

TECHNOLOGY BRIEFING SERIES

Briefing 1

Online Child Sexual Abuse Imagery

Centre for the Analysis of Social Media

DEMOS

TECHNOLOGY BRIEFING SERIES


Demos is producing a series of briefings about technology, bringing together experts from policy, practice and tech.

We recognise that technology can present a challenge to policy makers. The aim of this series is to help with that challenge: to explain the technology clearly and succinctly, to report expert opinion with clarity, and to share the views of big players in the world of technology.

This report is the first in the series. It examines child sexual abuse images (CSAI) and their distribution and consumption online.

We are especially grateful for interviews, input and expert advice from the Internet Watch Foundation, CEOP, law enforcement, academics, internet companies and third-sector organisations. A list of interviewees is contained in the appendix.

The report is based on a careful review of existing literature and interviews with various experts, including the Internet Watch Foundation, CEOP, law enforcement, academics, internet companies and third-sector organisations that work with offenders and victims.



EXECUTIVE SUMMARY

New technology has made the task of tackling CSAI significantly more difficult. Specifically, the internet has allowed for new channels of access and distribution that are often based overseas and change frequently with technological advance. While the problem is borderless, law enforcement remains geographically constrained.

There are no easy solutions to this problem. It is not possible to develop a singular, technological solution to this problem: success to date has turned on effective industry self-regulation and commitment of industry resources. This can be illustrated by the small proportion of illegal content identified on social media platforms and other major technology companies, and the reputation of regulators like the IWF.

However, there is a significant amount of investment in using technology to identify material, which is proving valuable in tackling the problem. This needs further support.

Police successes in identifying and prosecuting criminals who operate in this area have tended to rely on both international co-operation and forensic detective work. Investment in this type of policing is necessary. When resources are stretched, it is necessary for policing to focus resources on the most serious offenses: those which can be most effective in reducing harm to children.

Prevention work, while difficult, remains one area where more can be done. There is a general consensus that investing more in schemes to work with potential offenders and prevent re-offending would be a positive move.

It will not be possible to ensure informed public debate about CSAI without responsible reporting of the problem. It is everybody's responsibility to report on the subject carefully, in an informed way, and without conflating CSAI with other harmful online content. Lessons could be learned from well-established reporting guidelines, such as news related to suicide.

01.

Introduction to
CSAI Online

INTRODUCTION

The Internet has fundamentally changed the way in which child sexual abuse images (CSAI) are produced, distributed, consumed and combated. New sources and new channels for the online exploitation of children have been opened up. Millions of images in circulation are easily accessible online by thousands of adults, and are located in places frequently beyond the reach of national law enforcement.

Combating child sexual abuse online will require enforcement and

policy makers to keep up with the pace of technological change. There is, however, no technological silver bullet: child sexual exploitation is an old problem, and decision-makers and the media must do more to acknowledge this.

This briefing brings together expertise from the fields of law enforcement, technology, third-sector support and academia to clearly articulate the current state of play, and offers evidence-based recommendations for policy.

In 1990 the Home Office estimated the figure of video- or paper-based CSAI in circulation to around 7,000 images; today, police seizures often involve millions of digitally stored images.

LEGAL DEFINITIONS

Possessing, making or sharing indecent images of children is a criminal offence in the UK under the Protection of Children Act 1978 and the Criminal Justice Act 1988. Indecent images of children can include child sexual abuse images (CSAI) and self-generated indecent images. Since 2014, the UK Sentencing Council categorises CSAI into three levels:

Category A	Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.
Category B	Images involving non-penetrative sexual activity.
Category C	Other indecent images not falling within categories A or B.

Legally, a child is defined as a person under 18 years of age. In practice, the fight against CSAI tends to focus on images that are clearly illegal and illegal in many countries, typically including children 15 years and younger.

02.

Common Misconceptions about
Child Sexual Abuse Images Online

01.

“Technology is a Silver Bullet.”

