> "*we are not saying 'That's the tool. Use it religiously'. We are saying 'Use it as a guide and then use your own judgement as well and any further enquiries that may be required'.*"[196]

54. There are no national directives which require a police force to respond to a KIRAT risk assessment within certain timescales.

54.1. Kent Police has the following guidelines:

- very high risk: respond within 24 hours;
- high risk: respond within a maximum of 7 days;
- medium risk: respond within 14 days; and
- low risk: respond within 30 days.

Anthony Blaker, Assistant Chief Constable of Kent Police, said that referrals involving an immediate risk of harm had led to arrests "*within a matter of hours*".[197] Where the suspect had no identifiable access to children and had a KIRAT grading of low risk, Mr Blaker said in his statement that, as at October 2017, "*it is not uncommon … for several months to pass between receipt of referral and execution of a search warrant and/or arrest or other investigative action*".[198]

54.2. Mark Webster, Assistant Chief Constable of Cumbria Constabulary, said that his force met the expectation that a 'very high risk' case is responded to within 24 hours. In a 'high risk' case, Cumbria Constabulary's average response time was 5.6 days, in a 'medium risk' case it was 8.2 days, and in a 'low risk' case it was 11.3 days.[199]

55. The Inquiry's Rapid Evidence Assessment (REA) into the behaviour and characteristics of perpetrators[200] considered the extent of research as to whether those who offend online also commit, or are more likely to commit, a contact sexual offence. The REA found that:

> "*research findings about the cross-over offending between online and contact offences are mixed. The research studies conclude that most offenders do not cross over, or evolve from online-only to contact or dual offending*".[201]

[195] Keith Niven 24 January 2018 10/14-22

[196] Keith Niven 24 January 2018 11/4-7

[197] Anthony Blaker 25 January 2018 76/19

[198] Anthony Blaker 25 January 2018 76/23-77/2

[199] Mark Webster 26 January 2018 19/18-25

[200] Rapid Evidence Assessment: *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation*

[201] Rapid Evidence Assessment: *Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation* p39. Dual offending refers to those offenders who engage in both online and contact child sexual abuse.

56. Mr Jim Gamble QPM, a former Deputy Director General of the National Crime Squad[202] and former Head of CEOP, expressed his concern about whether policing should differentiate between online only and offline only (ie contact) offenders. He accepted that there needed to be prioritisation using a "*risk-based approach on the basis of the current funding and current resourcing*".[203] However, Mr Gamble's view was that:

> "*if you have a deviant sexual interest in looking at an image … you are likely to have already abused a child or may do so in the future on the basis of whether you think you can get away with it or not. To risk assess on the basis of what an individual has looked at just doesn't make sense and it doesn't bear out experience in my opinion.*"[204]

57. Ms Tink Palmer, Chief Executive Officer of the Marie Collins Foundation,[205] told us that in her experience:

> "*If I were to look at the majority of the cases I have either been involved with myself or acted as a consultant, I would say at least about 65 to 70 per cent there's been activities both online and offline.*"[206]

58. There may therefore be a dissonance between what the research indicates and the practical experiences of those who work in this area. There is clearly a need for law enforcement to prioritise its response, focussing on those offenders who are intent on committing contact offences, but this should not preclude pursuing any offender who views indecent images of children. There is also a need to focus on preventative measures that can be deployed by industry, which should reduce the burden on hard-pressed law enforcement agencies.

59. No witness suggested to us that the number of indecent images of children being viewed or shared was likely to fall.

60. Chief Constable Bailey told us that the police had reached "*saturation point*".[207] In early 2017 he made the same point in a number of press interviews,[208] in which he had said that the police and criminal justice system were "*not coping*"[209] even though "*400, 450, almost exclusively men, are being arrested, every month*".[210] In response to the Home Affairs Committee's request to explain his comments,[211] Chief Constable Bailey suggested a number of steps to combat the threat of online child sexual abuse:

- industry to do more to prevent this material being streamed on their platforms and services;
- more education for children about risks online; and
- a law enforcement response which "*prioritises and proactively targets those offenders at highest risk of contact offending*".[212]

[202] Until its merger into the Serious Organised Crime Agency in 2006, the National Crime Squad was the police agency responsible for organised and major crime.
[203] Jim Gamble 23 January 2018 24/22-23
[204] Jim Gamble 23 January 2018 24/8-16
[205] The Marie Collins Foundation is a UK-based charity which works with victims of online-facilitated child sexual abuse and their families.
[206] Tink Palmer 22 January 2018 123/9-13
[207] Simon Bailey 24 January 2018 102/6-7; Simon Bailey 20 May 2019 110/22
[208] OHY002228_001
[209] OHY002228_001
[210] Simon Bailey 20 May 2019 111/8-9
[211] OHY002228
[212] OHY002229

61. He said that, in his experience, a large proportion of those offenders being dealt with for the viewing of indecent images of children did not receive an immediate custodial sentence and for those offenders who did go to prison very few received any form of rehabilitation to address their underlying problem. It was against this background that he wanted to stimulate debate about whether "*alternative outcomes*"[213] for some types of offenders ought to be considered.

Alternative proposals for dealing with indecent image offences

62. Some witnesses suggested that a change of approach might be appropriate.

62.1. The personal view of Chief Constable Bailey (ie not in his role as NPCC Lead) was that, rather than going to court, low-risk offenders who had admitted indecent image offences could be subject to conditional cautioning with, for example, a requirement to submit to a rehabilitation and treatment programme. The offender would still be subject to notification requirements of the sex offenders register and the offence would still be registered with the Disclosure and Barring Service.[214] If the offender breached the conditions, the offender could be prosecuted for the original offence.[215] Chief Constable Bailey recognised that such a proposal "*instantly creates a real sense of anger, that there is the National Police Chiefs' Council lead for this going soft on paedophiles*"[216] and that this might simply shift the burden to a different agency or part of the criminal justice system. However, he considered that the number of individuals arrested each month demonstrated the commitment of the police to bring these perpetrators to justice. He added:

> "*I would much rather have the offender having to confront their offending behaviour and maybe they would stop viewing indecent images as a result.*"[217]

62.2. Mr Gamble agreed that police "*can't simply arrest our way out*"[218] of the scale of offending and that there may be some offenders who should be diverted away from the criminal justice system. However, he considered that the police should arrest more offenders in order to "*create a credible deterrent*"[219] and that the primary issue was that there needed to be "*actual real investment being made in the tactical options that we choose to use that minimise opportunities for offenders online*".[220]

62.3. Debbie Ford, Assistant Chief Constable of Greater Manchester Police (GMP), said "*Arresting our way out of the problem is clearly unrealistic*".[221] She also told us that the actual level of risk posed by an offender often is not known until after the offender has been arrested and further investigations undertaken, including the examination of any devices seized.

[213] Simon Bailey 24 January 2018 104/1
[214] The Disclosure and Barring Service (DBS) operates to assist employers in making safer recruitment decisions by preventing those who pose a risk of abuse to children from working with them.
[215] Simon Bailey 24 January 2018 107/1-109/12
[216] Simon Bailey 24 January 2018 104/3-5
[217] Simon Bailey 24 January 2018 111/3-5
[218] Jim Gamble 23 January 2018 28/10
[219] Jim Gamble 23 January 2018 28/11-12
[220] Jim Gamble 23 January 2018 34/20-22
[221] OHY003286_075

> *"The question therefore remains how confident can we be of categorising low-risk offenders at the intelligence stage? GMP has illustrative examples where offenders make admissions and plead guilty to charges to mask the actual gravity of their wider offending … By adopting alternative disposal methods at an early stage, we run a real risk of allowing potential high-risk offenders to slip the net."*[222]

62.4. Commander Richard Smith, the professional lead for child safeguarding for the Metropolitan Police Service, was of the view that "*demand will rapidly outstrip the resources that we have, and so a whole-systems approach is required with much more focus on preventing it*".[223] He said that the problem is particularly acute within the Metropolitan Police Service given "*the significant and continuing ongoing terrorist threat*"[224] and because, by 2020/21, it "*is required to reduce revenue across all of its policing expenditure by 400 million*".[225]

63. In 2015/16, the Home Office ran a pilot to test the practicalities of diverting low-risk offenders who "*had to have no previous offences, no unsupervised access to children*".[226] Mr Papaleontiou said that the pilot highlighted three problems:[227]

- the diversion scheme may have been more resource-intensive than prosecuting the individual through the criminal justice system;
- the crimes and potential sentences were themselves too serious to make it appropriate to issue a conditional caution; and
- there were concerns about how an offender would be deemed to be low risk.

The Home Office recognised that the viewing of indecent imagery "*still has a very direct and indirect impact on the victims*" and that there is a "*need for justice to be served in terms of victim impact*"[228] by ensuring that a conviction is recorded.

64. In June 2019, Justice (the law reform and human rights organisation) published its working party report *Prosecuting Sexual Offences*. It proposed a diversion scheme for those offenders who had viewed indecent images of children.

> *"The programme ought to be designed purely to educate and assist with moving forward in a pro-social manner, rather than to shame and punish, since this has been shown to be ineffective."*[229]

The report includes details about the criteria for participation in the diversion scheme, and its structure and management. The report considers that the pilot should be evaluated after three years.

65. Based on the evidence we heard in this investigation, there was no consensus as to whether, and what, alternative proposals should be considered for dealing with the so-called 'low risk' offenders who view indecent imagery.

[222] Debbie Ford 25 January 2018 131/2-11
[223] Richard Smith 25 January 2018 43/25-44/3
[224] Richard Smith 25 January 2018 41/7-10
[225] Richard Smith 25 January 2018 41/2-5
[226] HOM003247_019
[227] Christian Papaleontiou 22 May 2019 35/18-37/16
[228] Christian Papaleontiou 22 May 2019 37/10-16
[229] https://justice.org.uk/wp-content/uploads/2019/06/Prosecuting-Sexual-Offences-Report.pdf p42

66. While law enforcement cannot arrest its way out of this problem, that is true in respect of many criminal offences. It would undoubtedly assist law enforcement if offenders were prevented from accessing this material at the outset – it is clear that the increase in the number of indecent images of children offences is driven by images of child sexual abuse being too easily accessible. A greater focus on prevention is required.

C.3: Preventing access to indecent images of children

67. Given the concern about the growing scale of offending, the Inquiry considered the ways in which industry and government currently prevent perpetrators from accessing indecent images of children and the proposals for future technological developments.

Hash list

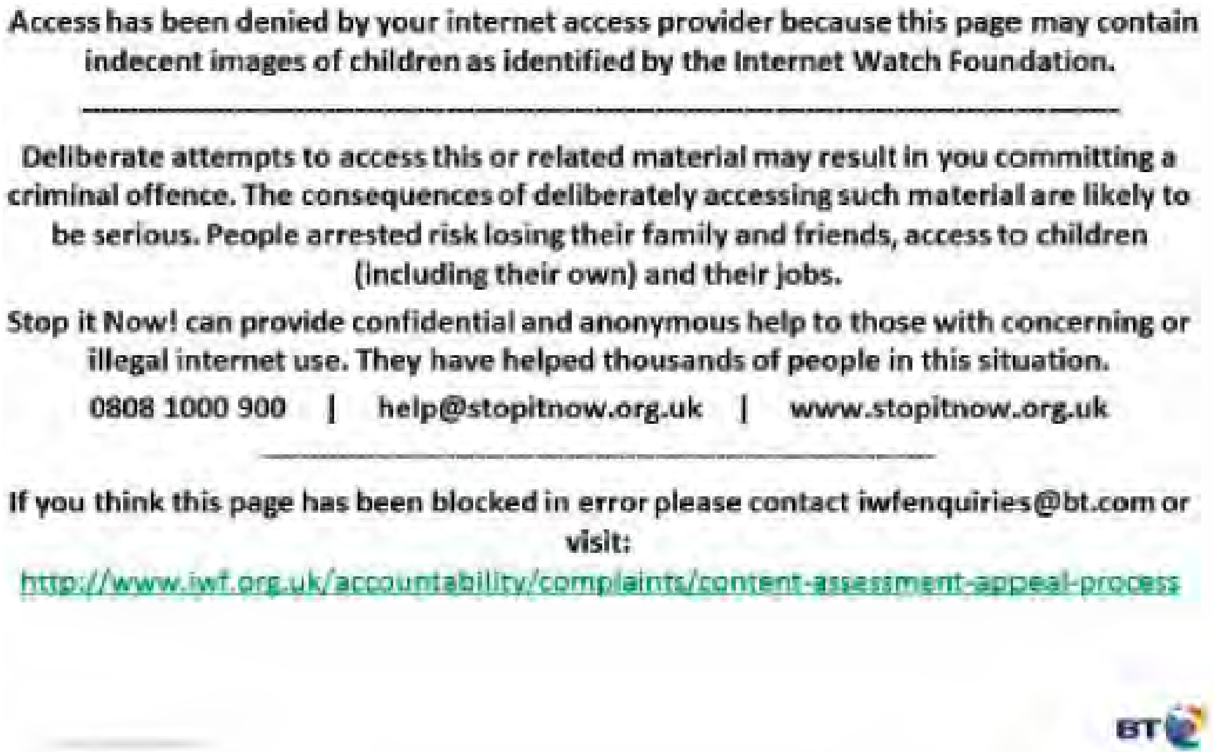
68. As explained above, the IWF operates a hash list. This is a separate list to the list of hashes within CAID. At present the IWF cannot share CAID hashes with any UK company but can share CAID hashes with six US companies. Ms Hargreaves explained that the hashes cannot be shared because the Information Commissioner's Office (ICO) has classified hashes as personal data within the meaning of the General Data Protection Regulation (GDPR).[230] The IWF is working with the Home Office, the NCA and the ICO to see if this obstacle can be overcome, which has the potential to increase the pool of known child sexual abuse images that can be detected in proactive searches.[231]

Blocking access to URLs

69. The IWF's URL list identifies those web pages where the IWF has found images or videos of child sexual abuse. The URL list is provided to industry members so that they can block access to those web pages. It is used by around 70 companies, including Google, BT and Microsoft. Once the indecent imagery is removed from the web page, the web page is removed from the URL list. The URL list is updated twice a day. Ms Hargreaves said that on the day she gave evidence, 17 May 2019, there were 5,800 URLs on the list "*which is pretty average*"[232] but that there had been as many as 12,000 URLs on the list.

70. Kevin Brown, Managing Director of BT Security, explained that by 2004 BT had developed a blocking tool called Cleanfeed, which downloaded the latest IWF URL list. If a BT customer tried to access a website that was on the URL list, access to that website would be blocked. Since approximately 2013, a warning message is displayed on-screen "*alerting customers to the fact that they have accessed a site that has been deemed as hosting indecent images*".[233]

[230] Personal data is information that relates to an identified or identifiable individual: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
[231] Susie Hargreaves 17 May 2019 113/4-114/3
[232] Susie Hargreaves 17 May 2019 106/2
[233] Kevin Brown 17 May 2019 16/6-8



Access has been denied by your internet access provider because this page may contain indecent images of children as identified by the Internet Watch Foundation.

Deliberate attempts to access this or related material may result in you committing a criminal offence. The consequences of deliberately accessing such material are likely to be serious. People arrested risk losing their family and friends, access to children (including their own) and their jobs.

Stop it Now! can provide confidential and anonymous help to those with concerning or illegal internet use. They have helped thousands of people in this situation.

0808 1000 900 | help@stopitnow.org.uk | www.stopitnow.org.uk

If you think this page has been blocked in error please contact iwfenquiries@bt.com or visit:

http://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process

Example of warning message for blocked website

Source: BTG000003_018

71. In 2015, BT conducted a one-off exercise to try and establish the number of times that BT blocked access to child sexual abuse imagery in the UK. Between January and November 2015, "*the average number of attempts to retrieve the CSA image was 36,738 every 24 hours*".[234]

72. Cleanfeed is automatically applied to all internet traffic delivered by BT, including BTnet customers such as Plusnet. Mr Brown told us that EE uses a blocking platform called Wolf which works in the same way as Cleanfeed.[235]

73. Facebook began discussing the use of the URL list with the IWF in 2014 but as at the public hearing in May 2019 still had not adopted the list. Both Facebook and the IWF were asked why it seemed that little progress had been made in the intervening five years. Ms de Bailliencourt said that it was a UK-based employee who in 2014 first started discussions with the IWF but that:

> *"At some time, there were other projects which were implemented ahead of the list … so I reinitiated those conversations, probably a year and a half ago, and we have been working on making this happen."*[236]

Ms Hargreaves stated that when Facebook first approached the IWF in relation to the URL list it was because Facebook "*wanted to use it for monitoring purposes, which is not a designated use of our list*".[237]

74. On 25 September 2019, Facebook stated that it had reached an agreement with the IWF and "*look forward to deploying* [the URL list] *soon*".[238]

[234] Kevin Brown 17 May 2019 20/5-7
[235] Kevin Brown 17 May 2019 14/13-16
[236] Julie de Bailliencourt 14 May 2019 82/9-16
[237] Susie Hargreaves 17 May 2019 123/3-4
[238] FBK000059_004

75. The use of the URL list is vital in the efforts to prevent access to child sexual abuse imagery. It is difficult to understand why Facebook did not deal with this matter sooner.

Keywords lists

76. Perpetrators often create their own search terms for finding and hiding indecent images of children. Ms Hargreaves told us that this language can include "*a series of numbers or exclamation marks or different languages or weird terms*".[239]

77. The IWF has therefore created a list of keywords which is available to its members, particularly those who operate internet search facilities or moderate content. This enables organisations to block a search for such material. Ms Hargreaves told us that, by May 2019, there were "*just under 500 key words*" on the list.[240] The IWF has another "*8500 that we just do not have the resource to assess at the moment*".[241]

Other measures

78. The Inquiry also heard about work undertaken between the NCA and Visa Europe, whereby Visa Europe sponsored NCA financial investigation officers to help prevent the use of payment cards to purchase indecent images of children. Mr Jones told us that "*the use of mainstream payment mechanisms … has been virtually eradicated from the mainstream providers*".[242] This appears to be an example of good collaborative practice.

C.4: Media reporting

79. In late 2018 and early 2019, a number of articles appeared in the media alleging that Google,[243] Microsoft[244] and Facebook[245] were allowing their services to be used by offenders to share child sexual abuse images and groom children. In advance of the hearing, the Inquiry provided witnesses from these companies with these articles, in order that they could respond to the contents.

80. In relation to Microsoft, one article stated that when terms such as 'porn kids' or 'nude family kids' were typed into Bing (Microsoft's search engine), indecent images of children were returned in the results. Microsoft's own investigations suggested that the images were not in fact illegal images but were sexually explicit images of individuals over the age of 18. As a result of the article, Microsoft made changes to Bing to ensure that adult content was not returned when search queries related to child sexual abuse or exploitation were made.

81. The article also stated that when seemingly innocent search terms were used, Bing auto-suggested search terms which led to indecent images. Microsoft accepted that common search terms should not deliver "*suboptimal results*".[246] Mr Milward said that this article had prompted Microsoft to "*fundamentally sit down and rethink the way in which we were devoting engineering attention to the challenge that we face here*".[247]

[239] Susie Hargreaves 17 May 2019 114/15-17
[240] Susie Hargreaves 17 May 2019 114/21
[241] Susie Hargreaves 17 May 2019 114/22-23
[242] NCA000363_016
[243] INQ004185
[244] INQ004187_001-002
[245] INQ004190
[246] Hugh Milward 15 May 2019 116/6
[247] Hugh Milward 15 May 2019 118/1-3

82. In December 2018, an article on the BBC news website[248] stated that apps were available to download on the Google Play Store which directed users to WhatsApp groups that were being used to share child sexual abuse images. On behalf of Google, Ms Canegallo explained[249] that a prospective app is reviewed before it is uploaded to the store to ensure it does not violate Google's policies. It is then subject to periodic reviews and would also be reviewed if a user flagged the app for a suspected breach of policy. Ms Canegallo said she was confident that had such material been present at the initial review, the app would not have been available in the app store.[250] Despite the review process, however, it would appear that, in this example, the review did not detect the material. Google told us that, once aware of the issues raised in the article, the apps were suspended from the Google Play Store and the developer accounts were terminated. Two reports were made to NCMEC due to the content of the apps.