There have been important technological responses to CSAI, but technology can't do everything. There is also a gap between who is able to implement technological solutions and who is responsible for the websites which are abused by CSAI offenders.

See more on page 19.

02.

“Social media is primarily to blame.”

Reports suggest only a small proportion of CSAI is hosted on social media platforms, in part because many platforms already take steps to tackle it. However, social media can unwittingly offer new material to consumers posted by young people themselves, and provides new avenues for online grooming.

See more on page 21.

03.

“Finding CSAI online is difficult.”

CSAI is not all hidden. It can be accessed easily, and even stumbled upon.

See more on page 7.

04.

“We can arrest our way out of the problem.”

Law enforcement, third-sector charities and academics agree that the numbers of adults engaging with CSAI online means arresting and prosecuting all offenders would not be possible. This underscores the need for a more wide-ranging response.

See more on page 24.

05.

“A ban on encryption would be effective.”

The difficulties caused to law enforcement by the blanket uptake of encryption should not be underestimated, but frequently are. However, a ban is not a feasible solution, as it would not deal with the problem targeted, and likely create new ones.

See more on page 13.

06.

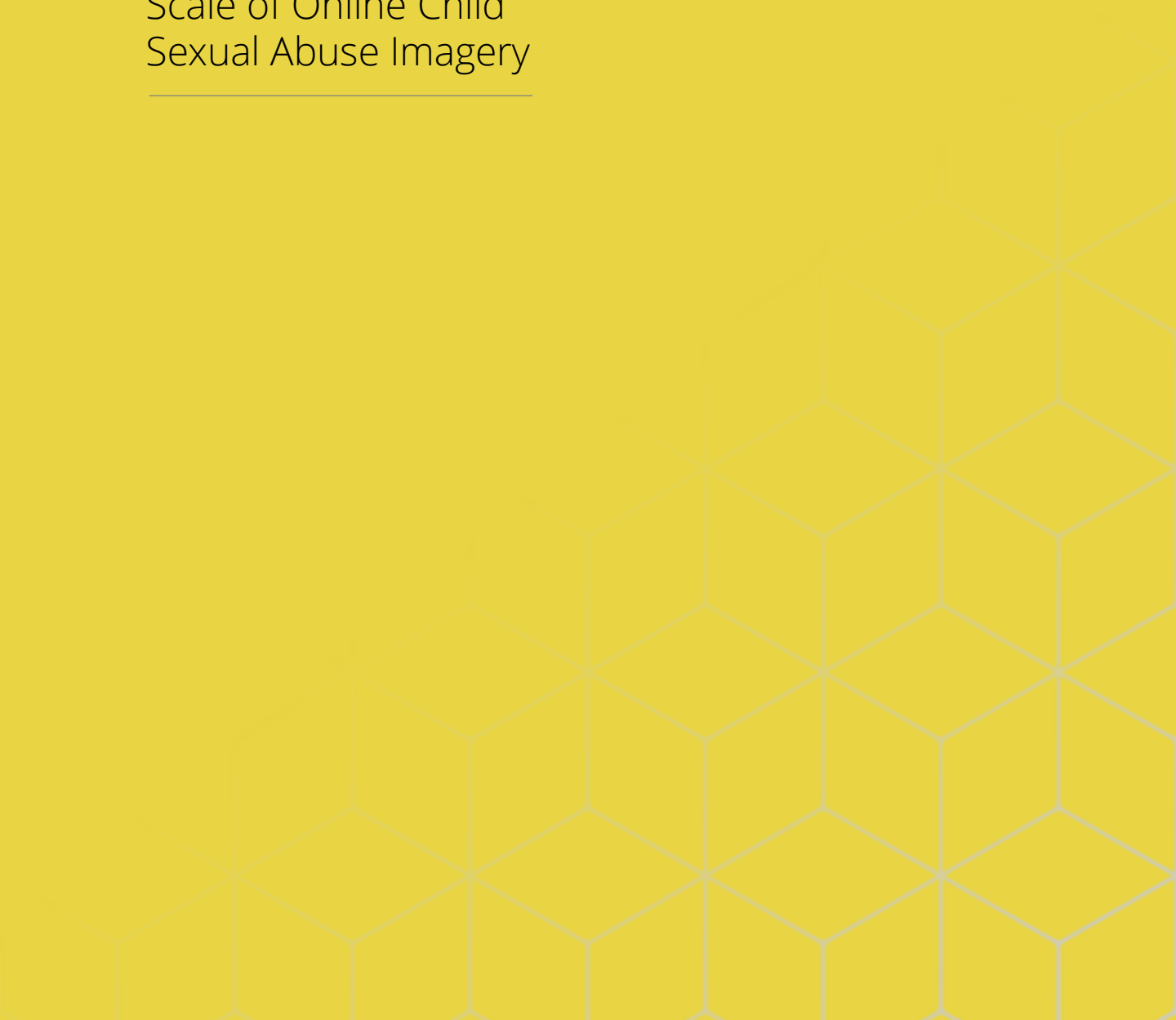
“Industry doesn't self-regulate.”