83. Following the BBC article, investigations[251] into WhatsApp revealed WhatsApp groups with names such as 'Only Child Pornography' and 'Gay Kids Sex Only'. The article stated that a WhatsApp spokesperson had said:

> *"Recent reports have shown that both app stores and communications services are being misused to spread abusive content, which is why technology companies must work together to stop it."*[252]

84. When asked how WhatsApp prevents a group from having such titles and from sharing indecent imagery, Ms de Bailliencourt told us that WhatsApp uses PhotoDNA and has "*some proactive detection mechanism in place to flag and pull down anything that may – that may appear to be of this nature*".[253]

85. One of the factors that prompted internet companies to review their current procedures, or consider future improvements, appears to be the reputational damage caused by adverse media reporting. Some changes we heard about were made as a result of negative publicity which impacts on their business model. It is this impact that seemingly drives or expedites revision and innovation as much as a concerted commitment to prevent access to indecent images of children.

C.5: Future proposals

Pre-screening or pre-filtering

86. In March 2018, the NCA gave evidence before the Home Affairs Select Committee Inquiry into 'Policing for the Future'. The NCA set out "*three asks that were made of industry*".[254] The first of those requests related to pre-screening or pre-filtering of known and unknown imagery to prevent indecent images offences occurring in the first place.

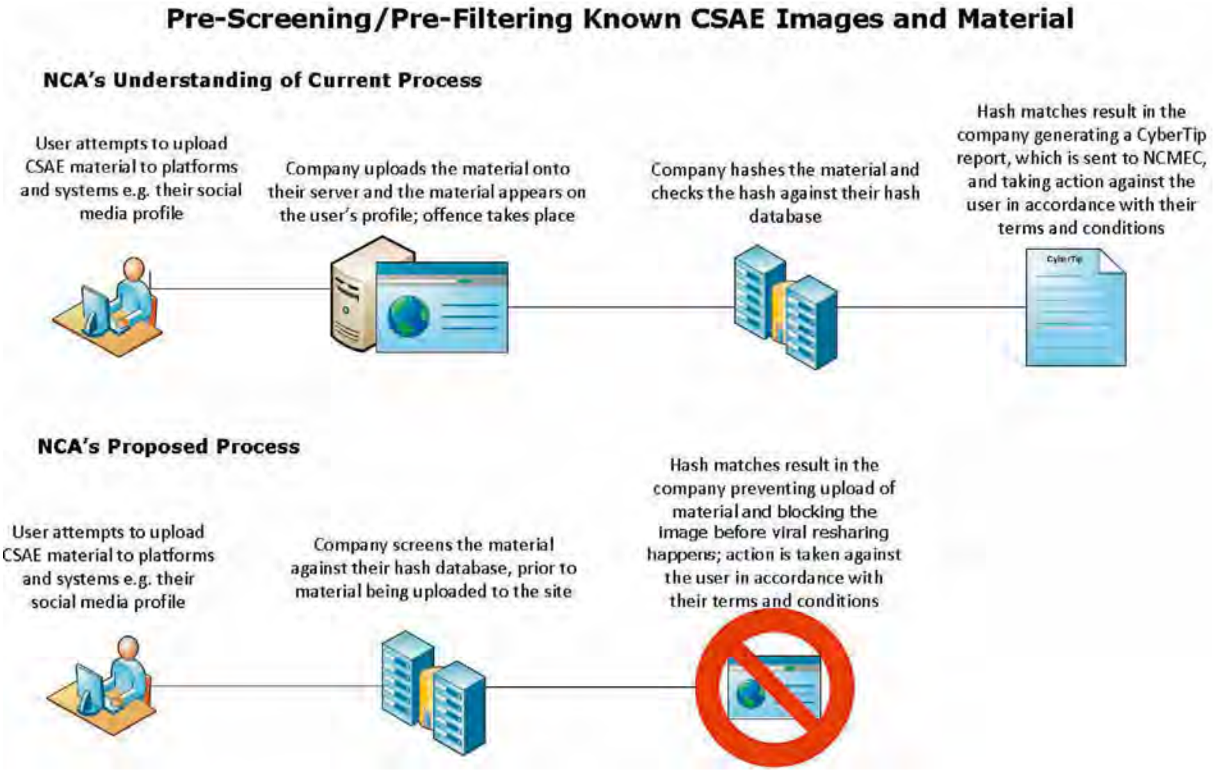
[248] INQ004185
[249] Kristie Canegallo 16 May 2019 72/23-75/10
[250] Kristie Canegallo 16 May 2019 75/20-24
[251] The investigations were carried out by AntiToxin Technologies, an Israeli online safety organisation.
[252] INQ004190_004
[253] Julie de Bailliencourt 14 May 2019 95/25-96/3
[254] Robert Jones 20 May 2019 35/5-6

87. In relation to known imagery, Mr Jones said:

> "*you can stop an offender from accessing a known image because it's been hashed, it's detectable, it's an illegal commodity which is moving digitally. So if you prevent access to that, you prevent an offence. It's as simple as that.*"[255]

88. In November 2019, the NCA stated that it was still possible to access known child sexual abuse imagery on "*mainstream*" search engines within just "*three clicks*".[256]

89. The essence of the NCA's proposal is for an internet company to scan the image against their hash database prior to the image being uploaded. If the image is identified as a known indecent image, it can then be prevented from being uploaded. The graphic below sets out the current screening process and the proposed process when pre-screening or pre-filtering is used:


Pre-Screening/Pre-Filtering Known CSAE Images and Material
NCA's Understanding of Current Process
User attempts to upload CSAE material to platforms and systems e.g. their social media profile
Company uploads the material onto their server and the material appears on the user's profile; offence takes place
Company hashes the material and checks the hash against their hash database
Hash matches result in the company generating a CyberTip report, which is sent to NCMEC, and taking action against the user in accordance with their terms and conditions
CyberTip
NCA's Proposed Process
User attempts to upload CSAE material to platforms and systems e.g. their social media profile
Company screens the material against their hash database, prior to material being uploaded to the site
Hash matches result in the company preventing upload of material and blocking the image before viral resharing happens; action is taken against the user in accordance with their terms and conditions

Current indecent image screening process and NCA's proposed process

Source: NCA000366

90. Mr Jones explained that the introduction of 5G will enable quicker upload and download speeds with a consequential increase in the speed at which indecent imagery can be shared. The NCA considers that if pre-screening or pre-filtering is used by companies to prevent access to the imagery at the outset, it will allow law enforcement the "*capacity and capability to chase first-generation images and safeguard children as quickly as possible*".[257] The internet companies could then use their classifier technology to identify previously unknown child sexual abuse material and first-generation images. These images would be hashed and incorporated into the NCMEC database thereby expanding the pool of images that could be prevented from being accessed.

[255] Robert Jones 20 May 2019 36/9-13
[256] NCA000376_003
[257] Robert Jones 20 May 2019 36/23-25

91. Google agreed that pre-filtering was a "*proactive*" approach that "*prevents the offending material from being disseminated*"[258] but said that the image needed to be uploaded (or found by a Google search on another website) in order for their image classifiers to be used.[259] Ms Canegallo stated that Google "*has not come to a conclusion on* [the] *feasibility or efficacy*" but she thought that pre-filtering "*presents serious technological and security challenges*".[260]

92. Ms de Bailliencourt was aware of the NCA's request for pre-screening and was asked "*What steps, if any, are Facebook taking to prevent the image being uploaded at the outset?*" She replied:

> "*we didn't develop PhotoDNA … Microsoft developed the technology, so they may be better placed to provide additional insights here. I know the way it is working on the platform would generally move so quickly that it's really a matter of seconds before its removal.*" [261]

Ms de Bailliencourt's answer was that, given the obligation to report any child sexual abuse material to NCMEC and the potential for an individual to be arrested, Facebook "*need to make sure that we have reasonable conclusion that the content was uploaded and is indeed matching any of the hashes that we have*".[262] As a result, we remain unsure about Facebook's position in relation to pre-screening indecent images of children.

93. Apple considered that filtering known child sexual abuse material images was "*effective*".[263]

94. Microsoft explained that it screens for known indecent images of children at the point at which the image is shared and that "*applying PhotoDNA at that point is actually very fast*".[264] Mr Milward explained that Microsoft:

> "*feel that the invasion of privacy around routinely screening people's private files and folders would not be accepted by the general public as being an appropriate level of intrusion by a technology company*".[265]

95. No industry witness said that it was technologically impossible to pre-screen their platforms and services. PhotoDNA is efficient in detecting a known indecent image once it has been uploaded but it is important to try and prevent the image being uploaded in the first place and thereby prevent access. The use of pre-screening or pre-filtering should be encouraged in order to fulfil the government's expectation that "*child sexual abuse material should be blocked as soon as companies detect it being uploaded*".[266] This is a key aspect of the preventative approach that is necessary.

[258] GOO000049_003
[259] GOO000049_003
[260] GOO000049_003
[261] Julie de Bailliencourt 14 May 2019 79/6-13
[262] Julie de Bailliencourt 14 May 2019 79/18-20
[263] Melissa Polinsky 15 May 2019 60/13
[264] Hugh Milward 16 May 2019 28/23-24
[265] Hugh Milward 16 May 2019 28/7-11
[266] HOM003253_030

Self-generated imagery

96. The ease and frequency with which children can share self-generated indecent imagery is all too apparent.

96.1. The government's *Online Harms White Paper* (published in April 2019)[267] refers to surveys that indicate between 26 percent and 38 percent of 14 to 17-year-olds have sent sexual images to a partner and between 12 percent and 49 percent have received a sexual image.

96.2. The IWF states that self-generated imagery now makes up one-third of the child sexual abuse material that it removes from the internet. Of that one-third, 82 percent of the imagery features 11 to 13-year-olds, with the overwhelming majority featuring images of girls.[268]

96.3. In Greater Manchester, children are recorded as the offender in nearly half of all indecent images of children offences.[269] In Cumbria, "*in the last three financial years, children make up the largest group of suspects recorded*" for indecent images of children offences.[270]

96.4. The *Learning about online sexual harm* research report stated that "*The issue of sexual images received considerable attention among interview and focus group participants*".[271] The children told the researchers about how they and/or their peers received unsolicited explicit messages (primarily sent by males to females) and requests to send someone nude images. As one 14-year-old interviewee said:

> "*I don't think my dad realises how many messages from random boys I get or how many dick pics I get. And I have to deal with it every day … it's kind of like a normal thing for girls now … I've been in conversations [online] like, 'Hi. Hi. Nudes?' I'm like, 'No' … yeah, it literally happens that quickly. Like, 'What's your age?' And you'll say how old you are, you're underage, and they'll be like, 'Oh OK', and then they'll ask for pictures.*"[272]

97. The Protection of Children Act 1978 criminalises the making, taking or distribution of an indecent image of a child irrespective of the circumstances in which the image is taken. Where, for example, sexual images are shared between two 16-year-olds who are, legally, sexually active, both are committing a criminal offence and could be prosecuted.

98. Chief Constable Bailey explained that, in conjunction with the Home Office, 'Outcome 21' was devised in response to the concern that:

> "*children were becoming criminalised, and as a result their life chances were then going to be significantly undermined because the Disclosure and Barring Service would then disclose if they wanted to become a police officer or a nurse or a social worker*".[273]

[267] INQ004232_023
[268] https://www.iwf.org.uk/sites/default/files/inline-files/IWF%20Online%20Harms%20White%20Paper%20Response.pdf p6
[269] OHY003286_018
[270] OHY002285_016
[271] *Learning about online sexual harm* p5
[272] *Learning about online sexual harm* p5
[273] Simon Bailey 24 January 2018 151/4-8

Outcome 21 enables police to record that a crime has been committed but the child is not prosecuted on the basis it is not in the public interest to do so.[274] Outcome 21 is only used where there are no aggravating factors, such as where the sharing of the image is not as a result of blackmail or extortion. Outcome 21 is therefore a sensible response to a very real problem.

99. The Inquiry heard about a joint NCA, IWF, National Society for the Prevention of Cruelty to Children (NSPCC), NCMEC and Home Office initiative called 'Report Remove'. The aim of Report Remove is to enable a child to report a self-generated image and request that the image be taken down. As Mr Jones said:

> "*we've … come up with a viable system that will allow us to quarantine the image, prevent the image from being shared amongst sex offenders, safeguard the child, who may need help and advice, and not criminalise them*".[275]

In reporting the image, the child will not be directed to law enforcement. The procedure is being designed to ensure that once the image is hashed it is flagged as a 'Report Remove' image. This will ensure that NCMEC and, subsequently, the NCA know that this is an image that has come from this initiative where the victim's identity is known.

Age verification

100. The Inquiry heard evidence that child sexual abuse material relating to older children is often found in public forums on the internet, including on adult pornography websites. Professor Warren Binford, a trustee of Child Redress International (CRI),[276] gave an example whereby 60 variations of an image of a pubescent victim were posted to 538,729 unique URLs and 99 per cent of those URLs were found on 14 adult sites.[277]

101. Chief Constable Bailey told us that "*the greatest percentage of people now viewing online is not, as I think an awful lot of people would perceive it to be, in the 40s and 50s, it's that age group of 18 to 24*".[278] He added that the availability of pornography is:

> "*creating a group of men who will look at pornography and the pornography gets harder and harder and harder, to the point where they are simply getting no sexual stimulation from it at all, so the next click is child abuse imagery. This is a real problem. It really worries me that children who should not be being able to access that material … are being led to believe this is what a normal relationship looks like and this is normal activity.*"[279]

102. The NCA gave the example of Tashan Gallagher, who in March 2019 was sentenced to 15 years' imprisonment for child sexual abuse offences, having:

> "*viewed images for probably two and a half years. By the time we captured that individual, he had progressed through a journey which had taken him through a series of forums who had told him his behaviour was normal, they had rationalised his behaviour,*

[274] Whether it is in the public interest to bring a prosecution is part of the test used by the Crown Prosecution Service in deciding whether an individual should face criminal charges.
[275] Robert Jones 20 May 2019 58/12-17
[276] CRI is a not-for-profit organisation that seeks to provide children with access to remedies including compensation for transnational crimes.
[277] Warren Binford 22 May 2019 169/6-14
[278] Simon Bailey 20 May 2019 120/9-12
[279] Simon Bailey 24 January 2018 148/16-24

> *he had become desensitised and he encountered the dark web. When he tried to get into the dark web ... They wouldn't let him into that forum unless he produced new, first-generation images.*"[280]

To gain access to the forum, Gallagher recorded himself raping a six-month-old baby girl and sexually assaulting a two-year-old boy.

103. Mr Jones explained that a number of perpetrators recently arrested by the NCA "*aren't people who would be seen as the stereotypical person that poses a threat to a child*".[281] These were people who had grown up in the internet age. They had initially viewed images online but had gone on to engage in contact child sexual abuse. Mr Jones said there was a "*very low barrier to entry for offenders who seek access to child abuse images*" and that these individuals had crossed it.[282]

104. The Inquiry's 'Learning about online harm' research considered that children's "*repeated exposure*" to being sent sexual images and/or requests for them "*could lead to desensitisation, which meant such incidents became accepted as an everyday part of life rather than something harmful to be acted on*".[283]

105. In 2016, the government proposed introducing legislation, the Digital Economy Act 2017 (DEA), that restricted access to pornographic websites to those aged 18 or over. In October 2019, the government announced that it would not be implementing the part of the DEA concerning age verification controls designed to ensure that those aged under 18 cannot access those sites. The government said that the reason for this decision was to ensure that "*our policy aims and our overall policy on protecting children from online harms are developed coherently*" and "*that this objective of coherence will be best achieved through our wider online harms proposals*".[284]

106. Chief Constable Bailey considered that the DEA was "*really an important element*"[285] in preventing children from becoming desensitised by viewing adult pornography and potentially seeking out indecent images of children. This echoes comments made by children who participated in the 'Learning about online sexual harm' research who identified exposure to pornography as being one of a number of examples of online sexual harm.[286] Legislation is required in order to ensure that children are protected from harmful sexualised content online, and this part of the DEA was an important measure designed to prevent children viewing adult sexual material. The value of this part of the legislation was, and remains, obvious – it may prevent some children being exposed to child sexual abuse material. Delaying or deferring action until the Online Harms legislation comes into force fails to recognise the urgency of the problem.

[280] Robert Jones 20 May 2019 21/6-16
[281] Robert Jones 20 May 2019 23/18-20
[282] Robert Jones 20 May 2019 17/21-24
[283] *Learning about online sexual harm* p5
[284] https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-10-16/HCWS13/
[285] Simon Bailey 20 May 2019 120/13-14
[286] *Learning about online sexual harm* p44

Part D

Online grooming

Online grooming

D.1: Introduction

1. Grooming is the process by which a perpetrator communicates with a child with the intention of sexually abusing or exploiting them. In the online world, it can be facilitated via text and online messaging services, emails, and online games that allow participants to message each other. There may be overlap between online grooming and other online-facilitated child sexual abuse. For example, child sexual abuse imagery may be shared with a child in an attempt to encourage him or her to perform a sexual act. There can also be an overlap between the platforms used by groomers. Initial contact can be made on public social media platforms. Once a rapport has been established, the perpetrator may suggest using the same platform's private messaging service or moving to an encrypted messaging service. Communication may remain online or the perpetrator may convince the child to meet in person.

2. Section 15 of the Sexual Offences Act 2003[287] criminalised those individuals who arranged to meet a child following sexual grooming. In April 2017, when section 15A was brought into force, it became a criminal offence to send a "*sexual communication*" to a child.

D.2: The scale of the problem

3. The scale of online grooming is of real and significant concern:

3.1. As discussed in Part B, the Inquiry's Rapid Evidence Assessment estimated that the proportion of adults holding sexualised conversations with a child is "*unlikely*" to be "*below the lowest estimate of 1 in 10 adults*".[288]

3.2. Freedom of Information requests made to the police by the National Society for the Prevention of Cruelty to Children (NSPCC) revealed that, in the first year that section 15A of the Sexual Offences Act 2003 was in force (April 2017 to April 2018), there were 3,171 recorded offences.[289] This amounts to more than eight offences each day. For the next six-month period (April 2018 to September 2018), there were more than 10 offences a day (with 1,944 offences recorded[290]). Mr Tony Stower, Head of Child Safety Online at the NSPCC, commented that the figures were "*far in excess*" of what the NSPCC expected to discover.[291]

3.3. The scale of online grooming was also clear in evidence given to the Inquiry by individual police forces. West Midlands Police specifically reported a growth in online grooming.[292] Online grooming was the fastest growing part of the work of Kent Police's specialist online child abuse unit.[293] Greater Manchester Police reported that,

[287] Sexual Offences Act 2003
[288] Rapid Evidence Assessment: *Quantifying the Extent of Online-facilitated Child Sexual Abuse* p14
[289] Tony Stower 22 May 2019 149/20-25
[290] Tony Stower 22 May 2019 150/1-3
[291] Tony Stower 22 May 2019 150/3-4
[292] OHY003315_015
[293] OHY003413_008

in 2015/16, the number of recorded cases of online grooming overtook the number of cases of 'offline' grooming.[294] There had been a 104 percent increase from 2014/15 to 2015/16 and the increase from 2015/16 to 2016/17 was expected to be around 47 percent.[295]

4. Over a three-month period in 2018, the National Crime Agency (NCA) received over 1,500 reports of grooming in respect of 12 internet platforms.[296] The NSPCC Freedom of Information requests revealed that – for the 2,097 offences where the police had recorded "*the method used to communicate*" – Facebook, Snapchat and Instagram were used in 70 percent of cases.[297] West Midlands Police[298] and Kent Police[299] both identified Facebook, Snapchat and Instagram as the three most common platforms used by offenders in child abuse (or domestic violence) reported to the force.

5. These statistics resonate with the Inquiry's research 'Learning about online sexual harm' where:

> "*Snapchat … Facebook, Instagram … were all repeatedly cited by participants across different elements of the research as spaces where sexual harassment or other forms of online sexual harm took place.*"[300]

6. Google, for example, acknowledged that online grooming was encountered on YouTube in particular.[301] Kik acknowledged that online grooming could occur in its public or private chat rooms.[302]

7. When asked about the scale of online grooming on its platforms, Ms Julie de Bailliencourt, Facebook's Senior Manager for the Global Operations Team, said that she "*can't comment on the specific numbers*"[303] provided by the NSPCC. Mr Hugh Milward, Senior Director for Corporate, Legal and External Affairs for Microsoft UK, acknowledged that grooming may take place on Microsoft platforms such as Xbox Live (an online gaming platform on which users can message one another) and Skype.[304] He said that Microsoft "*already know about instances where there has been grooming taking place on Xbox Live*",[305] but Microsoft did not keep data on how much grooming took place on Skype.[306]

D.3: Victims and survivors

IN-A1 and IN-A2

8. The Inquiry heard evidence from IN-A1 and IN-A2.[307] They are siblings, who were groomed online by Anthony O'Connor, a 57-year-old man who met IN-A1 on a music-sharing website, BearShare.

[294] OHY003286_019
[295] OHY003286_019-020
[296] NCA000363_008-009
[297] Tony Stower 22 May 2019 151/15-20
[298] OHY003315_011
[299] OHY003413_006
[300] *Learning about online sexual harm* p44
[301] Kristie Canegallo 16 May 2019 56/7-14
[302] KIK000009_003
[303] Julie de Bailliencourt 14 May 2019 87/9
[304] Hugh Milward 16 May 2019 10/7-13
[305] Hugh Milward 16 May 2019 14/1-4
[306] Hugh Milward 16 May 2019 10/10-12
[307] IN-A1 and IN-A2 13 May 2019 91/23-108/21

9. O'Connor duped IN-A1 into having contact with him by pretending, initially, to be a 22-year-old woman named 'Susan'. IN-A1 was 13 years old at the time. Initially, Susan seemed nice and was interested in IN-A1 and her hobbies. They would use Skype to message each other. IN-A1 introduced Susan to her 12-year-old brother, IN-A2. Susan's control over IN-A1 grew over time such that when Susan revealed he was a man, IN-A1 was not able to break contact with him.

10. One morning, O'Connor made IN-A2 sexually touch IN-A1 and even went so far as to suggest that IN-A2 should have sexual intercourse with her. After this incident, IN-A1 describes herself as becoming O'Connor's slave. O'Connor started to make IN-A1 commit sexual acts for him over webcam. He told IN-A1 that he had photographs of her and her family, but that he had deleted them. For a short period of time, she tried to stop contact but then he got in touch to say that, because she had ignored him, he had not really deleted the photographs. He sent her photographs of her and IN-A2 together and said that if she did not do as he asked, he would put the photographs on the internet. He even threatened to have her kidnapped (IN-A1 had told O'Connor her address, while he was masquerading as Susan). O'Connor kept saying that if IN-A1 did one more thing she would be free from him but the abuse continued. When sentencing O'Connor to 14 years' imprisonment, the judge referred to his behaviour towards IN-A1 as "*the grossest manipulation*".[308]

11. The impact of O'Connor's abuse can hardly be overstated. The children's mother (IN-H1) described the impact of the abuse:

> "*My daughter's terrified of everybody. She started self-harming, overdosing, starving herself, she wouldn't leave the house. She was aggressive, violent. She – she didn't want to be around me or talk to me. She couldn't handle – she couldn't handle anything. She overdosed about 20/30 times. She has scars all over her body from self-harming … they lost everything …* [My son] *is very vulnerable. He's always been very vulnerable. He's – he's very quiet. He – he just wants to forget it ever happened. He is – he just distances himself from everybody, he doesn't trust people. He clings to his dad a lot, because he knows he's protected …* "[309]

Ben

12. The Inquiry also heard about Ben (not his real name). In 2010, at the age of 13, Ben started to explore his homosexuality by using online forums.[310] This led him into contact with a number of adult males, many of whom went on to groom and sexually abuse Ben. All Ben's abusers knew that he was only 13 or 14 years old.[311]

13. Ms Tink Palmer, Chief Executive Officer of the Marie Collins Foundation, told us that the majority of his abusers were white men aged between 23 and 56 years old.

> "*The majority were middle-class with jobs. There was a teacher, two senior management positions, one man who owned his own business. So they were what I would call comfortably off people. And they were also from all parts of the country and would travel to him or try to get him to go to them.*"[312]

[308] https://www.examinerlive.co.uk/news/west-yorkshire-news/14-years-paedophile-anthony-oconnor-6311007
[309] IN-H1 14 May 2019 12/21-14/19
[310] MCF000008_004
[311] MCF000008_010
[312] Tink Palmer 22 January 2018 142/10-15

14. The offending came to light when, in 2010, Ben contacted ChildLine because a man was threatening to post naked photos of Ben on the internet. ChildLine referred the matter to the police.[313] Despite the involvement of the police and various agencies in early 2011, Ben continued to be abused and travelled to different parts of the UK to meet his abusers.

15. In early February 2011,[314] one of Ben's abusers was uncovered when Ben's parents overheard Ben making arrangements to go to Portsmouth to meet a 23-year-old male. Ben's mother found that Ben had electronically sent sexually explicit photos of himself to this unknown male. His parents reported this matter to the police, who passed the matter to their safeguarding unit. No immediate response was forthcoming. Ben's parents also reported the matter to their GP, who referred the matter to Bradford's Children's Social Care, and a meeting was arranged at Ben's school. At that meeting, police seized Ben's laptop and forcibly removed his phone from him.[315] However, no police investigation commenced and it was not until mid-February that Ben was formally video interviewed and asked for his account.

16. Ben reported to the police that he had been abused by over 30 adult males.[316] The volume of offenders who gained access to and the trust of Ben via the internet is shown below.[317]

Table 4 Offences against Ben that proceeded to court

Date of offence	*Offence*	*Status*
January 2011	*Grooming; sexual assault*	*Trial; not guilty verdict*
August/November 2010 Reported February 2011	*Grooming; penetrative assaults*	*Guilty plea; 36 months prison*
January 2011 Reported February 2011	*Grooming; penetrative assaults*	*Guilty plea; 32 months prison*
June 2011 Reported same day	*Abduction; grooming*	*Guilty plea; 16 months suspended 2 years*
January/June 2011 Reported June 2011	*Grooming; penetrative assaults*	*Guilty plea; 42 months prison*
January 2011 Reported March 2011	*Penetrative assaults*	*Guilty plea; 24 months prison*
January 2011 Reported February 2011	*Penetrative assaults*	*Trial; not guilty verdict*
January/June 2011 Reported March 2011	*Grooming; inciting a minor*	*Guilty plea; sentenced 20 months prison*
Autumn 2010 Reported March 2011	*Grooming; penetrative assaults*	*Guilty plea; 3 years prison*
September 2011 Reported September 2011	*Grooming; penetrative assault*	*Guilty plea; 24 months Young Offender Institution*

[313] MCF000007_10; In this Serious Case Review Overview Report, Ben is referred to as Jack, which is also not his real name.

[314] MCF000007_011

[315] Ben spoke of the horror of this incident in an interview, saying the "*police just pinning my arms behind me to get my phone out of my pocket when I'm already as distraught as can be*" (MCF000008_020).

[316] MCF000007_014

[317] MCF000004

Date of offence	*Offence*	*Status*
November 2011 *Reported November 2011*	*Grooming; penetrative assault*	*Guilty plea; 30 months prison*
October 2011 *Reported November 2011*	*Grooming; penetrative assault*	*Guilty plea; 37 months prison*
2011	*Inciting a minor*	*Guilty plea; 2 years supervision*
2011	*Inciting a minor x 1*	*Guilty plea; 3 years supervision*
2011	*Inciting a minor x 4*	*Guilty plea; 1 year community*
2011	*Inciting a minor x 2*	*Guilty plea; 3 years community*
2011	*Inciting a minor x 3*	*Guilty plea; 12 months prison*
2011	*Inciting a minor x 3*	*4 years Young Offenders Institution; 7 years supervision*
2011	*Grooming/CSE*	*Charged in Merseyside NFA in WY*
2011	*Grooming/CSE*	*27 months prison*
2011	*Inciting a minor*	*18 months prison*
Autumn 2010 *Reported February 2011*	*Inciting a minor x 13 Voyeurism x 1*	*3 years plus 8 months for voyeurism*
2011	*Inciting a minor x 3*	*9 months suspended for two years*

Source: MCF000004

17. In total, 23 offenders were taken to court. One case was not pursued. In all but two of the other cases, the offenders pleaded guilty to offences of sexually abusing Ben or inciting the sexual abuse of Ben. The sentences imposed by the courts ranged from supervision and community orders to sentences of immediate imprisonment.

18. A Serious Case Review, conducted by the Bradford Safeguarding Children Board[318] and published in June 2017, found that West Yorkshire Police and Bradford Children's Social Care failed in their statutory duty to protect Ben.[319] It concluded that the police's response to reports of Ben's contact with an offender in August 2010 was poor and that the initial police investigation was inept, badly managed and under resourced. As Ben told Ms Palmer in September 2016:

> *"I wasn't treated like a victim properly, there was one policeman who said that I was wasting police resources, and I knew what I was doing, almost blaming me, saying I'd be put into an offender's unit for a month. So definitely they need to adjust how they view boys in this situation."*[320]

The review also concluded that the use of technology exposed children to contact with child sexual abusers that no individual (for example, Ben's parents who attempted to restrict his access to the internet) or agency (such as the police who removed his devices) could prevent.[321]

[318] MCF000007
[319] MCF000007_052
[320] MCF000008_024
[321] MCF000007_039

19. As Ben's parents told the Serious Case Review:

> *"The enormity and horror of what our son suffered would be any parent's nightmare; the effect on our family was and is truly shocking … These should have been the happiest days of our son's life, but he was robbed of his childhood. We still cannot bear to think of what was done to his young and immature mind and equally to his young and immature body."*[322]

D.4: Preventing grooming

Industry

20. The Inquiry heard of various ways in which industry sought to prevent online grooming occurring.

21. Ms Kristie Canegallo, Vice President and Global Lead for Trust and Safety at Google, explained that YouTube now requires a user to accept an invitation to engage in a private conversation with another.[323] This gives users control over who they chat to and allows users to block approaches from someone they do not wish to be in contact with.

22. Mr Milward explained the parental controls available on Xbox. The set-up procedure specifically asks if the Xbox is going to be used by a child. If so, a main administrator can be designated giving them a level of control over the child's account. Microsoft ensures that the administrator is an adult "*by demanding various age verification which is required by law, and we ensure that it is in fact a parent by taking a small credit card payment*".[324] Where a child account is set up, various settings such as the live chat function are switched off by default and permission for access to such functions can only be granted by the adult administrator.[325]

Age verification

23. The Inquiry heard evidence that many social media and technology companies stipulate that, in respect of some of their platforms or services, users must be at least 13 years old. Facebook's terms and conditions state that children under 13 cannot use Facebook.[326] The same applies to Kik.[327] In order to have a YouTube account, the user needs to be at least 13 years old.[328] Skype has no age limit but its "*websites and software are not intended for or designed to attract users under the age of 13*".[329]

24. Mr John Carr OBE, who advises on matters of child internet safety, was asked how the age of 13 came to be the minimum age for subscription to online platforms and services. He explained that this requirement originated from evidence gathered in the US in the late 1990s in relation to marketing and advertising. The evidence suggested that 13 was the age at which a child could "*decide for themselves whether or not to be part of an environment*

[322] MCF000007_009
[323] Kristie Canegallo 16 May 2019 57/17-22
[324] Hugh Milward 16 May 2019 15/5-7
[325] Hugh Milward 16 May 2019 15/12-21
[326] FBK000005_003
[327] KIK000009_003
[328] Kristie Canegallo 16 May 2019 61/8-9
[329] INQ004284_001

where those kinds of advertisements, commercial advertisements, would be present".[330] Although this research was conducted before social media companies existed, the age limit has not changed.

25. In reality, the steps taken to ensure that users are at least 13 years old amount to no more than requiring the child to enter a date of birth which makes them at least 13. IN-A3 said that she opened a Facebook account when she was 12 because all her friends at school were on Facebook and that she could not now remember being told about the age limit.

> "*I can't remember if I lied about my age, but if I did lie about my age, think how simple that is, just to be able to put a different age, different year you was born and just being able to set up your account straight away.*"[331]

26. The NSPCC research for 2017/18 revealed that children aged 11 and under were victims of one-quarter of offences.[332] Mr Stower described it as:

> "*astonishing … And I find the fact that children under 11 are being targeted … quite systematically by offenders here is something I don't think the internet companies have yet got to grips with.*"[333]

27. The internet companies that gave evidence explained the ways in which they worked to detect underage users.

27.1. Ms de Bailliencourt said that, in her view, there was "*no easy solution to implement age verification*".[334] For example, she said, a requirement to present government ID cards or credit cards could exclude those who did not have them and would involve the processing of a substantial amount of information. She explained that Facebook's reporting tool includes the ability to report a possible underage user but said that Facebook did not keep data on the number of underage reports made in respect of the UK because:

> "*under COPPA,*[335] *Facebook is required to permanently wipe out any data potentially related to the account of a child under the age of 13 quite swiftly. So when we remove an account from the platform, we remove any associated data with this.*"[336]

Facebook had "*started to look into*" artificial intelligence to help detect underage users.[337]

27.2. When asked whether Facebook was able to assure the public that children would not be able to open accounts if they were underage, Ms de Bailliencourt said "*this is something that we all need to work on together*".[338] Similarly, when asked whether Facebook could guarantee that children would be safe from being groomed online, Ms de Bailliencourt said that this would be a "*very difficult promise to make*" but that Facebook would "*put the manpower and the technology that we have at our fingertips to make this as difficult as possible*".[339]

[330] John Carr 22 May 2019 121/10-12
[331] IN-A3 13 May 2019 87/14-18
[332] Tony Stower 22 May 2019 151/7-14; NSP000054_004
[333] Tony Stower 22 May 2019 151/10-14
[334] Julie de Bailliencourt 14 May 2019 121/7-8
[335] Children's Online Privacy Protection Act of 1998 (COPPA) is a federal law in the US.
[336] Julie de Bailliencourt 14 May 2019 30/25-31/4
[337] Julie de Bailliencourt 14 May 2019 121/18-23
[338] Julie de Bailliencourt 14 May 2019 122/4-5
[339] Julie de Bailliencourt 14 May 2019 122/11-123/4

27.3. In relation to YouTube, Ms Canegallo said that if there are reasons to suspect a user is under 13 years old, for example where the user reveals their age,[340] YouTube requires the user to submit additional verification or it will terminate the account. YouTube "*terminate thousands of accounts on a weekly basis for not passing that age verification process*".[341] When asked whether this signified that the process was inadequate in the first place, Ms Canegallo said that YouTube was "*constantly looking to improve*" its age verification process while "*looking to ensure that we are weighing those considerations of safety on the platform as well as privacy and data minimisation appropriately*".[342]

28. The NCA was clear, however, that not enough was being done by social media platforms to ensure that users were at least 13 years old. Mr Robert Jones, Director of Threat Leadership for the NCA, said it was "*absolutely pointless*" simply to rely on users declaring they were 13 years old if this was not then checked[343] because experience showed that this was "*no defence in terms of preventing underage use*". He said there were a "*viable set of measures which could be applied across the social media platforms as well*".[344] Mr Jones also said that the measures used to verify a child's age for the purposes of the Report Remove initiative,[345] which may require the involvement of a parent or carer, were another model that could be considered.[346]

29. Mr Christian Papaleontiou, Head of the Home Office's Tackling Exploitation and Abuse Unit, told us about a practical initiative taken by the social network, Yubo. Yubo partnered with Yoti (a digital identity provider) to use machine learning to detect whether website users are in the right age band for their platform.[347] He also described a recent 10-week study[348] by the Home Office and GCHQ to understand what more can be done to identify underage users. The study – which involved representatives from government, charities, academia, industry and law enforcement – found that at present no single "*technical approach*" could accurately identify child users while protecting privacy and ensuring a "*frictionless customer experience*".[349] However, "*early product tests*" conducted as part of the study revealed that a number of potential solutions "*show promise*".[350]

30. In closing submissions, a number of core participants called for industry to adopt age verification as well as identity verification. It was said – on behalf of IN-A1, IN-A2 and IN-A3 – that age verification on social media platforms was required now to protect children from grooming as it was "*not good enough to rely on self-certification*".[351]

31. The NCA agreed that both age and identity verification were "*vital in mitigating the online child abuse threat*", particularly for encrypted services and platforms as "*it is one of the few things that can be done to mitigate*" the difficulties that they posed to law enforcement.[352] As the NCA questioned:

[340] Kristie Canegallo 16 May 2019 61/18
[341] Kristie Canegallo 16 May 2019 61/22-23
[342] Kristie Canegallo 16 May 2019 66/7-23
[343] Robert Jones 20 May 2019 56/9-15
[344] Robert Jones 20 May 2019 57/6-7
[345] See Part C of this report.
[346] Robert Jones 20 May 2019 59/20 to 61/9
[347] Christian Papaleontiou 22 May 2019 70/6-24
[348] HOM003308
[349] HOM003308_013
[350] HOM003308_013
[351] Counsel for IN-A1, IN-A2 and IN-A3 24 May 2019 15/6-7
[352] Counsel for the NCA 24 May 2019 57/1-8

> "*Why, if you operate a service designed for children above a certain age, should you have any difficulty whatsoever in requiring children to establish their age when opening an account? … What is the legitimate and compelling reason for not doing so, that is sufficiently powerful to outweigh the child protection benefit?*"[353]

32. Based on the evidence we heard, the risk of being groomed online is particularly acute for children aged under 13 years old. It is plain that a more robust mechanism is required to verify the age of users than simply requiring them to declare their age on sign-up to a platform or service. The internet companies must also do more to identify users who are under 13 years old. As the Home Office and GCHQ study[354] reveals, there is much work still to be done before a practical technical solution to the problem can be achieved.