Experts spoke to the advantages of self-regulation. In the UK, the IWF and its industry partners have tended to be quick to remove content and quicker to react and adapt to technological change.

See more on page 18.

03.

Scale of Online Child
Sexual Abuse Imagery



SCALE OF ONLINE CSAI

Estimating the scale of online Child Sexual Abuse Imagery (CSAI) is difficult. Investigations only identify a fraction of offenders, victims can take a long time to come forward, and strong societal attitudes deter self-reporting.

Accurate statistics for engagement with CSAI online are a vital requirement. Without knowing the scale of the problem, policy and law enforcement responses will remain poorly informed and “the ability to differentiate high risk cases and suspects is reduced.”

However, changes to the way images are produced and distributed has made this extremely difficult. There were 7000 indecent images of children in circulation in 1990 in the UK. According to sources in the police, that figure has now risen to tens of millions. The precise number of individuals convicted of CSAI offences is not published in the UK, but is included in the number of people arrested for ‘obscene publications’ violations. This increased by 134 per cent to 7,324 in 2014/15. In total, 54,000 child sexual abuse offences (contact abuse and CSAI) were recorded in the UK 2015/16.

The actual number of offenders is likely to be even higher. The Child Exploitation and Online Protection Centre (CEOP) estimated in 2013 that 50,000 individuals viewed CSAI each year in the UK. A more recent survey in Germany found that 2.4 per cent of men reported viewing CSAI. Applying these figures to the UK, the NSPCC estimates there may be as many as 590,000 men in the

UK who have at some point viewed CSAI, far higher than previous estimates.

Offenders who access CSAI fall into two broad categories. ‘Consumers’ view and distribute material, while ‘producers’ create material as well as viewing and distributing it. Offenders can also be classed by technological sophistication. Sophisticated offenders take steps to protect their activity online, for example, using encryption (see below). Unsophisticated offenders do not, and are therefore significantly more vulnerable to law enforcement investigation.

Estimates of the scale of CSAI in the UK come primarily from the Internet Watch Foundation (IWF), which publishes annual statistics on the CSAI identified on UK servers. It is difficult to assess how well these estimates reflect the true scale and nature of CSAI offences in the UK – images are widely duplicated and, as with any crime, the criminals we catch aren’t necessarily reflective of the criminals at large.

Although it is well established that CSAI is distributed across the internet, exactly how is less well understood. According to the IWF, less than 0.01 per cent of identified content is hosted in the United Kingdom, down from 18 per cent in 1996. Most of the material the Foundation identifies is hosted in Europe (60 per cent) and North America (37 per cent). According to IWF reports, the Netherlands, the USA and Canada are the most frequent national hosts of CSAI.