Education

33. Children who participated in the Inquiry's 'Learning about online sexual harm' research[355] told the researchers that education focussed too much on "*stereotypical 'stranger danger' images of perpetrators and abuse*".[356] In fact, where the secondary school aged children commented on the nature of online sexual harm they did so "*almost exclusively with reference to online approaches from unknown adults*".[357] In one of the focus groups conducted by the researchers, "*every participant said they had met up with at least one person who they had initially met online, without an adult present, and showed little concern about having done so*".[358]

34. The research found that children wanted to learn more about the potential to be sexually abused online from people they knew, including their friends and peers. One 15-year-old female interviewee said:

> "*Obviously they can tell you, 'Don't talk to strangers, don't let strangers talk to you', and stuff, but they should also talk about people that you know and trust, or you think you trust, because they might be more of, you might be more of a target to them because they think you trust them.*"[359]

35. The Department for Education's draft statutory guidance *Relationships Education, Relationships and Sex Education (RSE) and Health Education* (February 2019)[360] states that, by the end of secondary school, pupils should know, amongst other topics, "*the concepts of and laws relating to … grooming*".[361] This guidance will be compulsory in England from September 2020, with schools being encouraged to teach it from September 2019.

36. The guidance states that, before leaving primary school, children should know "*that people sometimes behave differently online, including by pretending to be someone they are not*"[362] but there is no specific reference to primary school aged children being taught about grooming. One 14-year-old who was interviewed as part of the 'Learning about online sexual harm' research recounted that by the time she was in year 6 (10 to 11 years old) she was "*already getting messages from random people and I didn't know what to do*".[363]

[353] Counsel for the NCA 24 May 2019 59/9-15
[354] HOM003308
[355] *Learning about online sexual harm*
[356] *Learning about online sexual harm* p7
[357] *Learning about online sexual harm* pp43–44
[358] *Learning about online sexual harm* p74
[359] *Learning about online sexual harm* p7
[360] HOM003273
[361] HOM003273_029
[362] HOM003273_022
[363] *Learning about online sexual harm* p57

37. The Department for Education will need to ensure that the guidance for primary school aged children sufficiently protects them from the dangers of being groomed online.

D.5: Detection

Law enforcement

38. The law enforcement response to online grooming initially lagged behind the response to the viewing and distribution of child sexual abuse imagery. In 2016, law enforcement acknowledged that:

> "*The police approach to targeting those who abuse children online has been disproportionately directed to those accessing indecent imagery. Comparatively little resource has been directed towards grooming which arguably represents a greater threat to children.*"[364]

39. Mr Keith Niven, Deputy Director Support to the NCA's Child Exploitation and Online Protection Centre, said that policing was "*very focused*"[365] on grooming and that law enforcement "*proactively deploys sensitive techniques*" to detect online grooming.[366] These techniques include officers operating in internet chatrooms and forums used by suspected offenders.[367] Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, explained that "*dedicated trained specialists*" were used "*to interact with offenders online*".[368]

40. In 2017, the Police Transformation Fund (PTF)[369] awarded £20.39 million over three years to enable regional organised crime units (ROCUs) to increase their undercover online (UCOL) capabilities.[370] Mr Papaleontiou described UCOL work as "*critically important in terms of bearing down on grooming*".[371] In September 2018, the Home Secretary announced a further £4.6 million to support UCOL work in the ROCUs.[372]

41. It is clear that the scale of the law enforcement response to online grooming has increased in a short period of time. However, as we consider in the next section of this report, the Inquiry also heard criticisms of the law enforcement response.

Online child abuse activist groups

42. Dark Justice is an online organisation which aims to uncover those who groom children over the internet. Its founders pose as children, on platforms such as Facebook and Snapchat, by setting up a decoy profile. The decoy profile makes clear that the person is a child. When the offender sexualises the communication and arranges to meet the 'child' in person, Dark Justice films the encounter. Dark Justice then contacts the police and provides the police with records of the offending.

[364] OHY003408_010
[365] Keith Niven 24 January 2018 38/18
[366] NCA000163_050
[367] NCA000230_008
[368] OHY003408_011
[369] The Police Transformation Fund was launched by the Home Office in May 2016. It is designed to allocate extra investment to reform policing.
[370] HOM003247_016
[371] Christian Papaleontiou 22 May 2019 20/4-6
[372] HOM003247_016

43. Dark Justice said that they were seeking to assist the police "*in an area where they do not have the expertise, understanding or resources to act properly or at all, to protect children from sexual abuse*".[373] Dark Justice gave an example where they were told (by a parent) that the police had been unable to trace an online groomer but that "[*w*]*ithin 15 minutes*" they were able to ascertain a name and address for the person and pass those details to the police.[374] They also said they had assisted in the arrests of 165 people of whom 96 were convicted.

44. Chief Constable Bailey told the Inquiry that the police did not support working with online child abuse activist groups "*for a significant number of reasons*".[375] His "*greatest fear*"[376] was that the operations of these groups were mounted without due regard to safeguarding risks to suspects and their families, including any children. He had concerns about whether the investigations had been conducted properly, about the quality of the evidence that these groups collected and he told us of instances where the suspects had been blackmailed or assaulted. Chief Constable Bailey gave an example where an online child abuse activist group had live-streamed their confrontation with a man accused of trying to meet a 14-year-old child.[377] The man denied the allegation, saying that he thought he was meeting a 48-year-old woman. The man was verbally abused by a neighbour who had seen the broadcast, and later that same day took his own life. The police reviewed the evidence provided by the online child activist group and found:

> "*no evidence to suggest that the male thought that he was meeting a 14 year old child … there was nothing to show that they had said that they were 14 years of age*".[378]

45. When asked whether (as suggested by Dark Justice) he envisaged there could be a framework or agreement so that police could use the resources of such groups while avoiding safeguarding risks, Chief Constable Bailey answered "*genuinely – I don't*".[379] He defended the law enforcement response to online grooming:

> "*over 400 people being arrested every month, month after month, after month … to say that we don't have the expertise, the skills, the capacity, quite frankly, I just think is misleading and it's not true*".[380]

Industry

46. In the *Serious and Organised Crime Strategy 2018*, the government expressed a clear and unqualified expectation of what technology companies must do about online grooming:

> "*companies must stop online grooming taking place on their platforms*".[381]

47. Companies use a variety of techniques to detect grooming.

[373] INQ004149_010
[374] INQ004149_010
[375] Simon Bailey 20 May 2019 125/1-3
[376] Simon Bailey 20 May 2019 126/14-15
[377] OHY008834
[378] OHY008834_001
[379] Simon Bailey 20 May 2019 127/7-14
[380] Simon Bailey 20 May 2019 127/17-20
[381] HOM003253_030

Moderators

48. Between February 2018 and May 2019, Facebook doubled its number of moderators (referred to by Facebook as 'content reviewers') from 7,500 to 15,000 reviewers worldwide.[382] The moderators review content and take action where there has been a breach of Facebook's 'Community Standards'. The Community Standards cover a wide range of content and include a policy on 'child nudity and sexual exploitation of children'.

49. When asked why the number of reviewers was increased, Ms de Bailliencourt said:

> "*I don't think there was anything specifically that triggered this particular investment, I think the company, as a whole, is incredibly dedicated to making sure that we have the right amount of people able to review content …* "[383]

She was not aware if there were plans to increase the numbers of moderators throughout 2019 into 2020.[384]

50. When asked how Facebook knew whether 15,000 moderators was enough, Ms de Bailliencourt said:

> "*When I speak to experts in this area, they often focus really on the number of people. We don't tend to look at it this way, we tend to think of the speed of our response and the adequacy of our response. We do this by using automation, machine learning, AI, as well as people … If we had reasons to believe that we were lagging behind or not good enough or taking too long to respond to a particular challenge, this is where I have seen investment in new teams, new technology, new expertise brought in on certain topics.*"[385]

51. Mr Milward did not provide the Inquiry with the number of moderators employed by Microsoft:[386]

> "*we would rather keep that information private. It is in the tens, not in the hundreds or in the thousands, and bear in mind that this is the team that reviews content to determine whether it is child sexual abuse material or not. This is not the limit to the resources that are placed on tackling this whole issue, which, again, is in the thousands.*"[387]

52. In December 2017, Google announced that by 2018 it aimed to have over 10,000 people working on content that might violate Google's policies.[388] Ms Canegallo could not state the number of reviewers prior to the increase. When asked what prompted this increase, she said:

> "*I think it was a – a natural reflection of the priority that we, at Google, place … in ensuring that users are having a safe experience and that we're being a responsible platform. So as online and off-line harms proliferate, it is natural that that responsibility necessitates Google to increase our investment in this area …* "[389]

[382] Julie de Bailliencourt 14 May 2019 53/19-55/12
[383] Julie de Bailliencourt 14 May 2019 55/19-23
[384] Julie de Bailliencourt 14 May 2019 56/3-6
[385] Julie de Bailliencourt 14 May 2019 56/12-22
[386] Hugh Milward 15 May 2019 80/25
[387] Hugh Milward 15 May 2019 84/19-25
[388] GOO000007_001
[389] Kristie Canegallo 16 May 2019 44/9-16

53. The increase in the number of people employed by Google and Facebook to review content, including child sexual abuse content, is significant but it is still unclear if the increase is enough. Industry needs to demonstrate a better understanding of the scale of the child sexual abuse imagery and grooming on their services and products. It is only once this data is known that the adequacy of resources (in terms of developing technology and employing sufficient numbers of human reviewers or moderators specifically focused on child sexual abuse and exploitation) can be assessed.

Technological methods of detection

54. Ms de Bailliencourt explained that, in 2012, Facebook realised that given the "*high probability*" that a child would not report being groomed, it needed to take a further step to "*identify this type of behaviour regardless of a user report*".[390] Since then, Facebook had been "*working hard*"[391] to improve its detection mechanism. The technology had developed from a "*quite rudimentary*" state in 2012, to what is now a "*behavioural classifier*" involving "*quite sophisticated pattern recognition*" rather than simply "*key word flagging detection*" to detect grooming.[392] The behavioural classifier looks at "*patterns of behaviour that may indicate that someone is trying to approach, or behaves in a predatorial way towards children on the platform*".[393] Where grooming is detected, the matter is reported to the National Center for Missing & Exploited Children (NCMEC) or, where necessary, directly to law enforcement.

55. Mr Milward said that Microsoft uses "*real time moderation technologies*" on XBox Live to detect grooming.[394] Conversations over XBox Live are public communications and are not encrypted. Microsoft will:

> "*dip in and out of a whole variety of these conversations to check on language being used … and then, equally, we will look for indications that there might be grooming taking place*".[395]

56. A "*level of automation*" was applied to detect indications that grooming may be occurring.[396] This might be combinations of words to indicate that somebody is trying to take a public conversation into a private forum: for example, 'are your parents around?' or 'do you have a number I can call you on?' Where potential grooming is detected, the "*intention*" is that the live chat stops, a warning message appears, the account of the potential groomer is suspended, and human moderators investigate.[397] Mr Milward acknowledged, however, that Microsoft:

> "*already know about instances where there has been grooming taking place on Xbox Live and has transferred to other platforms. So it's not perfect. Without a doubt, there's work to do on this.*"[398]

[390] Julie de Bailliencourt 14 May 2019 83/5-15
[391] Julie de Bailliencourt 14 May 2019 83/16
[392] Julie de Bailliencourt 14 May 2019 83/17-84-17
[393] Julie de Bailliencourt 14 May 2019 84/12-14
[394] Hugh Milward 16 May 2019 11/15-21
[395] Hugh Milward 16 May 2019 12/2-8
[396] Hugh Milward 16 May 2019 12/10
[397] Hugh Milward 16 May 2019 13/1-18
[398] Hugh Milward 16 May 2019 14/1-4

57. Google's "*comments classifier*" uses machine learning to detect potential grooming in comments on YouTube videos and brings them to the attention of a human moderator for review.[399] The classifier is an automated system that looks for "*potentially inappropriate comments*", captures them, removes them and if necessary reports them to NCMEC.

58. In November 2018, the Home Secretary convened a 'hackathon'. Hosted by Microsoft, engineers from leading technology companies including Microsoft, Facebook and Google worked for two days to analyse tens of thousands of conversations to understand patterns used by online groomers. This enabled engineers to develop a prototype that could potentially be used to flag conversations that might be indicative of grooming.

59. Mr Milward described the hackathon as a "*significant brainstorming resulting in an engineering solution*".[400] The prototype was improved following a second, mini-hackathon in May 2019, and it was put into live testing with three companies. At the May 2019 public hearing, Mr Milward said the testing was reporting "*very strong accuracy*"[401] and that it was a matter of "*months*" rather than years for the prototype to be finalised and deployed.[402] In January 2020, Microsoft announced the launch of this technology. Known as Project Artemis, the technology will be licensed free of charge to smaller and medium-sized technology companies worldwide.[403]

60. While acknowledging the useful work on the prototype, Mr Papaleontiou of the Home Office emphasised the need for follow-up. He said the Home Office:

> "*will be continuing to engage closely with industry and partners in terms of making sure that good intentions and a good prototype actually manifests itself in a product that delivers real world tangible benefits to those we are focused on protecting*".[404]

61. Mr Jones of the NCA emphasised the need for industry to implement the measures that it had developed:

> "*the real challenge for this type of event – you know, what's not to like about very clever people in Silicon Valley coming together and writing code to detect child abuse? Brilliant. What we need is the delivery and prevention of that offending and we are not seeing that at the pace that we should.*"[405]

He described frustrations that very positive measures taken by some smaller companies to tackle online grooming had not been adopted by bigger organisations. For example, Mr Jones told us about a company called Jagex which developed "*sophisticated*"[406] technology that can identify potentially inappropriate communication between users within its online gaming community. Where there is such communication, players receive a live pop-up advising them that a conversation is inappropriate. He said that "*over 87 percent*"[407] of the players who received the pop-up modified their behaviour. Mr Jones said he struggled to understand why bigger companies had not followed suit, despite efforts by the NCA to highlight and promote the innovation.[408]

[399] Kristie Canegallo 16 May 2019 57/17-58/3
[400] Hugh Milward 15 May 2019 91/18-20
[401] Hugh Milward 16 May 2019 21/3
[402] Hugh Milward 15 May 2019 93/23 to 94/4
[403] https://www.gov.uk/government/news/new-ai-technique-to-block-online-child-grooming-launched
[404] Christian Papaleontiou 22 May 2019 74/14-19
[405] Robert Jones 20 May 2019 32/16-21
[406] Robert Jones 20 May 2019 65/6
[407] Robert Jones 20 May 2019 65/24-66/1
[408] Robert Jones 20 May 2019 66/24-67/16

62. Ms Canegallo explained that online grooming is not always easy to detect. She said that "*grooming could begin with interaction that seems innocuous or comments that, without clear understanding of the intent … could not raise suspicion*".[409] It can happen both online and offline across many platforms "*in a way where it may not be clear the individual's age*".[410] When asked about media reports of grooming on YouTube, Google pointed (among other things) to having "*dramatically improved*" its comments classifier.[411]

63. In light of the NSPCC research revealing approximately two incidents of grooming a day on Facebook in the UK,[412] Ms de Bailliencourt was asked about the adequacy of Facebook's response to online grooming. Ms de Bailliencourt said that Facebook "*have invested and are and will continue to invest a huge amount*" in its response to online grooming and took its responsibility seriously.[413]

64. The results of the 2018 hackathon show how much can be achieved, in a short space of time, when government takes the lead and internet companies collaborate with one another.

65. Given the evidence of the scale of online grooming, industry's response will necessarily involve the increased development and use of technology. Companies will also need to ensure that there are sufficient numbers of human moderators to follow up on potential instances of online grooming identified by those technologies.

D.6: The interaction between law enforcement and industry

66. The law enforcement response to online grooming, and other forms of online-facilitated child sexual abuse, necessarily involves close and constant interaction with industry. Chief Constable Bailey, having consulted with a number of police forces, told us that "*relationships between policing and some Industry platforms is good*". One industry platform was said to demonstrate "*extremely good practice and support … by providing law enforcement with detailed information upon which to conduct a criminal investigation*". Another had a "*very active group of moderators*" of its chat rooms.[414] However, there were two particular issues on which there was a notable divergence of views between law enforcement and industry: encryption and access to data.

Encryption

67. Smartphones are not just telephones; they are also computers.[415] They enable communication between individuals but also store vast amounts of personal data, including work and social diaries, banking applications, photographs and videos of friends and family. In order to keep this information private, many of the technology companies use encryption. Encryption is the process of converting information or data into a code that makes it unreadable to unauthorised parties. Ms Melissa Polinsky, Director of the Global Security Investigations and Child Safety Team for Apple, said that Apple viewed encryption as "*fundamental to the protection of our customers*" from "*bad actors, by hackers, by various governments around the world for different purposes*".[416]

[409] Kristie Canegallo 16 May 2019 57/5-7
[410] Kristie Canegallo 16 May 2019 57/8-11
[411] Kristie Canegallo 16 May 2019 70/12-24
[412] As reported by BBC News: INQ004186
[413] Julie de Bailliencourt 14 May 2019 88/4-13
[414] OHY007220_002
[415] Simon Bailey 20 May 2019 120/4-5
[416] Melissa Polinsky 15 May 2019 38/14-39/19

68. The use of encryption is growing. The number of encrypted websites has increased substantially. According to Google, desktop users spend two-thirds of their time on such websites.[417] Facebook is considering applying encryption to Facebook Messenger.[418]

69. Communications made via many common platforms – such as WhatsApp, iMessage and Facetime – are subject to end-to-end encryption. This means that the content of the communication can only be seen by the sender and recipient and not by third parties – including the providers of the platforms themselves.[419] In practice this means that if, as part of a criminal investigation, law enforcement needs to access the messages between two people, then the company running the messaging service would not be able to provide police with that information. The only way for law enforcement to ascertain what was being said in the messages would be to obtain the data from one of the devices (eg the telephone handset or computer) used or from an (un-encrypted) online backup.

70. End-to-end encryption has significant implications for the law enforcement response to online grooming, the sharing of child abuse imagery and live streaming of abuse. The NCA acknowledged that encryption can be "*a force for good*" but said that if "*applied without thought to platforms that could be used by this type of offender, then, quite frankly, the lights could go out for law enforcement*".[420] Many of the techniques used to detect online offending do not work where the communication in question is encrypted. For example, PhotoDNA cannot scan the content of WhatsApp messages (which are encrypted) to detect child abuse imagery.[421] BT's Cleanfeed system, designed to prevent access to child abuse imagery, cannot operate over encrypted websites.[422] While Microsoft can monitor conversations over XBox Live (which are not encrypted) for potential grooming,[423] Apple cannot monitor conversations over iMessage (which are encrypted)[424] or live streaming via Facetime.[425]

71. Offenders are aware and take advantage of the protection afforded by encryption. Mr Stower for the NSPCC gave evidence that groomers will often move children between platforms to "*platforms which are smaller, that are more difficult for law enforcement to get into, particularly those that are encrypted*".[426] A large amount of child abuse imagery is stored in "*encrypted archives*" on the open web, beyond the reach of scanning techniques, with the means to access such archives (the encryption keys) stored on the dark net.[427]

72. The Home Office explained that the government's goal was to secure "*exceptional and targeted access to specific individuals' communications*".[428] Mr Papaleontiou said that "*Possible, platform-specific technical solutions exist, but these require working with individual service providers*".[429] Ms Polinsky said:

[417] Kevin Brown 17 May 2019 24/6-9
[418] Julie de Bailliencourt 14 May 2019 97/23-98/9
[419] HOM003247_030
[420] Robert Jones 20 May 2019 54/9-18
[421] Julie de Bailliencourt 14 May 2019 92/12-94/22
[422] Kevin Brown 17 May 2019 23/17-20
[423] Hugh Milward 16 May 2019 11/21-12/1
[424] Melissa Polinsky 15 May 2019 37/17-38/2
[425] Melissa Polinsky 15 May 2019 35/6-18
[426] Tony Stower 22 May 2019 158/10-14
[427] CRS000031_031-032
[428] HOM003247_030-031
[429] HOM003247_031

> "*as much as I would love to have an exception that would only be an exception for child protection … the truth of the matter is that any exception to encryption is an exception for anyone and is something that can be exploited by anyone*".[430]

73. On 4 October 2019, the Home Secretary and her counterparts in the US and Australia sent an open letter to Facebook asking it not to proceed with its plan to implement end-to-end encryption across all of its messaging services. The letter stated that the risks to public safety were:

> "*exacerbated in the context of a single platform that would combine inaccessible messaging services with open profiles, providing unique routes for prospective offenders to identify and groom our children*".[431]

74. When asked how the NCA envisage dealing with the consequences of end-to-end encryption, Mr Jones said that the technology companies should adopt a "*range of mitigations*"[432] and "*use hash lists, use machine learning, use AI*" on the un-encrypted areas to "*make sure there are no child sexual abuse images in there*".[433] For example, if an offender downloaded a known child sexual abuse image from a website and sought to send it to a third party via a WhatsApp message, whilst the WhatsApp message itself could not be pre-screened (because WhatsApp messages are encrypted), if pre-screening had been deployed on the website it would not have been available for download in the first place.