(CEOP 2013)

(Home Office 2010)

(ONS 2016)

(CEOP 2013)

(Dombert et al. 2016)

(Jütte 2016)

The IWF's figures suggest that the majority of CSAI is found on image hosting sites (72 per cent) and cyberlockers (11 per cent). Only 0.01 per cent of the CSAI identified by the IWF is hosted on social networking sites. However, according to the Chief Online Safety Officer at Microsoft, Jacqueline Beauchere, many CSAI are detected and removed by social networking sites themselves, before images can be reported to the IWF. This suggests that tech companies could be more transparent about how much material they are encountering and the efforts they are taking to identify, report, and remove CSAI.

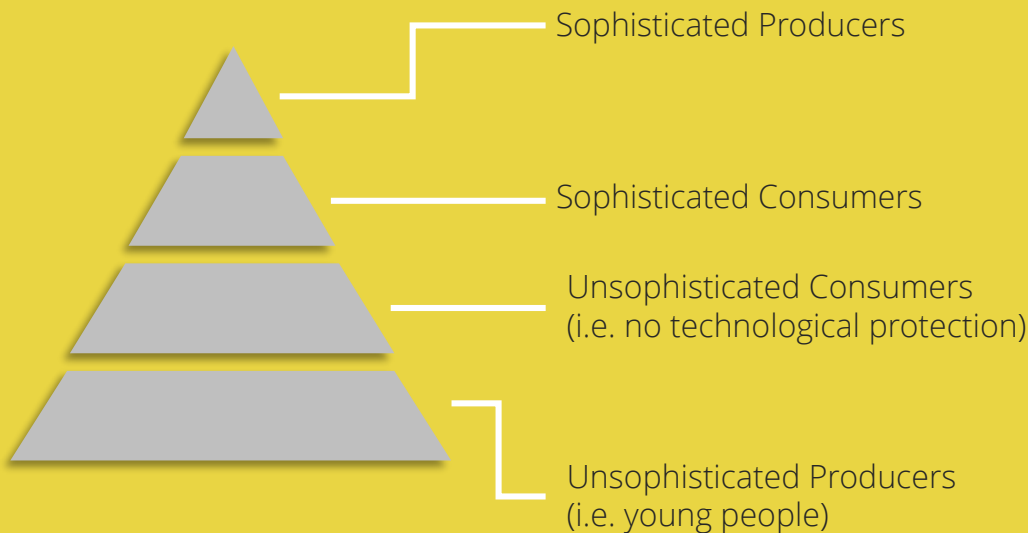
Similarly, the IWF reports that only 1 per cent of the CSAI it identifies is hosted on 'Tor Hidden Services', often referred to as the 'dark net'. Because of the difficulty involved in identifying illegal material on the dark net, this figure is unlikely to reflect the true scale of CSAI on hidden services. This is further compounded by content rarely being 'publicly available', but limited to site or forum members: the IWF is

not legally able to access this content.

Earlier this year, some 20 per cent of the dark net (under Freedom Hosting II) was taken over by hackers, which claimed that half of the sites – or 10 per cent of the dark net – were dedicated to CSAI. Research by the Global Commission on Internet Governance found that CSAI was the most popular type of content on the dark net.

Adding to the growing volume of CSAI is a newer phenomenon. A growing proportion of indecent images of children are 'self-generated' images, produced by minors: one fifth of reported images in 2015 were self-generated. This is supported by the fact that around 16 per cent of young people aged 11-16 have reported sending sexual images in the UK and 1 in 6 people reported to the police for indecent images are minors.

The chart below shows indicative volumes of CSAI producers and consumers online.



An image hosting site stores images uploaded by its users. A cyberlocker is a website allowing users to store and download files. Both are often low-budget, hosted outside the UK and run by a handful of people.

(McCoogan 2017; Lewis 2016)

(Owen & Savage 2015)

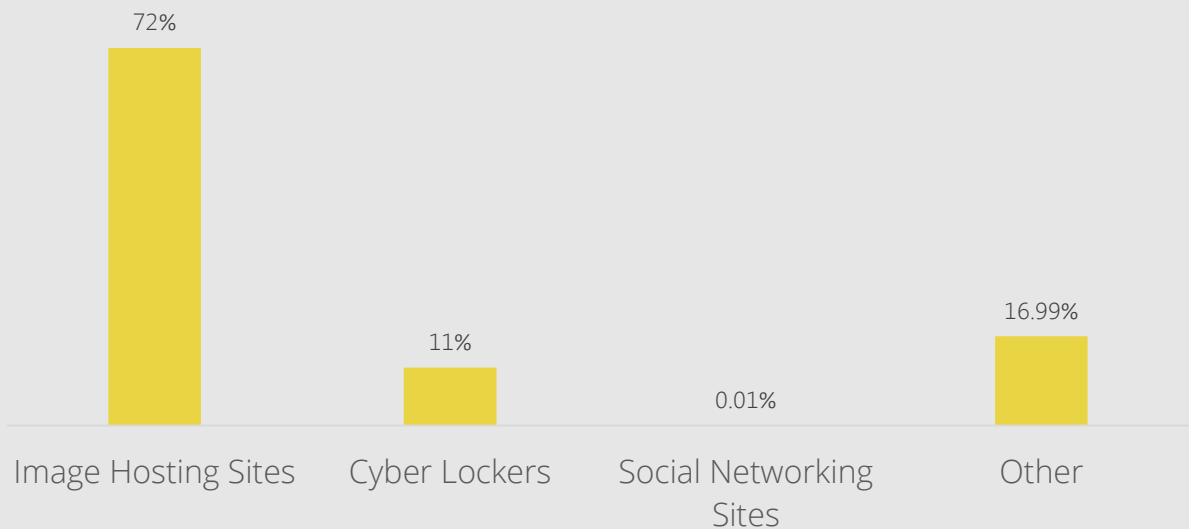
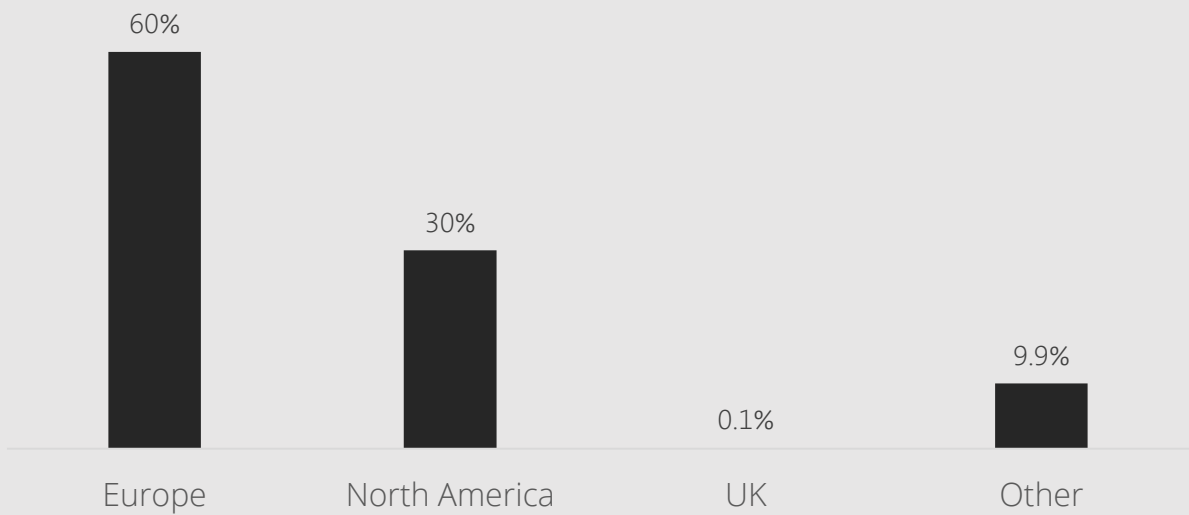
(NSPCC 2016)

(Martellozzo et al. 2017)

(NSPCC 2016)

Where is Child Sexual Abuse Imagery Hosted?