75. In closing submissions, a number of core participants challenged the growing use of end-to-end encryption and called for industry to fundamentally change its approach. The NCA said:

> "*It is simply not good enough, therefore, for a company which chooses to operate an encrypted service to shrug its shoulders and say there is nothing it can do. The making of that choice generates a responsibility to mitigate its harmful effects*".[434]

76. Submissions on behalf of IN-A1, IN-A2 and IN-A3 suggested that the technology companies' insistence on "*absolute privacy … is an excuse, a way in which platform providers, with a digital shrug, divest themselves of all responsibility*".[435] It was submitted that communications should be able to be accessed by the police.[436] In response to Apple's evidence that an exception to encryption could not be created just for child protection,[437] counsel for the NCA asked rhetorically "*how hard have you tried?*"[438]

77. Encryption represents a serious challenge to the detection of, and response to, online grooming and other forms of online-facilitated child sexual abuse. The public should be under no illusion: a consequence of encryption, and in particular end-to-end encryption of messages, is that it will make it harder for law enforcement to detect and investigate offending of this kind and is likely to result in child sexual abuse offences going undetected.

[430] Melissa Polinsky 15 May 2019 39/10-14
[431] https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg
[432] Robert Jones 20 May 2019 54/21-22
[433] Robert Jones 20 May 2019 55/13-16
[434] Counsel for the NCA 24 May 2019 58/12-16
[435] Counsel for IN-A1, IN-A2 and IN-A3 24 May 2019 18/12-15
[436] Counsel for IN-A1, IN-A2 and IN-A3 24 May 2019 17/19-22
[437] Melissa Polinksy 15 May 2019 39/10-19
[438] Counsel for the NCA 24 May 2019 56/17-25

Securing data

78. According to Chief Constable Bailey, the "*main challenge encountered by police nationally*" is obtaining data from industry to support investigations into online-facilitated child sexual abuse.[439] This is because data is typically stored by internet companies based overseas and there is an "*extremely lengthy*" and complex mutual legal assistance treaty (MLAT) process typically required to access content data. This leads to "*significant delays in gathering evidence to pursue offenders and protect children*".[440]

79. The NCA gave an example of an investigation which commenced in 2017. The suspect was alleged to have used Facebook, Instagram, Gmail and Snapchat to groom teenage boys into sending him indecent images and videos of themselves committing sexual acts.[441] Over 150 potential victims had been identified. The suspect was arrested in early 2018 but, as at March 2019, the NCA was still awaiting "*authorisation from a US judge to release content to further the investigation towards a potential prosecution*".[442]

80. As Mr Milward said, the MLAT process is "*not suitable for the digital age at all*".[443] As explained in Part B of this report, in October 2019 the Home Secretary signed a UK–US bilateral data access agreement allowing UK law enforcement to directly request communications service providers to produce communications data and content.[444] It is envisaged that the new agreement will mean that data can be accessed in weeks if not days.

81. Where law enforcement sought data (other than content data) or other types of assistance from industry, Chief Constable Bailey's evidence was that the response was mixed.[445] There was "*consensus*" that, where life was at risk, industry responded well and that, in such cases, support from social media applications was "*very good*".[446] Where there was no immediate risk to life – as in the vast majority of cases – there were examples of good practice; one industry platform responded within 48 hours but the response was "*generally slow*".[447] One platform was identified by two forces as having an "*extremely burdensome and lengthy law enforcement request process*".[448] Forces also noted that there were disparities between platforms as to how they dealt with law enforcement requests, the threshold for when assistance would be provided, and the quality and duration of data retained.

82. It is clear that improvements can and should be made to the speed and quality of the response by industry to law enforcement requests for data. Greater collaboration between law enforcement and industry ought to be capable of resolving the problem of inexpedient provision of information. It may be that the government will want to consider whether, if the regulator envisaged in the *Online Harms White Paper* is established, there should be a protocol setting out time limits for industry to respond to law enforcement requests.

[439] OHY007220_004
[440] OHY007220_004
[441] NCA000363_028-029
[442] NCA000363_028-029
[443] Hugh Milward 16 May 2019 24/15-19
[444] https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement
[445] OHY007220_001-003
[446] OHY007220_002
[447] OHY007220_003
[448] OHY007220_003

Part E

Live streaming

Live streaming

E.1: Introduction

1. Live streaming involves:

> *"live child abuse anywhere across the world, and in some of these sites and some of these facilities it enables them to direct individuals who are abusing children to abuse them in a way to which they gain some form of satisfaction. They can do this from the comfort and apparent safety of their own home, they can do it across the internet and, on occasions, there can be people that are gaining money out of this, because there can be a money aspect, or it could be between individuals, like-minded individuals, who are doing this to support each other."*[449]

2. The National Crime Agency (NCA) considers live streaming "*one of the emerging threats*".[450] The increased use of webcam and video-conferencing technology has led to an increased risk of child sexual abuse by live streaming. The instantaneous nature of the broadcast poses challenges for how law enforcement and industry detect such abuse.

3. The international nature of this offending is not uncommon. In 2015, the NCA investigated Mark Frost (also known as Andrew John Tracey), a UK national who raped and sexually assaulted a number of children in Thailand. His crime was uncovered when Dutch police arrested a Dutch national who was in possession of videos showing the Dutch national directing some of the abuse that Frost inflicted on his victims.[451] In another example, the NCA told us they had:

> "*very recently … prosecuted* [an individual] *using section 72 of the Sexual Offences Act. That individual incited abuse in the Philippines and in a range of other environments.*"[452]

4. The commercial live streaming of abuse for payment, particularly from countries in Southeast Asia, is familiar to the Inquiry. In the Children Outside the UK investigation,[453] the Inquiry heard about 'Lorna'. 'Lorna' lives in the Philippines and started doing online "*shows*" when she was seven years old. She was recruited by a neighbour to perform online sexual acts on a webcam for foreigners. She did shows three times a day and was paid six US dollars. She used the money to buy food. The Inquiry is also aware of a case where the perpetrator paid just 93 pence to watch a girl being sexually abused.[454]

5. According to Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, the UK is "*the third greatest consumer in the world of the live streaming of abuse*".[455] He told us that technology:

[449] Keith Niven 24 January 2018 34/13-23
[450] Keith Niven 24 January 2018 34/10
[451] NCA000163_054
[452] Rob Jones 20 May 2019 25/23-26/2; Section 72 of the Sexual Offences Act 2003 enables a UK national to be prosecuted in the UK for certain sexual offences committed outside of the UK.
[453] *Children Outside the United Kingdom Investigation Report*, Pen portraits
[454] https://www.dailymail.co.uk/news/article-7209173/Paedophile-faces-jail-paying-just-93p-live-stream-young-girl-abused.html
[455] Simon Bailey 20 May 2019 121/17-19

> *"now allows somebody to go on and use their credit card to pay for and instruct the live-time sexual abuse rape of a child in the Philippines … So you will sit in front of a monitor, having paid maybe as little as £10 or £15, no more than that … You will then direct how that child is then sexually abused."*[456]

6. Live streaming is also a problem facing children in England and Wales. We heard, for example, that during his abuse of IN-A1 and IN-A2, Anthony O'Connor was able to direct his victims into committing sexual acts, streaming it to him via Skype.

7. In 2018, the Internet Watch Foundation (IWF), assisted by funding from Microsoft, published research[457] examining the distribution of captures of live streamed child sexual abuse.[458] The IWF in fact said that it was "*uncommon*"[459] for the IWF to encounter images or videos captured by live streaming to feature Southeast Asian children. The IWF more frequently encountered images "*involving white girls, apparently from relatively affluent Western backgrounds*".[460]

8. Over a three-month period between August and October 2017, the IWF examined 2,082 images and videos. Its findings included that:

- 96 percent of the children depicted were on their own, typically in a home setting such as a bedroom or bathroom;[461]
- 96 percent of the imagery depicted one or more girls;[462] and
- 69 percent of the imagery depicted children assessed as aged 11 to 13 years old and 28 percent depicted children assessed as aged seven to 10 years old.[463]

9. Ms Susie Hargreaves OBE, Chief Executive of the IWF, told the Inquiry that in the first four months of 2019, there had been an increase in the amount of self-generated content:

> *"now at 36 percent of all the content we actioned … we took action on 15,264 URLs of self-generated content … 81 per cent of those were children aged 11 to 13 and predominantly girls … 90 per cent girls. So we are extremely worried about girls, young girls, 11 to 13, in their bedroom with a camera-enabled device and an internet connection."*[464]

10. The IWF's research drew on Ofcom's *Children and Parents: Media Use and Attitudes Report 2017*. Ofcom found that 53 percent of 12 to 15-year-olds who go online agreed with the statement 'I can easily delete information that I have posted about myself online if I don't want people to see it'.[465] However, the IWF's research found that 100 percent of the imagery included in the study had been taken from its original upload location and distributed via third-party websites.

[456] Simon Bailey 20 May 2019 122/5-13
[457] IWF000010
[458] Content that has been live streamed and then been photographed or videoed and made its way onto a child sexual abuse website.
[459] IWF000010_002
[460] IWF000010_002
[461] IWF000010_012
[462] IWF000010_012
[463] IWF000010_011
[464] Susie Hargreaves 17 May 2019 134/19-135/6
[465] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf p159

> *"this finding suggests there is still a lack of awareness amongst children of the risks of live interactions via webcam and the potential for permanent records to be created and distributed outside of their control"*.[466]

E.2: Challenges posed by live streaming

11. Live streaming offences pose unique legal and technical challenges for law enforcement and industry.

Issues

12. The speed and real-time nature of live streaming make it extremely difficult to proactively police interactions between the live streamer and the recipient. The practical effect of this is that it is harder for industry to deploy technology to detect, moderate or prevent live streamed child sexual abuse material. End-to-end encryption exacerbates this problem as it means the content of the communication cannot be accessed by industry or law enforcement.

13. On behalf of the NPCC, Chief Constable Bailey told us:

> *"the emergence of 4G and 5G and live streaming is going to present a greater risk … we know that there is a real problem in the area of the Philippines, and … I would have a real fear that with the emergence of 4G and 5G on the African continent, we are going to end up with a very similar situation"*.[467]

14. We also heard evidence that, on occasions, law enforcement has difficulty in obtaining information about the online accounts of individuals suspected of grooming and live streaming. Commander Richard Smith, the professional lead for child safeguarding for the Metropolitan Police Service, told us about the live streaming of two girls aged six and nine who were being groomed to commit sexual acts. A number of offenders were watching and contributing to the grooming. The Metropolitan Police Service asked the service provider to remove the streaming and requested information which would identify the offenders. Commander Smith said that although the content was removed and the offenders' accounts closed, the service provider:

> *"refused to provide any information regarding the offenders. While those offenders could no longer use their previous accounts to access the platform, there was nothing to stop them creating new accounts and to continue their previous offending. Without the police having access to data which might lead to the identification of offenders*, [the Metropolitan Police Service are] *unable to safeguard the children to whom offenders may have access."*[468]

Industry response: detection

15. When asked if Facebook knew the scale of live streaming on its platform, Ms Julie de Bailliencourt, Facebook's Senior Manager for the Global Operations Team, explained that Facebook:

[466] IWF000010_015
[467] Simon Bailey 20 May 2019 121/15-24
[468] Richard Smith 20 May 2019 163/14-164/4

> "*don't tend to look at prevalence of abuse across the content types but, rather, across the platform … whether it is a comment, a video or a photo, rather than specifically looking at live* [streaming]".[469]

She said that Facebook did not encounter "*child safety specific streaming … on the platform too often*".[470]

16. Ms de Bailliencourt explained that concerns about the content of a live stream can be reported via Facebook's reporting tools and that reports can be made as they are happening so that the reporter does not need to wait until the live broadcast is over. Facebook has a team of reviewers available 24 hours a day, seven days a week. She explained that, since late 2017, Facebook has been using machine learning to detect posts and live streams where someone might be expressing suicidal thoughts. When asked if such technology could be adapted to detect child sexual abuse, Ms de Bailliencourt said:

> "*this could offer really interesting opportunities on the child safety side. Although, again, as I have mentioned, because live streaming of child abuse is not a very common undertaking, thankfully, you know, this may provide limits to the learning that we may get from such reports.*"[471]

17. Microsoft does not record figures about the number of specific live streaming offences reported to the National Center for Missing & Exploited Children (NCMEC)[472] but said that live streaming most commonly took place on Skype. Mr Hugh Milward, Senior Director for Corporate, Legal and External Affairs for Microsoft UK, said that this, in part, was the motivation behind Microsoft's decision to fund the IWF research. He explained that based on the research:

> "*we quickly realised that, if you have one single live stream of abuse, that live stream is then captured and then shared on multiple times. And while it was – it is incredibly … difficult to stop that one instance of the live stream, that there must be a way … of developing technology that tries to address the way in which that live stream is then shared on multiple times.*"[473]

It was this finding that "*prompted us to focus more attention on to the development of PhotoDNA for video*".[474]

18. The collaboration between the IWF and Microsoft resulted in the development of PhotoDNA for Video. It is an example of the positive results that such cooperation can bring.

19. Google told us that, of all its products and services, YouTube was the platform most commonly used for the live streaming of child sexual abuse.[475] Users of YouTube can watch videos and upload their own videos to the platform. They can create a live stream via a webcam and other users can post comments or live chat as they watch the live stream. Google deploys its comments classifier to detect potentially inappropriate comments.[476] Those comments are then captured and removed and, if necessary, reported to NCMEC.

[469] Julie de Bailliencourt 14 May 2019 102/3-8
[470] Julie de Bailliencourt 14 May 2019 103/11-13
[471] Julie de Bailliencourt 14 May 2019 104/14-19
[472] MIC000026_010
[473] Hugh Milward 15 May 2019 98/15-24
[474] Hugh Milward 15 May 2019 99/4-5
[475] Kristie Canegallo 16 May 2019 56/15-18
[476] Kristie Canegallo 16 May 2019 62/11-17

20. In relation to detecting child sexual abuse within the live stream itself, Ms Kristie Canegallo, Vice President and Global Lead for Trust and Safety at Google, told us that Google has "*invested in technology that would allow us to monitor live streams and flag any potential inappropriate behaviour as well as flag whether minors are engaging in a live stream*".[477] In such cases, the live stream would be queued in a list pending review by a moderator.

> "*We have a dedicated team of human reviewers, that reply within minutes, to look at any live streams that are flagged and, to the extent that we saw CSAM there, we would terminate … that live stream … and then report it to NCMEC.*"[478]

21. The live streaming of child sexual abuse is one of the most harmful forms of abuse that is affecting children today. Although it may be difficult to detect, the internet companies must demonstrate that they understand fully the scale of this abuse and are deploying sufficient resources to detecting this type of online-facilitated harm.

E.3: Media reporting

22. Ms Canegallo was asked about an article in *The Times* in December 2018.[479] The article suggested that perpetrators were posting comments on the live chat section of a live stream which encouraged children to take off their clothes or pose in sexualised positions and that YouTube failed to remove live streamed videos that showed the sexual abuse of children. The article said:

> "*YouTube acknowledged that paedophiles had found a way to target children on the platform and 'it recognised there's still more to do'.*"[480]

23. Ms Canegallo told us that Google had investigated the matters raised in the article prior to its publication. As a result, 22 of the 37 videos (the videos had originally been live streams) were removed for violating Google's child safety policies. Google also analysed the comments and live chats associated with the 37 videos which resulted in 75 accounts being terminated and some referrals made to NCMEC.[481] Ms Canegallo said that Google had "*dramatically improved*"[482] its comments classifier and that "*the improvements in our comment classifier was not in response to this article*"[483] but had been work that was ongoing throughout 2018.

24. In light of this response, Ms Canegallo was asked about a second newspaper article that appeared in *The Guardian* on 21 February 2019.[484] The article raised concerns about the comments section on YouTube. As the article explained, the YouTube videos themselves did not contain child sexual abuse material and were in fact videos of young girls playing, exercising and doing gymnastics. However, comments posted alongside those videos included sexual comments about children and "*shared tips on when to pause the videos to take*

[477] Kristie Canegallo 16 May 2019 63/8-11
[478] Kristie Canegallo 16 May 2019 63/16-21
[479] INQ004188
[480] INQ004188_003
[481] Kristie Canegallo 16 May 2019 70/2-10
[482] Kristie Canegallo 16 May 2019 70/14-15
[483] Kristie Canegallo 16 May 2019 71/15-17
[484] INQ004184

compromising still images of the children".[485] The videos were accompanied by advertisements placed by companies such as Fortnite[486] and Disney, causing those companies to remove their adverts from YouTube.

25. The article also alleged that YouTube's 'Watch Next' feature recommended more videos of children with similar comments.

> *"After watching a few such videos on a new YouTube account … the site's algorithm – designed to provide users with content they might like, to keep them watching – would serve up endless videos of apparently underage children where the comments section contained inappropriate comments."*[487]

26. In the article, YouTube commented that the company had taken:

> "*immediate action by deleting accounts and channels, reporting illegal activity to authorities and disabling comments on tens of millions of videos that include minors. There's more to be done, and we continue to work to improve and catch abuse more quickly."*[488]

Ms Canegallo explained to us that Google turned off the comments section because "[*w*]*e saw that the comments classifier was not working as well as we wanted it to*".[489] She told us that Google is continuing to try and improve the comments classifier and is working on the 'Watch Next' algorithm to try and mitigate the risk of recommending inappropriate content.