Reported websites (IWF, 2016)



The data shown above is based on the websites reported to the IWF in 2016. Unreported, hidden sites are not included, nor are examples of CSAI that have been removed before a report was filed.

04.

Technology Challenges
in CSAI



“The Internet has significantly changed offender behaviour. The key challenges now are the huge volume of material and the borderless nature of the Internet, compared to the bordered nature of law enforcement.”

Fred Langford
Deputy CEO at the Internet Watch
Foundation

‘Law enforcement offline relies on CCTV and DNA. We still need to find this audit trail in the online space, but it is much harder.’

David Gray
National Online Coordinator for CSE



TECHNOLOGY CHALLENGES

This section explains the key technological developments which have affected the ways in which CSAI is stored and communicated,

changes in offender culture, and the technological solutions implemented or proposed by parties dealing with CSAI online.

Replicability & Interconnectedness

The Internet's capacity to facilitate the storage and transfer of billions of files, to host communities of like-minded Internet users, and to allow both on an international scale, has had predictable consequences for CSAI. Files are replicated in multiple locations, both online and offline.

around the world, close-cooperation by technologically-savvy law enforcement is a necessity. One recent investigation resulted in arrests across fifteen countries in Central and South America, and Europe. Known as Operation Tantalio, it was coordinated by Interpol and Europol to target offenders sharing CSAI over the messaging app Whatsapp.

(Interpol 2017)

A web server is a computer system which stores, processes, and delivers webpages to clients.

Tackling the sources and hosts of the files is difficult: with servers that host Internet content located

Encryption

Encryption – essentially a means of keeping messages or Internet activity hidden except to those who are intended to see them – has become an important part of how the Internet works. According to former director of GCHQ Robert Hannigan, 'encryption is overwhelmingly a good thing', keeping us all 'safe and secure'.

However, the recent uptake of powerful encryption has been picked up and used by various individuals involved in the distribution and storage of CSAI (as well as extremism and the drugs trade). This is especially true of offenders with a relatively high level of technical sophistication. Three forms of encryption are worth exploring in the context of CSAI.

(BBC 2017)

Encrypted Web Browsing and the 'Dark Net'

Some perpetrators rely on 'Tor Hidden Services' (websites where server location is obscured using proxies, also known as the 'dark net'). These websites are accessible through special browsers, such as 'Tor', which encrypt the connection and make tracing a user who is browsing these 'hidden services' difficult. Similarly, those sharing CSAI across peer-to-peer platforms which allow the transfer of files from one computer to another are frequently protected by encryption.

Tor Hidden Services have a reputation for hosting illegal material. As discussed, the volume of CSAI content in these systems is difficult to measure accurately. However, they play an important role in the general availability of material. Being difficult to censor entirely, they can provide a 'warehouse' function, meaning there is always a source of available material.

A proxy network is a computer or program which acts as an intermediary for local requests to other servers.

(Bartlett 2014)

'End-to-end' Encrypted Messaging

End-to-end encryption is where the contents of a message sent between two people cannot be read by a third party. It is increasingly included as standard in most messaging apps and platforms by companies increasingly conscious of their customers' privacy.

Experts confirm that end-to-end encryption has made the tasks of law enforcement more difficult: prosecution requires an audit trail of evidence which is frequently inaccessible to either law enforcement or even a cooperative technology company.

Hardware Encryption

Encryption is also used by offenders to store material. For example VeraCrypt can create a virtual encrypted disk for 'on-the-fly encryption'. TAILS, an encrypted operating system, can be run from a USB. However, the UK's Regulation

of Investigatory Powers Act (RIPA) 2000 requires suspects to give up passwords to encrypted systems or face up to 5 years prison (for suspected cases of 'child indecency').