27. Google reviewed the videos referenced in *The Guardian* article (including any comments). As a result, 360 accounts were terminated for violation of Google's policies including "*in large part*"[490] violations related to child sexual abuse material. Ms Canegallo said that she would have thought that the withdrawal of advertisements by the companies would have led to a loss of revenue to Google. When asked if she thought that the financial loss was the motivation behind Google's efforts to combat the problems highlighted by the article she said:

> "*the work that the YouTube team has been doing throughout 2018, some of which has come to fruition recently, is the result of continued effort on the part of the team that was not prompted by any one article or news inquiry*".[491]

28. In summer 2018, BT invested £100,000 to fund research into how machine learning techniques could help combat live streaming. Mr Kevin Brown, Managing Director of BT Security, told us that this investment arose following a meeting between BT's Chief Executive and the NCA, where the NCA explained the trends that were emerging in respect of live streaming. The NCA asked if, and how, BT could help from a technological perspective. Mr Brown explained that in a typical live stream of child sexual abuse and exploitation, the perpetrator:

[485] INQ004184_001
[486] Fortnite is a multi-player video game with a 12+ age rating. There is no age verification when signing up to the game.
[487] INQ004184_001
[488] INQ004184_002
[489] Kristie Canegallo 16 May 2019 83/16-20
[490] Kristie Canegallo 16 May 2019 84/22
[491] Kristie Canegallo 16 May 2019 84/7-11

> "*would join a video to the end destination where the abuse was actually taking place and, therefore, you focus in on the traffic behaviour, which … wouldn't be consistent with a normal conversation as if myself and you were over a Skype conversation … the characteristics would be significantly different*".[492]

29. Mr Brown said that this technology was still at the testing stage but was due to be discussed at a round table meeting with the Home Secretary focussed on the issue of live streaming.[493] That meeting took place on 21 May 2019. Mr Christian Papaleontiou, Head of the Home Office's Tackling Exploitation and Abuse Unit, gave an update on this meeting when he gave evidence at the public hearing the following day. He explained that the Home Office had established the Joint Security and Resilience Centre (JSaRC) to work "*with industry to respond to emerging security challenges*".[494] Through JSaRC, the Home Office had a £250,000 fund available and invited bids from technology companies that were looking "*to develop technical, technological solutions to tackle live streaming*".[495]

30. Five projects were successful in bidding for the fund.[496] They include:

- a project that takes existing techniques used in processing still imagery and applies those techniques to live streaming;
- technology that can analyse video streams and automatically link content depicting the same individuals or locations to assist in identifying victims and offenders;
- development of a tool that identifies, disrupts and prevents child sexual abuse and exploitation by analysing viewers' comments around the live streams; and
- using machine learning to analyse video streams and automatically detect child sexual abuse and exploitation content.

31. The Home Secretary announced a further £300,000 to help these projects develop. As Mr Papaleontiou said:

> "*this is government trying to take a lead and show leadership in terms of identifying solutions … we want to work with and pick up with industry in terms of how we can … deploy some of those companies' technical capabilities and technological capabilities to build on that and advance those projects or, indeed, other projects*".[497]

32. In terms of how law enforcement and industry work together, Mr Robert Jones, Director of Threat Leadership for the NCA, gave a number of examples where a collaborative approach was beneficial in tackling live streaming. In particular, he identified Yubo as being a company that took positive steps to make the platform safer for children. Yubo (formerly called Yellow) is a social media app created in France that allows users to create live videos. It reportedly has approximately 20 million users. Mr Jones told us that Yubo was initially criticised for having no age verification or privacy controls. As a result, the app provided perpetrators with the opportunity to masquerade as a child and thereby groom children and live stream the abuse.

[492] Kevin Brown 17 May 2019 29/23-30/6
[493] Kevin Brown 17 May 2019 30/15-16
[494] Christian Papaleontiou 22 May 2019 75/12-13
[495] Christian Papaleontiou 22 May 2019 75/22-23
[496] Christian Papaleontiou 22 May 2019 76/5-77/12
[497] Christian Papaleontiou 22 May 2019 77/25-78/8

33. One of the ways in which Yubo enhanced its child safety measures was to live moderate live streaming. Yubo used algorithms to help detect child nudity. Where detected a moderator will:

> *"drop into live streams … and tell underage users to effectively cease and desist, to put their clothes back on, to stop. If that doesn't happen, they will potentially lock that account."*[498]

34. Mr Jones said that Yubo's approach to moderation was shared by the NCA with other industry companies. He said:

> *"there is nothing in this which other industry providers don't know about. The issue is scale and, you know, that is something that can be solved with investment."*[499]

35. Mr Jones also told us about a live streaming platform that, following feedback from the NCA, changed its reporting systems to NCMEC to provide additional information that would assist in identifying the perpetrator's account or accounts.[500]

36. In the context of online-facilitated child sexual abuse, live streaming is a relatively new phenomenon and, as such, the law enforcement and industry response is not as well developed as it is in respect of grooming and the viewing of indecent images. It is important for companies to understand the scale of the problem on their platforms and ensure they have sufficient numbers of moderators to monitor and review suspected live streaming of child sexual abuse and exploitation. Although it is difficult to technologically detect and prevent the live streaming of child sexual abuse, the methods adopted by Yubo are a good example of what can be achieved by combining technology and human moderation.

[498] Robert Jones 20 May 2019 69/19-23

[499] Robert Jones 20 May 2019 70/21-24

[500] NCA000363_014-015

Part F

Future developments

Future developments

F.1: Background

1. In October 2017, the Department for Digital, Culture, Media & Sport (DCMS) published its *Internet Safety Strategy Green Paper*.[501] The Green Paper considered proposals to tackle a wide range of online harms including, for example, hate crime and cyber bullying, and set out three key principles:[502]

- what is unacceptable offline should be unacceptable online;
- all users should be empowered to manage online risks and stay safe; and
- technology companies have a responsibility to their users.

The Green Paper explained that the Home Office led the government's response to online child sexual exploitation and abuse, so the Internet Safety Strategy would only make "*appropriate links … where the Strategy offers additional solutions to these problems*".[503]

2. The government invited responses to the Green Paper and in May 2018 published its own response.[504] Its response set out plans for a social media code of practice and a requirement for companies to produce transparency reports providing data about the scale of harmful content on their platforms. The government also announced its intention to publish a joint DCMS and Home Office White Paper[505] which specifically included reference to both harmful and illegal online content.

3. In April 2019, the *Online Harms White Paper* was published.[506] Having set out its proposals (considered below), the government posed a number of consultation questions. The consultation period ran from 8 April 2019 to 1 July 2019 and thus spanned the second public hearing in this investigation. The initial consultation response was published in 2020.[507]

F.2: *Online Harms White Paper*

The proposals

4. The aim of the White Paper is to "*tackle content or activity that harms individual users, particularly children*".[508] It outlines plans to "*make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services*".[509]

[501] HOM003270; A Green Paper is a consultation document produced by the government which sets out proposals for consideration by people and organisations who work both in government and outside it.
[502] HOM003270_007
[503] HOM003270_008
[504] HOM003271
[505] A White Paper sets out the government's proposals for future legislation.
[506] INQ004232
[507] *Online Harms White Paper – initial consultation response*
[508] INQ004232_009
[509] INQ004232_010

5. In support of this, the government proposes a new regulatory framework for online safety on the open web[510] with a statutory (or legal) duty of care.

6. The proposed duty of care will require companies[511] "*to take reasonable steps to keep users safe, and prevent other persons coming to harm as a direct consequence of activity on their services*".[512] This will include the company preventing known child sexual abuse and exploitation content from being made available to users, taking action following a report of such content and supporting law enforcement investigations into criminal conduct.

7. Compliance with this duty of care will be overseen and enforced by an independent regulator.

8. In order to comply with the legal duty, the regulator will draft codes of practice. In relation to both child sexual abuse and exploitation and terrorism,[513] the government will have the power to direct the regulator in relation to the codes of practice and the codes must be approved by the Home Secretary. The regulator will not normally agree to companies adopting proposals which diverge from these codes.

9. In relation to child sexual abuse and exploitation, it is envisaged that the code of practice will include:[514]

- the reasonable steps companies should take proactively to prevent known and new indecent images of children (and links to such material) being made available and to identify and act in respect of grooming and live streaming;
- the reasonable steps companies should take to prevent searches linking to child sexual abuse and exploitation activity and content;
- the reasonable steps companies should take to ensure services are 'safer by design' and to implement effective measures to identify which users are children and adopt enhanced safety measures for child users;
- the reasonable steps companies should take to promptly inform law enforcement about a child sexual abuse and exploitation offence, including provision of sufficient information to enable victims and perpetrators to be identified;
- the steps companies should take to ensure they continually review their efforts to tackle child sexual abuse and exploitation and remain 'up to date' with the scale and nature of the threat and adapt their procedures and technology in accordance with that threat; and
- steps to ensure that users who are affected by child sexual abuse and exploitation are directed to and able to access support.

[510] INQ004232_035; The government's response to tackling harm on the dark web is set out in the *Serious and Organised Crime Strategy*.
[511] INQ004232_008
[512] INQ004232_045
[513] In relation to child sexual abuse and exploitation and terrorism, the White Paper prioritises action in respect of both of these online harms. For the purposes of this Part of the report, the Inquiry will only refer to child sexual abuse and exploitation.
[514] INQ004232_068-069

10. The White Paper stated that the government would publish interim codes of practice on child sexual abuse and exploitation by the end of 2019. This did not happen. In January 2020, the Home Office informed the Inquiry that the interim codes will be published "*later this year*".[515]

11. The regulator will have enforcement powers. The potential powers include issuing an enforcement notice (requiring the company to respond to a breach of the code and provide an action plan to resolve the problem), civil fines, and publishing public notices where a company fails to comply with the regulations or the regulator.

12. The White Paper also asked consultees for their views on whether the enforcement powers should include the ability to block the companies' platforms from being accessible in the UK and whether senior managers should be personally liable for a major breach of the statutory duty. As Mr Christian Papaleontiou (Head of the Home Office's Tackling Exploitation and Abuse Unit) said, the power to block access to services or platforms is "*very controversial*".[516] He said this would only be considered as a final step in the enforcement regime but "*if there is to be a regulator, the regulator needs to have teeth. These are potentially big companies that it's working with.*"[517]

Responses

13. The National Crime Agency (NCA) considered that the White Paper was right to tackle "*The piece in the middle, which is industry and the platform where all of the offending has taken place*".[518] The NCA wanted to see "*a regime where it actually matters to industry*".[519]

14. Facebook said that they "*welcome*"[520] both input from the government in relation to online harm and the proposal for there to be codes of practice and a regulator. The Internet Watch Foundation (IWF) adopted a similar stance, adding:

> "*We very much hope that the legislation will be flexible enough to allow growth within the internet and the changes within the internet, but also allow for different companies of different sizes to be able to engage with and take advantage of the technologies around.*"[521]

15. Apple said "*we are generally in favour of additional regulation, but I think it depends on what that looks like, and the devil really is in the details*".[522] Microsoft considered that a regulatory framework was important to help "*re-establish trust between the general public and technology … to give them the reassurance that they're not just relying on technology companies to do what they say they're going to do*".[523]

[515] HOM003317
[516] Christian Papaleontiou 22 May 2019 61/17-18
[517] Christian Papaleontiou 22 May 2019 64/2-5
[518] Robert Jones 20 May 2019 83/21-23
[519] Robert Jones 20 May 2019 84/5-6
[520] Julie de Bailliencourt 14 May 2019 111/18 and 25
[521] Susie Hargreaves 17 May 2019 138/8-13
[522] Melissa Polinksy 15 May 2019 69/8-11
[523] Hugh Milward 16 May 2019 31/9-12

16. Google was still in the process of considering the White Paper and said it would be responding to the consultation.[524] BT was also in the process of formulating its response and considered the issue was "*one of making sure … that there are clear legal frameworks that will enable us to enact perhaps further blocking or further content examination*".[525]

17. Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, told us that the NPCC was still drafting its response. His personal view was that any legislation needed to be "*extra-territorial*"[526] given that so many of the technology companies were based outside the UK. He supported the need for sanctions to include the ability for internet service providers to block service for non-compliant companies and thought "*a liability for executives is absolutely right*".[527] He added:

> "*the White Paper will only deliver something meaningful if the powers are given to a regulator, whereby the companies recognise that actually they have now got to do something over and above what they are currently doing*".[528]

18. The Inquiry also heard from Mr John Carr OBE, who has been working in and advising on online safety for over 20 years and is a former board member of the IWF.[529] He considers that the time has come for an end to self-regulation because, as he put it:

> "*everything seemed to take forever … unless there was a catastrophe, and then suddenly everything could happen very quickly, and there was no visible means of ever confirming that what the industry said they were doing they were actually doing*".[530]

19. The children spoken to as part of the 'Learning about online sexual harm' research "*identified a clear role for the online industry to play in protecting children and young people from online sexual harm*".[531] As one 15-year-old interviewee put it:

> "*I think they* [online companies] *have a major responsibility, and they don't do it, they don't think about it at all. On Instagram, I've seen no posts about safety.*"[532]

20. When the participants were asked about the steps that companies could take, five common actions were suggested:

- embedded warnings and advice for users to read when signing up to an online platform;
- improved enforcement of age restrictions;
- improved privacy settings including the use of default privacy settings when setting up an account;
- more obvious and accessible reporting options and stronger action when reports are made; and

[524] Kristie Canegallo 16 May 2019 130/5-10
[525] Kevin Brown 17 May 2019 42/3-6
[526] Simon Bailey 20 May 2019 147/5
[527] Simon Bailey 20 May 2019 147/8
[528] Simon Bailey 20 May 2019 148/6-10
[529] Mr Carr is also the secretary of the Children's Charities' Coalition on Internet Safety (CHIS), a UK-based charity focussed on child safety policy, and a member of the executive board of the UK Council for Internet Safety (UKCIS, formerly the UK Council for Child Internet Safety, UKCCIS), which is a forum that enables government, technology companies and the third sector to promote a safer online experience.
[530] John Carr 22 May 2019 100/20-25
[531] *Learning about online sexual harm* p10
[532] *Learning about online sexual harm* p81

- enhanced moderation of online activity by apps and platforms.[533]

21. Industry, government and law enforcement should take note of these five key actions. Steps to give effect to them within the current institutional response and as part of the proposed online harms regulatory framework should be taken as soon as possible.

F.3: Transparency reports

The content of transparency reports

22. The White Paper also proposes that the regulator will have the power to require companies to provide annual transparency reports "*outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address these*".[534] It envisages that the transparency reports will include details about the procedures the company has in place for reporting illegal (and harmful) content, including the number of reports received and how many of those reports led to action being taken. The reports will also include information about what proactive steps or tools the company uses to prevent and detect illegal content and detail about its cooperation with UK law enforcement.

23. The publication of transparency reports is not a concept that is new to the internet industry. Google has been publishing such reports since 2010 and Facebook, Apple and Microsoft since 2013.

24. There is, however, no consistency in the content of the reports. For example, Apple's reports focus upon the number of government requests it receives for information about emergency cases (where there is a risk of death or serious injury), accounts or devices, or 'financial identifiers' (to assist in cases of suspected fraud). Microsoft's reports look at the number of law enforcement requests and whether the request is for content or non-content data from a Microsoft account. Google's and Facebook's reports include some details about the amount of content that is removed from their services and the reasons for that removal.

25. Facebook was asked about its transparency report in respect of 'Child Nudity and Sexual Exploitation of Children', published in November 2018.[535]

> **25.1.** In response to a question in the transparency report 'How prevalent were child nudity and sexual exploitation violations on Facebook?', Facebook replied "*we can't reliably estimate it*".[536] The report says Facebook took action on 8.7 million pieces of content (in the quarter July to September 2018) and that 99.2 percent of this content was flagged and removed before users reported it to the company. What is not set out though is any real context to these figures. For example, these figures include both illegal images of child sexual abuse and lawful images of child nudity – it is therefore not possible to ascertain how much illegal content was found on Facebook. Second, while the removal of millions of pieces of content is significant, the report does not state how much general content was uploaded to Facebook in this period. It is difficult to assess therefore whether these figures represent a 'success story' or are being used to mask an underlying problem in the way Facebook tackles child sexual abuse material.

[533] *Learning about online sexual harm* pp81–82
[534] INQ004232_010
[535] INQ004287_001
[536] INQ004287_001

25.2. We were told that Facebook could not express "*the prevalence related to child sexual exploitation in a way that is accurate yet*".[537] Ms Julie de Bailliencourt, Facebook's Senior Manager for the Global Operations Team, explained that Facebook was working with the Data Transparency Advisory Group (based at Yale University) to ensure that Facebook was approaching its data collection in the "*right way*".[538] She said that "*Adult nudity is more prevalent on the platform than child sexual exploitation*".[539] When asked how Facebook could make such an assertion if the amount of child sexual abuse and exploitation content was not known, she said:

> "*the amount of time our team may encounter child sexual exploitation versus other types of violating content is minimal*".[540]

26. Google's transparency report for April to June 2018[541] records that YouTube removed nearly 7.8 million videos for breach of its Community Guidelines in the quarter. Of those, 88 percent were identified as a result of automated flagging. In the same quarter, YouTube removed over 9.6 million videos that had been reported by human flaggers (including trusted flaggers[542]). The report states that where a human flagger reports a video, the human flagger can select a reason for their report and that 27.4 percent of reviewers selected 'sexual' as the reason.

27. It would be wrong to assume that 27.4 percent of content removed from YouTube related to sexual offending. The data only records the reason the reporter gave for flagging the video and does not inform the reader if the video did in fact breach the Community Guidelines and, if so, whether the content was illegal and/or related to child sexual abuse and exploitation. Ms Kristie Canegallo, Vice President and Global Lead for Trust and Safety at Google, explained that Google "*continually update the transparency report to provide more information*"[543] and that "*there would be more information around child safety in subsequent reports*".[544]

28. In relation to the transparency reports, Mr Carr was of the view that Google and Facebook "*tell us what they think they want to be transparent about*".[545] He said:

> "*And they're very reluctant to disclose, as you can imagine, exactly what scale of illegal activity is taking place on their platform, but I think we have a right to know*".[546]

29. Mr Tony Stower, Head of Child Safety Online at the National Society for the Prevention of Cruelty to Children (NSPCC), was equally critical of the reports.

> "*The crucial point is, here, that they are deciding what to be transparent about … and that makes it completely impossible for any parent, or indeed any child, to compare the services and make an informed choice.*"[547]

[537] Julie de Bailliencourt 14 May 2019 70/24-25
[538] Julie de Bailliencourt 14 May 2019 71/7
[539] Julie de Bailliencourt 14 May 2019 70/22-23
[540] Julie de Bailliencourt 14 May 2019 72/5-8
[541] GOO000024
[542] Trusted flaggers are individuals, governmental agencies and non-governmental organisations that are particularly effective at notifying YouTube of content that violates its Community Guidelines.
[543] Kristie Canegallo 16 May 2019 101/7-8
[544] Kristie Canegallo 16 May 2019 101/14-15
[545] John Carr 22 May 2019 111/6-7
[546] John Carr 22 May 2019 111/18-21
[547] Tony Stower 22 May 2019 153/20-24

30. Transparency reports are important to the public's ability to scrutinise industry's efforts to combat online-facilitated child sexual abuse. The Inquiry heard repeatedly from industry witnesses that their respective companies were doing all they could to detect and prevent their platforms from being used to facilitate child sexual abuse. It is difficult at present to assess the accuracy or otherwise of those assertions. There needs to be consistency in respect of the information a company provides about the amount of child sexual abuse content on their platforms or services. This could include, for example, data about the number of reports made to the National Center for Missing & Exploited Children (NCMEC), how many accounts were closed for child sexual abuse and exploitation violations, how many requests the company receives from law enforcement for detail in respect of child sexual abuse and exploitation investigations, and how much illegal content was found as a result of proactive detection technology and/or because of human reporting.

'Naming and shaming'

31. One of the proposals of the White Paper is to publish public notices setting out where a company fails to comply with the regulations/regulator. Mr Carr said that in his experience "*the threat of naming and shaming is one of the few weapons that seems to work reliably with internet companies*".[548]

32. Earlier parts of this report have considered the ways in which the industry responded in 2018/19 to reports in the media of child sexual abuse content being found on their platforms. Invariably, once alerted to the problem, the companies were quick to take action.

33. Mr Robert Jones, Director of Threat Leadership for the NCA, was asked why the NCA does not routinely 'name and shame' those companies that law enforcement considers are failing to respond to the growing online threat. Mr Jones said that when dealing with the companies individually there was "*good and regular dialogue*"[549] and that, generally speaking, when the NCA made a request for intelligence or evidence, that information was provided. He considered that the companies' responses were reactive but that the "*proactivity of going on the front foot to … meet this threat, isn't what we would like it to be*".[550]

34. Mr Jones explained that the NCA did hold joint forums with industry but that it was "*very, very difficult to get the level of openness and transparency amongst all of the companies at the same time*".[551] He thought that it would be "*unfair*" to name and shame a company without providing "*operational context*".[552] From the NCA's perspective:

> "*the challenge for us is that calling out one company doesn't help, because the internet is a global phenomenon and we need everybody to get behind the objective of reducing access to these images*".[553]

35. Chief Constable Bailey was asked about a May 2019 press release[554] in which he advocated a public boycott of social media. He told us that whilst he was "*proud*" of the work done by law enforcement to protect children, he did not consider that efforts to raise the public profile in respect of online child sexual abuse had received "*the public impact in*

[548] John Carr 22 May 2019 134/1-3
[549] Robert Jones 20 May 2019 27/16
[550] Robert Jones 20 May 2019 29/3-5
[551] Robert Jones 20 May 2019 27/19-21
[552] Robert Jones 20 May 2019 29/17-18
[553] Robert Jones 20 May 2019 29/5-9
[554] INQ004303

terms of outrage at what has actually taken place".[555] He said that the power of the regulator to impose fines would be an appropriate and effective sanction for some companies but that "*for some of these companies, who are worth billions, then actually a fine is a drop in the ocean*".[556] It was for this reason that he advocated a boycott because, as he said in the press release:

> "*Ultimately … the only thing they will genuinely respond to is when their brand is damaged.*"[557]

36. In the event of a failure to comply with the regulations or the regulator, the power to name and shame is an important tool for the regulator.

F.4: Compensation

37. IN-A1 and IN-A2's mother (IN-H1) told us that the Criminal Injuries Compensation Authority (CICA) refused both her children's claims for compensation. IN-H1 said that the reason given for the refusal was that online grooming and child sexual abuse and exploitation was not 'a crime of violence' because the offences did not take place in physical proximity.[558]

38. The CICA has responsibility for making awards of compensation to those who have been injured by 'a crime of violence'. There is no legal definition of the term 'a crime of violence' but Annex B to the CICA Scheme lists what is and what is not 'a crime of violence' for the purposes of the scheme.[559]

39. In September 2018, the Ministry of Justice announced a review of the CICA Scheme which includes consideration of whether the definition of 'a crime of violence' should be broadened to include sexually exploitative crimes such as grooming. As Mr Papaleontiou told us, the review would be considering:

> "*how the scheme does or doesn't appropriately capture injury, in its widest sense … and, again, looking at … the definitions around harm … in terms of what we now understand more richly in terms of the impact of child sexual abuse and exploitation*".[560]

40. The government needs to ensure that the CICA Scheme is fit for the internet age and takes account of the fact that online-facilitated abuse is often a feature of sexual offending against children.

41. In IN-H1's opinion, the internet companies should pay compensation to victims of online-facilitated child sexual abuse:

> "*it's their responsibility to look after it, it should be their responsibility to pay compensation for anything that goes wrong, and not only that, it should be their responsibility to get my kids the help and support they need to get through this because, if they created the problem, they should fix it*".[561]

[555] Simon Bailey 20 May 2019 150/20 and 151/1-2
[556] Simon Bailey 20 May 2019 153/18-20
[557] Simon Bailey 20 May 2019 152/2-3; INQ004303
[558] INQ003770_005
[559] Criminal Injuries Compensation Scheme 2012 (amended)
[560] Christian Papaleontiou 22 May 2019 67/13-21
[561] IN-H1 14 May 2019 17/8-14

42. Mr Papaleontiou was asked whether the government had considered whether monies raised by any fines imposed by the regulator should be used in whole or in part to compensate victims of online harm. He said that the government had not yet gone as far as considering how the money from fines should be allocated but that those discussions "*will rightly need to take place*".[562]

F.5: Education

43. A number of witnesses highlighted the importance of education in the fight against online-facilitated child sexual abuse. As one witness said:

> "*We have to educate, empower and protect our children, and those who are working with them, with the right information.*"[563]

Children

44. The Inquiry heard a range of evidence about how children are taught about online safety.

44.1. Sixty-seven percent of children aged 12 and under and 46 percent of 13 to 18-year-olds would welcome more education in schools about online safety.[564]

44.2. The 'Learning about online sexual harm' research[565] asked participants if they thought the age at which they first received school-based education about online sexual harm was appropriate:

- 95 percent of those who first received school-based online sexual harm education in primary school (years 4 to 6) thought this was the right age;[566]
- 67 percent of those who first received such education in years 7 to 9 (secondary school) thought it was the right age; 29 percent thought it was too late.[567] One 16-year-old girl said:

  > "*Younger students are using social media and are online from a younger age than secondary school, so they need to be informed on this serious matter.*"[568]

- 80 percent of those who first received it in year 10 or later said this had been too late.[569]

44.3. IN-A3 told us:

> "*I really do believe you can't just give them one – one lesson, like we did really about online safety … have more lessons, maybe once a month, about it. Give them scenarios … show them real-life things that can happen online. It's not just a simple thing of someone just popping up to you who's an old man, it's not like that … so many people can lie about who they are, that there needs to be education for that.*"[570]

[562] Christian Papaleontiou 22 May 2019 65/25-66/1
[563] Jim Gamble 23 January 2018 32/23-25
[564] INQ004232_090
[565] *Learning about online sexual harm*
[566] *Learning about online sexual harm* p57
[567] *Learning about online sexual harm* p57
[568] *Learning about online sexual harm* p59
[569] *Learning about online sexual harm* p57
[570] IN-A3 13 May 2019 87/24-88/8

Similar comments were made by the children in the 'Learning about online sexual harm' research which found "*there was a strong consensus among participants that such education needed to be provided on an ongoing, rather than one-off, basis*".[571]

44.4. In October 2017, Google conducted a survey of just over 200 teachers who had taught for an average of 10 years to learn about the teachers' perspectives. Teachers thought that online safety (not limited to online sexual harm) should be taught from the age of seven and "*82 per cent of the teachers did not think they had all of the resources they needed*" to teach online safety to their students.[572]

45. There are a number of initiatives and training programmes designed to try and raise children's awareness of the dangers of being sexually exploited online. In addition to the NCA's 'Thinkuknow' programme, a number of local police forces also provide similar projects. For example, West Midlands Police worked with local councils on the 'See Me, Hear Me' campaign designed to raise awareness of child sexual exploitation.[573] Kent Police and Norfolk Constabulary deliver online safety presentations to secondary schools.

46. A number of internet companies have also established educational programmes and have dedicated web pages which the public can access to learn about staying safe online. For example, Facebook has a 'Safety Centre' on its website. In the UK, Google runs two educational programmes – 'Be Internet Legends' developed for seven to 11-year-olds and 'Be Internet Citizens' aimed at 13 to 15-year-olds. Google also established the 'Google for Education Teacher Center'.[574]

47. For a number of years now, the UK Safer Internet Centre has run the 'Safer Internet Day' in schools. The Safer Internet Day is a global event held in February each year designed to help teachers, children, parents, law enforcement, social workers and internet companies promote safer use of digital technology.

48. The Department for Education not only plays the lead role in prescribing what children are taught in schools but it is also the government department with responsibility for safeguarding children and child protection. From September 2020 in England it will be compulsory for primary schools to teach 'Relationships Education' and for secondary schools to teach 'Relationships and Sex Education'. Schools are encouraged to start teaching these topics from 2019 and the government has announced a budget of £6 million to help schools receive support and training in preparation for the introduction of these subjects in 2020.[575]

49. At primary school level this includes teaching children that sometimes people behave differently online, including by pretending to be someone they are not, and of the significance of keeping personal information private. The importance of these topics cannot be overstated. During the course of her messages with 'Susan' (ie Anthony O'Connor), IN-A1 told 'Susan' her address. In due course, 'Susan' set up an account which referenced IN-A1's address. Later, towards the end of the abuse, IN-A1 received a letter including a photograph of herself which described all the sexual things 'Susan' was going to do to her. IN-A1 told us that what happened to her caused her mental health to deteriorate such that she even attempted suicide.[576]

[571] *Learning about online sexual harm* p60
[572] GOO000008_001
[573] OHY003315_043
[574] GOO000001_025-026
[575] Christian Papaleontiou 22 May 2019 79/20-24
[576] IN-A1 13 May 2019 101/16-19

50. By the time children leave secondary school, the draft statutory guidance states that they should know, for example, about the risks of material being shared online, the impact of viewing harmful content and that the sharing and viewing of indecent images of children is a criminal offence. The difficulty in stemming the tide of self-generated indecent imagery is encapsulated by this comment made by a 14 to 16-year-old child who participated in the 'Learning about online sexual harm' research:

> "*I think educating about things like nudes and stuff is hard because yeah, people are taught that it's illegal and everyone understands that but it doesn't stop people being, like wanting to explore. And like, yeah, it is illegal and everyone knows that but* [you] *still do it because you may be attracted to that person or you're just generally just intrigued.*"[577]

51. The participants in this research were asked for their views about the way in which staying safe online was/should be taught. Many felt that there was a disproportionate emphasis on the negative aspects of spending time online.

> "*If you* [teachers] *sort of just come with the approach – this is bad – then you just think – 'you don't understand so why should I listen?' (16-year-old female)*"[578]

52. Nearly two-thirds of students thought that online education should be taught, not by a teacher, but by someone from an external organisation as they would have specialist knowledge.

> "*Because it is coming from someone who knows what they are talking about. (14-year-old male)*"[579]

Particular mention was made of the potential benefits of hearing directly from young people who had experienced online sexual harm.

> "*By talking to people who have had those experiences it makes it a lot more real. (16-year-old female)*"[580]

53. Participants indicated a strong preference for education to be less vague. They want to learn about the details of what online sexual harm looks like and the circumstances where they might encounter this (with some suggesting use of real-life cases or scenarios). Several participants said that the main focus of their education was 'stranger danger' when in fact they wanted a broader focus.

> "*I knew about passwords and blocking people, and stranger danger type things, but I didn't know that you can get groomed, or sexual abuse online, or something like that, I didn't know anything about that. (16-year-old female)*"[581]

[577] *Learning about online sexual harm* p71
[578] *Learning about online sexual harm* p72
[579] *Learning about online sexual harm* p61
[580] *Learning about online sexual harm* p62
[581] *Learning about online sexual harm* p45

Parents

54. IN-H1 told us that when IN-A1 and IN-A2 got their laptops, she tried to limit their usage before bedtime, would not allow them to have the laptops in their bedroom overnight and that her partner would monitor their internet history. She said she did not know what her son and daughter had been taught about online safety at school and she had not had any education herself on this subject.[582]

55. Ms Lorin LaFave (Breck's mother) told us:

> *"There were so many people in the story that had they known a little bit more, been better educated, myself included … all of us would have done what we could have, had we been taught where to go."*[583]

56. The children spoken to in the 'Learning about online sexual harm' research said that their parents did not properly understand children's use of the internet. They noted that many parents grew up without the internet and, even those who did use it, did so under very different conditions to young people.

> *"My parents have Instagram and Facebook, whatever, but the experience that they have on it as adults, even if they try and put that experience into the mind of a young person, it's not the same as actually being a young person being brought up around this sort of social media culture. (14–16-year-old female)"*[584]

57. Educating children about the need to stay safe online is an important part of the response to tackling online-facilitated child sexual abuse and exploitation. There is a balance to be struck between the need to educate children about the potential dangers of online sexual harm and the desire by children to use the internet as part of their normal, everyday lives. As one 16-year-old interviewee said:

> *"With school and stuff, people say, 'Have your account on private', but then, it's all about likes and followers and views nowadays … if your account's on private, then only the people that follow you can like your things … people don't really follow the privacy rules because then it don't really benefit them in lots of ways."*[585]

58. Children need to understand how the internet is misused by those intent on sexually abusing children, including by adults masquerading as children. The 'Learning about online sexual harm' research highlights the need for teachers and parents to convey messages about staying safe online in different ways. The 'Relationships Education' and 'Relationships and Sex Education' lessons are therefore important parts of the curriculum that will help prevent children being harmed online.

[582] IN-H1 14 May 2019 4/5-5/25
[583] Lorin LaFave 22 January 2018 107/16-21
[584] *Learning about online sexual harm* p36
[585] *Learning about online sexual harm* p9

Part G

Conclusions and recommendations

Conclusions and recommendations

G.1: Conclusions

1. The number of indecent images of children worldwide is in the many millions. The National Society for the Prevention of Cruelty to Children (NSPCC) has estimated that approximately half a million men in the UK may have viewed indecent images of children. In 2018, the Internet Watch Foundation (IWF) received nearly 230,000 reports of suspected online child sexual abuse. UK law enforcement record more than 10 grooming offences per day and arrest between 400 and 450 people per month for offences of online-facilitated child sexual abuse and exploitation.

2. The last five years have seen improvements in the response of law enforcement, industry and government to online-facilitated child sexual abuse. There have been many technological advances designed to prevent and detect online child sexual abuse, particularly in response to the volume of indecent images of children now available on the internet. More recently, attention has turned to the response to online grooming and live streaming.

3. Despite this, there has been an explosion in online-facilitated child sexual abuse. Law enforcement is struggling to keep pace.

4. There was no evidence to suggest that the number of offenders who use the internet to facilitate their abuse of children is diminishing. It is unclear whether the increase in reporting of online-facilitated child sexual abuse is indicative of an increase in offending or an increase in detection, or both.

5. It is difficult to assess the efficacy of the industry's response to online-facilitated child sexual abuse if the companies do not know the scale of the problem on their platforms and services. The internet companies must do more to identify the true scale of the different types of offending. Such information should be publicly available.

6. It is also difficult to gauge whether the myriad of responses across all sectors are adequate if the offender's underlying motivations and drivers are unknown. We therefore welcome the Home Office's decision to fund the Centre of Expertise on Child Sexual Abuse and its work into the reasons why perpetrators commit child sexual abuse.

7. Most online-facilitated child sexual abuse is committed on the open web and the vast majority of sites that host indecent images of children are available on the open web.[586] By contrast, the dark web can only be accessed by means of specialist software. The abuse found on the dark web is often of the most depraved and deviant kind. While it is not illegal to access the dark web, the dark web is also used by those who have a sexual interest in children, particularly by more sophisticated offenders.

[586] Keith Niven 24 January 2018 4/9-12

Detection and prevention

8. Since the development of PhotoDNA technology in 2009 (and PhotoDNA for Video in 2018), the detection of known child sexual abuse imagery on the internet has improved greatly. As one witness said, PhotoDNA is the "*industry standard*".[587] In addition to this, internet companies have also developed their own technology – such as crawlers to identify large volumes of child sexual abuse imagery and software that can identify child nudity – to detect newly created or previously unseen indecent images.

9. Such developments are invaluable but preventing access to this imagery at the outset is what is required.

10. The National Crime Agency (NCA) has asked industry to pre-screen or pre-filter material before it is uploaded to their platforms and systems to prevent a user from gaining access to child sexual abuse images. While there may be challenges before pre-screening can be implemented, no industry witness said that such a step was technologically impossible. Any argument that pre-screening at the point of upload is unnecessary (given the speed with which known child sexual abuse material can be detected) misses the point. Industry has failed to do all it can to prevent access to such imagery.

11. Indecent images of children can be accessed all too easily. Every time a child sexual abuse image is viewed, the victim is re-victimised, and the offender is potentially drawn into a search for increasingly depraved material. The time has come for the government to stop access to indecent images of children by requiring industry to pre-screen material.

12. The UK government must also continue to prompt change not just nationally but internationally. As a result of the IWF's work, the UK hosts a tiny proportion of child sexual abuse material (0.04 percent). The work of the IWF in removing significant amounts of child sexual abuse material is a genuine success story. The response of some other countries seemingly lags behind. It is beyond the remit of this Inquiry to make recommendations to other countries but it is clear that more needs to be done internationally to try and reduce the amount of child sexual abuse content that is available online and the government should do all it can through the WeProtect Global Alliance to help achieve this aim.

13. Encryption makes data unreadable to unauthorised parties and, in the case of end-to-end encrypted communications such as WhatsApp, iMessage and FaceTime, the content of the communication can only be seen by the sender and recipient. Many of the techniques used to detect online offending do not work where the communication is encrypted. One consequence of encryption, and in particular end-to-end encryption of messages, is that it will make it harder for law enforcement to detect and investigate offending of this kind and is likely to result in child sexual abuse offences going undetected. Encryption therefore represents a significant challenge to the detection of and response to online-facilitated child sexual abuse.

14. In late 2018, the Home Secretary convened a hackathon, where engineers from the leading internet companies developed a prototype that highlights conversations that might be indicative of grooming. That technology has now been launched. The progress made in the course of two days demonstrates what can be done when government, industry and law

[587] Kristie Canegallo 16 May 2019 88/22

enforcement work together. This proactive approach is to be commended and, as the *Online Harms White Paper* itself acknowledges, "*more of these innovative and collaborative efforts are needed*".[588]

15. While developments in technology play an important role in trying to detect such offending, they are not a substitute for the internet companies investing in live moderation. The internet companies need to ensure that there are sufficient numbers of human moderators with a specific focus on online child sexual abuse and exploitation. The value of human moderation is evident from the success achieved by the social network Yubo, whose moderators interrupt live streams to tell underage users to put their clothes on.

Age verification

16. The online abuse of children continues to grow. In the first three months of 2019, the IWF found that 81 percent of self-generated imagery they took action on showed children between 11 and 13 years old, predominantly girls. NSPCC research in 2017/18 recorded that children aged 11 and under were victims in one-quarter of offences where a child had been sent a sexual communication.

17. The majority of children own a smartphone from around the time they start secondary school. Although industry companies either prohibit or discourage children under 13 years old from accessing their platforms or services,[589] the age verification process can be often easily subverted – simply by inputting a false date of birth.

18. While some of the internet companies know how many users have failed the current age verification requirements and how many accounts have been terminated because the user is under 13 years old, such information is not contained within transparency reports and so the true scale of underage use is not public knowledge. Increased transparency about the extent and scale of underage use is required. Transparency reports are now commonplace but, in the absence of independent and consistent reporting standards, the reports only tell the public what the organisation wants and thinks the public should know.

19. Many social media platforms and online services have parental controls. Whilst these can be set so that parents can monitor who their children communicate with and how much time they spend online, the Inquiry heard no evidence of a comprehensive plan from industry and government to address the problem of underage use.

20. Children aged under 13 years old need additional protection. The industry must do more than rely on children to supply their true age when signing up to a platform. There must be better means of ensuring compliance with the current age restrictions.

Education and awareness

21. As the 'Learning about online sexual harm' research revealed, education about online safety at primary school is necessary. The Inquiry welcomes the Department for Education's decision to make 'Relationships Education' in primary schools compulsory from September 2020. Coupled with the introduction of compulsory 'Relationships and Sex Education' in secondary schools, it is anticipated that these lessons will make children more aware of the ways the internet can be misused by those intent on sexually abusing children. Teaching

[588] INQ004232_012
[589] Other than those specifically designed for children under 13 years old.

children about the harm caused by the taking and sharing of self-generated imagery will help to raise awareness of how quickly a child can lose control over who has access to such material.

22. Educating children about the need to stay safe online is an important part of the response to tackling online-facilitated child sexual abuse and exploitation. We heard evidence from parents and children that even those parents who were regular users of social media did not necessarily understand the realities of children's online lives. The 'Learning about online sexual harm' research highlights the need for teachers and parents to convey messages about staying safe online in a variety of ways. The introduction of the new compulsory 'Relationships Education' and 'Relationships and Sex Education' is an essential step in helping to prevent children from being harmed online.

Future reform

23. While we heard evidence of the positive intentions by industry to tackle online-facilitated child sexual abuse and exploitation, there is a lack of a coherent long-term strategy on how this is to be achieved. Responses by industry were varied and sometimes appeared to be reactive rather than proactive. One of the motivating factors that prompted some companies to take action seemed to be the reputational damage caused by adverse media reporting, rather than seeking to ensure the protection of children is given a high priority within their business models.

24. The children who participated in the 'Learning about online sexual harm' research identified five key areas which they thought would enhance their safety online:

- users should be given warnings and advice about online harm when they first set up a device or open a social media account;
- improved enforcement of age restrictions when accessing social media accounts and other online content;
- improved use of privacy settings and, in particular, the use of default privacy functions when setting up an account;
- more obvious and accessible reporting options and stronger action taken when concerns are reported; and
- greater moderation of online activity by apps and platforms.[590]

Industry, government and law enforcement should take note of what children have suggested and take steps to give effect to them.

25. Regulation of the internet industry is now required. No witness who gave evidence to the Inquiry has argued otherwise. The December 2019 Queen's Speech included the government's commitment to progressing the Online Harms Bill, a matter to which the Inquiry will return in its final report.

26. The *Online Harms White Paper* stated that an interim code of practice for child sexual abuse and exploitation would be published by the end of 2019. This did not happen. The interim code will require companies to take reasonable steps across a wide range of areas, all of which are designed to protect children from online-facilitated sexual harm. The code is therefore invaluable and should be published without further delay.

[590] Learning about online sexual harm pp89–90

27. The volume of online child sexual abuse and exploitation offences undoubtedly "*represents a broader societal failure to protect vulnerable children*".[591] Continued and increased collaboration across all three sectors, coupled with education of children about the need to stay safe online, is what is required to protect children.

G.2: Matters to be explored further by the Inquiry

28. The Inquiry will take into account a number of issues which emerged during this investigation, including but not limited to:

- regulation;
- age verification controls and other proposals contained within the *Online Harms White Paper*; and
- the progress of the Ministry of Justice's Criminal Injuries Compensation Authority review.

We anticipate these issues will be addressed in our final report.

G.3: Recommendations

The Chair and Panel make the following recommendations, which arise directly from this investigation.

Those referred to in these recommendations should publish their response to each recommendation, including the timetable involved, within six months of the publication of this report.

Recommendation 1: Pre-screening of images before uploading

The government should require industry to pre-screen material before it is uploaded to the internet to prevent access to known indecent images of children.

Recommendation 2: Removal of images

The government should press the WeProtect Global Alliance to take more action internationally to ensure that those countries hosting indecent images of children implement legislation and procedures to prevent access to such imagery.

Recommendation 3: Age verification

The government should introduce legislation requiring providers of online services and social media platforms to implement more stringent age verification techniques on all relevant devices.

Recommendation 4: Draft child sexual abuse and exploitation code of practice

The government should publish, without further delay, the interim code of practice in respect of child sexual abuse and exploitation as proposed by the *Online Harms White Paper* (published April 2019).

[591] OHY002229_004-005

Annexes

Annex 1

Overview of process and evidence obtained by the Inquiry

1. Definition of scope

The Internet investigation is an inquiry into institutional responses to child sexual abuse and exploitation facilitated by the internet.

The scope of this investigation is as follows:

> "1. *The Inquiry will investigate the nature and extent of the use of the internet and other digital communications technology (collectively 'the internet') to facilitate child sexual abuse, including by way of sharing indecent images of children; viewing or directing the abuse of children via online streaming or video conferencing; grooming or otherwise coordinating contact offences against children; or by any other means. The investigation shall incorporate case specific investigations and a review of existing information available from published and unpublished reports and reviews, court cases, and previous investigations.*
>
> 2. *In doing so, the Inquiry will consider the experiences of victims and survivors of child sexual abuse facilitated by the internet, and investigate the adequacy of:*
>
> 2.1. *government policy relevant to the protection of children from sexual abuse facilitated by the internet;*
>
> 2.2. *the relevant statutory and regulatory framework applicable to internet service providers, providers of online platforms, and other relevant software companies;*
>
> 2.3. *the response of internet service providers, providers of online platforms, and other relevant software companies to child sexual abuse facilitated by the internet;*
>
> 2.4. *the response of law enforcement agencies to child sexual abuse facilitated by the internet;*
>
> 2.5. *the response of the criminal justice system to child sexual abuse facilitated by the internet."*[592]

2. Core participants and legal representatives

Counsel to this investigation:

Jacqueline Carey
Eesvan Krishnan

[592] Definition of Scope: The Internet and Child Sexual Abuse

Complainant core participants:

IN-A1, IN-A2, IN-A3 (Phase two)	
Counsel	William Chapman
Solicitor	David Greenwood and Kieran Chatterton (Switalskis)

Institutional core participants:

National Crime Agency (NCA) (Phase one and phase two)	
Counsel	Neil Sheldon QC
Solicitor	Sarah Pritchard and Karen Park (NCA)
National Police Chiefs' Council (NPCC) (Phase one and phase two)	
Counsel	Debra Powell QC and James Berry
Solicitor	Craig Sutherland and Ian Coleman (East Midlands Police Legal Services)
Commissioner of Police of the Metropolis (Metropolitan Police Service) (Phase one and phase two)	
Counsel	Jason Beer QC (Phase one) Christopher Butterfield (Phase two)
Solicitor	Metropolitan Police Service's Directorate of Legal Services
Home Office (Phase one and phase two)	
Counsel	Tom Kark QC (Phase one) Nicholas Griffin QC (Phase two)
Solicitor	Daniel Rapport (Government Legal Department)
Internet Watch Foundation (IWF) (Phase two)	
Counsel	Peter Alcock
Solicitor	Charles Arrand and Joanne Sear (Shoosmiths)

3. Evidence received by the Inquiry

Number of witness statements obtained:
96
Organisations and individuals to which requests for documentation or witness statements were sent:
Apple
Avon and Somerset Constabulary
BT
Child Redress International (CRI)
Coadec
College of Policing
Cumbria Constabulary
Eastern Region Specialist Operation Unit (ERSOU)
Facebook
Google

Organisations and individuals to which requests for documentation or witness statements were sent:
Greater Manchester Police
Gwent Police
Home Office
IN-A1
IN-A2
IN-A3
IN-H1
IN-X1 and IN-X2, Dark Justice
Internet Watch Foundation (IWF)
James (Jim) Gamble QPM
John Carr OBE
Kent Police
Kik
Lorin LaFave
Metropolitan Police Service (MPS)
Microsoft
National Crime Agency (NCA)
National Society for the Prevention of Cruelty to Children (NSPCC)
Norfolk Constabulary
Chief Constable Simon Bailey, National Police Chiefs' Council (NPCC)
Tink Palmer, Marie Collins Foundation
West Midlands Police (WMP)

4. Disclosure of documents

Total number of pages disclosed: 17,347

5. Public hearings including preliminary hearings

Preliminary hearings	
1	19 September 2017
2	1 November 2018
Public hearings: Phase one	
Days 1–5	22–26 January 2018
Public hearings: Phase two	
Days 1–5	13–17 May 2019
Days 6–8	20–22 May 2019
Day 9	24 May 2019

6. List of witnesses

Surname	Forename	Title	Called, read, summarised or adduced	Hearing day
LaFave	Lorin	Ms	Called	1 of phase one
Palmer	Gillian (Tink)	Ms	Called	1 of phase one
Gamble	James (Jim)	Mr	Called	2 of phase one
Niven	Keith	Mr	Called	2, 3 of phase one
Bailey	Simon	Chief Constable	Called	3 of phase one 6 of phase two
Murray	Alex	Temporary Assistant Chief Constable	Read	4 of phase one
Smith	Richard	Commander	Called Read	4 of phase one 6 of phase two
Blaker	Anthony	Assistant Chief Constable	Read	4 of phase one
White	William	Detective Superintendent	Called	4 of phase one
Ford	Debbie	Assistant Chief Constable	Read	4 of phase one
Webster	Mark	Assistant Chief Constable	Called	5 of phase one
Ackland	Emma	Acting Assistant Chief Constable	Read	5 of phase one
Kirk	Rhiannon	Acting Assistant Chief Constable	Read	5 of phase one
IN-A3			Called	1 of phase two
IN-A1			Read	1 of phase two
IN-A2			Read	1 of phase two
IN-H1			Called	2 of phase two
de Bailliencourt	Julie	Ms	Called	2 of phase two
Polinsky	Melissa	Ms	Called	3 of phase two
Milward	Hugh	Mr	Called	3, 4 of phase two
Canegallo	Kristie	Ms	Called	4 of phase two
Brown	Kevin	Mr	Called	5 of phase two
Roberts	Michael	Mr	Read	5 of phase two
Hargreaves	Susan (Susie)	Ms	Called	5 of phase two
Jones	Robert	Mr	Called	6 of phase two
IN-X1			Read	6 of phase two
IN-X2			Read	6 of phase two
Smith	Richard	Commander	Read	6 of phase two
Papaleontiou	Christian	Mr	Called	8 of phase two
Carr	John	Mr	Called	8 of phase two

Surname	Forename	Title	Called, read, summarised or adduced	Hearing day
Stower	Anthony (Tony)	Mr	Called	8 of phase two
Binford	W Warren H	Professor	Read	8 of phase two

7. Restriction orders

On 23 March 2018, the Chair issued an updated restriction order under section 19 of the Inquiries Act 2005 granting anonymity to all core participants who allege they are the victim and survivor of sexual offences (referred to as complainant core participants). The order prohibited:

(i) the disclosure or publication of any information that identifies, names or gives the address of a complainant who is a core participant; and

(ii) the disclosure or publication of any still or moving image of a complainant core participant.

This order meant that any complainant core participant within this investigation was granted anonymity, unless they did not wish to remain anonymous. That order was amended on 7 March 2019, but only to vary the circumstances in which a complainant core participant may themselves disclose their own core participant status.[593]

On 7 March 2019, the Chair issued a restriction order under section 19 of the Inquiries Act 2005 to protect the identity of IN-X1 and IN-X2 who established Dark Justice. The order prohibits the disclosure and publication of any information that identifies or tends to identify IN-X1 or IN-X2. The order does not prohibit disclosure of this information to the core participants in the Internet investigation, namely: the National Crime Agency (NCA), the National Police Chiefs' Council (NPCC), the Home Office, the Commissioner of Police of the Metropolis (Metropolitan Police Service), the Internet Watch Foundation (IWF), IN-A1, IN-A2 and IN-A3.[594]

In addition to the restriction orders granting anonymity to individuals whose identity has been redacted or ciphered by the Inquiry, the Chair issued a number of restriction orders to prohibit the disclosure and/or publication of evidence that was relevant to the proceedings but which had been assessed as being too sensitive to put into the public domain. The restriction orders relate predominantly to sensitive detection techniques deployed by law enforcement and industry.[595] Some of the evidence subject to these restriction orders was heard in private or 'closed' sessions.

8. Broadcasting

The Chair directed that the proceedings would be broadcast, as has occurred in respect of public hearings in other investigations.

[593] Restriction Order 23 March 2018
[594] Restriction Order 7 March 2019
[595] Restriction orders issued by the Chair in relation to the Internet investigation

9. Redactions and ciphering

The material obtained for this investigation was redacted and, where appropriate, ciphers were applied, in accordance with the Inquiry's Protocol on Redaction of Documents (the Protocol).[596] This meant that (in accordance with Annex A of the Protocol), for example, absent specific consent to the contrary, the identities of complainants and victims and survivors of child sexual abuse and other children were redacted. If the Inquiry considered that their identity appeared to be sufficiently relevant to the investigation, a cipher was applied.

Pursuant to the Protocol, the identities of individuals convicted of child sexual abuse (including those who have accepted a police caution for offences related to child sexual abuse) were not generally redacted unless the naming of the individual would risk the identification of their victim, in which case a cipher would be applied.

The Protocol also addresses the position in respect of individuals accused, but not convicted, of child sexual or other physical abuse against a child, and provides that their identities should be redacted and a cipher applied. However, where the allegations against an individual are so widely known that redaction would serve no meaningful purpose (for example where the individual's name has been published in the regulated media in connection with allegations of abuse), the Protocol provides that the Inquiry may decide not to redact their identity.

Finally, the Protocol recognises that, while the Inquiry will not distinguish as a matter of course between individuals who are known or believed to be deceased and those who are or are believed to be alive, the Inquiry may take the fact that an individual is deceased into account when considering whether or not to apply redactions in a particular instance.

The Protocol anticipates that it may be necessary for core participants to be aware of the identity of individuals whose identity has been redacted and in respect of whom a cipher has been applied, if the same is relevant to their interest in the investigation.

10. Warning letters

Rule 13 of the Inquiry Rules 2006 provides:

> "(1) *The chairman may send a warning letter to any person –*
>
> > a. *he considers may be, or who has been, subject to criticism in the inquiry proceedings; or*
> >
> > b. *about whom criticism may be inferred from evidence that has been given during the inquiry proceedings; or*
> >
> > c. *who may be subject to criticism in the report, or any interim report.*
>
> (2) *The recipient of a warning letter may disclose it to his recognised legal representative.*

[596] Inquiry Protocol on Redaction of Documents

> (3) *The inquiry panel must not include any explicit or significant criticism of a person in the report, or in any interim report, unless –*
>
> > a. *the chairman has sent that person a warning letter; and*
> >
> > b. *the person has been given a reasonable opportunity to respond to the warning letter.*"

In accordance with rule 13, warning letters were sent as appropriate to those who were covered by the provisions of rule 13, and the Chair and Panel considered the responses to those letters before finalising the report.

Annex 2

Glossary

Child Abuse Image Database (CAID)	A single secure database of illegal images of children.
Classifier	A computer programme that learns from data given to it, to then identify similar data.
Cloud	A network of remote servers hosted on the internet to store, manage and process data.
Criminal justice system	The system which investigates, prosecutes, sentences and monitors individuals who are suspected or convicted of committing a criminal offence. This also encompasses institutions responsible for imprisonment, probation and sentences served in the community.
CyberTipline	An online tool which enables the public and industry to report indecent images of children and incidents of grooming and child sex-trafficking found on the internet.
Dark web (or dark net)	Part of the world wide web that is only accessible by means of specialist software and cannot be accessed through well-known search engines.
Encryption	The process of converting information or data into a code that makes it unreadable to unauthorised parties.
End-to-end encryption	Where the content of the communication can only be seen by the sender and recipient, and not by any others – including the providers of the platforms themselves.
First-generation imagery	A child sexual abuse image taken by an adult that has not previously been recorded by law enforcement or industry as indecent.
Freedom of information requests	Under the Freedom of Information Act 2000, members of the public may request information from public authorities.
Geolocation	The process of identifying the location where the internet is being accessed, whether on a computer or a mobile device.
Green Paper	A consultation document that sets out the government's proposals for future policy or legislation.
Grooming	The process by which a perpetrator communicates with a child with the intention of committing sexual abuse or exploitation. Includes forcing, manipulating or enticing a child to engage in sexual activity, either with themselves or with other children.
Hash	A unique digital signature of an image.
Indecent images of children	A photograph or pseudo-photograph of a child under the age of 18 that is deemed to be indecent.
Industry	Includes internet service providers (ISPs); communication service providers (CSPs) such as BT; software companies such as Microsoft; social media platforms such as Facebook; providers of search engines such as Google; and providers of email and messaging services and cloud storage such as Apple.

INHOPE	A foundation that develops national hotlines to help deal with child sexual abuse material online.
Internet protocol (IP) address	A number assigned to a device connected to a computer network.
Internet Watch Foundation (IWF)	An independent, not-for-profit organisation which aims to remove child sexual abuse images and videos from the internet and to minimise the availability of such material.
Known images	An image of a child that law enforcement and/or industry has identified as an indecent image.
Law enforcement agencies	Statutory agencies with responsibility for policing and intelligence, including police forces, the intelligence services and the National Crime Agency.
Live streaming of child sexual abuse	The broadcasting of real-time, live footage of a child being sexually abused over the internet.
National Security Council	A weekly forum in which government ministers meet to discuss national security. The meeting is chaired by the Prime Minister.
Personal data	Information that relates to an identified or identifiable individual.
PhotoDNA	Technology developed by Microsoft which assists in finding and removing known images of child sexual abuse on the internet.
Project Arachnid	A web crawler designed to discover child sexual abuse material on sites that had previously been reported to the Canadian CyberTipline as hosting such material.
Pseudo-photograph	An image, often created on a computer, which looks like a real photograph.
Rapid Evidence Assessment (REA)	A review which gives an overview of the amount and quality of evidence on a particular topic as comprehensively as possible within a set timetable.
Self-generated imagery	A naked or partially naked image of a child taken by the child him or herself.
Trusted flaggers	Individuals, governmental agencies and non-governmental organisations that are particularly effective at notifying YouTube of content that violates its Community Guidelines.
Uniform resource locator (URL)	The network identification or address where a particular page or resource (eg images, sound files) can be found on the world wide web.
Unknown images	An image of a child that has not previously been recorded by law enforcement or industry to be an indecent image of a child.
US	United States of America.
Web crawler	A computer programme that automatically searches for documents, or in this case for indecent images, on the web.
White Paper	A document that sets out the government’s proposals for future legislation.

Annex 3

Acronyms

CAID	Child Abuse Image Database
CEOP	Child Exploitation and Online Protection Centre
CHIS	Children's Charities' Coalition on Internet Safety
CICA	Criminal Injuries Compensation Authority
CRI	Child Redress International
CSA	child sexual abuse
CSAE	child sexual abuse and exploitation
CSAI	child sexual abuse imagery or images
CSAM	child sexual abuse material
CSEA	child sexual exploitation and abuse
CSP	communication service provider
DCMS	Department for Digital, Culture, Media & Sport
DEA	Digital Economy Act 2017
ERSOU	Eastern Region Specialist Operation Unit
ESP	electronic service provider
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
ICAT	Internet Child Abuse Team
ICO	Information Commissioner's Office
IPCC	Independent Police Complaints Commission
ISP	internet service provider
IWF	Internet Watch Foundation
JSaRC	Joint Security and Resilience Centre
KIRAT	Kent Internet Risk Assessment Tool
MLAT	Mutual Legal Assistance Treaty
MPS	Metropolitan Police Service
NCA	National Crime Agency
NCMEC	National Center for Missing & Exploited Children
NGO	non-governmental organisation
NPCC	National Police Chiefs' Council
NSPCC	National Society for the Prevention of Cruelty to Children

NUWG	National Undercover Working Group
PTF	Police Transformation Fund
REA	Rapid Evidence Assessment
ROCUs	Regional Organised Crime Units
SOCA	Serious and Organised Crime Agency
UCOL	Undercover Online
UKCIS	UK Council for Child Internet Safety
URL	uniform resource locator