Encryption has become a difficult policy area in recent months. While used by those accessing CSAI, it is also very widely used by journalists, whistleblowers, and ordinary members of the public. Encryption is the cornerstone of a digital economy and a digital culture. Internet banking, protection from hacking, and secure processing of data all depend on secure encryption systems.

Despite the challenges, limiting the use of encryption is not widely supported by experts in this area. Making the Internet less safe for everyone will not necessarily make it less safe for those sharing CSAI, and will expose British citizens to cybercrime at a time when they are increasingly at risk. The mathematics underpinning encryption are well known, and it is highly likely that security-conscious offenders would continue to use it under any kind of blanket ban.

Social Media Platforms

The last decade has seen a huge growth in social media platforms online, with 96 per cent of 16-24 year olds now using at least one. Although not often used to distribute CSAI, they provide a platform through which young people publish images that are either publically available or vulnerable to being shared without permission. Social media also provides a route between a potential contact offender and

a victim, usually referred to as grooming. A 2014 survey found that 12 per cent of children with a social media profile had received unwanted sexual messages online. In 2012, CEOP identified social networking sites as the most common offending environment for child exploitation: over 80 per cent of online child exploitation cases in the UK involved social networking or instant messaging sites.

(Lilley et al. 2014)

(compared to the UK average of 69 per cent; ONS 2017)

(CEOP 2013)

Digital Culture Change

'Revenge porn' is sexually explicit material shared without a person's consent. Sextortion is blackmail using explicit material.

(Suler 2004)

(Martellozzo et al. 2016)

(Jütte 2016;
Cline 2001)

The Internet has had major impacts on sexual culture, resulting in changes in the nature and sources of illegal pornography. Several studies suggest that the high volumes of Internet pornography in circulation have normalized it, changing attitudes to this type of content among young people. A recent study found that 53 per cent of 16 year olds had seen pornography, and 94 per cent of them had seen it by the age of 14.

Alongside the circulation of existing CSAI, the use of smartphones by young people to take indecent images of themselves, or sharing indecent images of other young people they know, has created a new challenge. Images posted to social media by young people are

also at risk of being misappropriated by paedophiles, and both have inspired new criminal activity, such as revenge porn, sexortion and peer-on-peer abuse.

Technological change has brought with it cultural change among offenders. Online anonymity can create a feeling of safety, and lead to a sense of disinhibition. As noted, ease of access to all pornography has been greatly increased by the web. Voices within the child protection community have suggested that this availability has also desensitized viewers of pornography who may turn to extreme or illegal pornography as interest in legal content dwindles.

Emerging Trends

Technological change continues apace, creating new opportunities for both offenders and those tasked with stopping them. A comprehensive list is impossible, but the following areas are likely to grow in importance in the coming 3-5 years

- Live streaming of abuse or webcams, which is especially difficult to detect in real-time and leaving little or no digital trace.
- Online 'cloud' storage, which reduces the need for offenders to store images offline. Increasing broadband speeds also support the use of online-only services.
- Default encryption, which is now bundled by default with all phones, messaging applications and online services.
- Use of distributed networks, which are difficult to censor.
- Unsecured 'Internet of Things' devices (such as a 'smart' TV) acting as 'safe' repositories of images, without the knowledge of the device owner.
- Improvements in mobile technology, such as the move from 3G to 4G (and the forthcoming 5G), will further encourage streaming and 'peer-to-peer' sharing, and reduce reliance on offline storage.

A distributed network is not reliant on a central server: it could be operated across connected computers. This could be enabled by a new technology called 'blockchain', which acts as a distributed ledger for files or information.

A CHANGING LANDSCAPE



Proliferation of pornography online has changed attitudes to sexual imagery.



Increasing availability of CSAI as internet connectivity becomes universal.



Websites are hosted around the world, requiring international cooperation to combat them.



Access to smart phones has allowed young people to produce sexual images themselves, and images shared by parents are being misused.



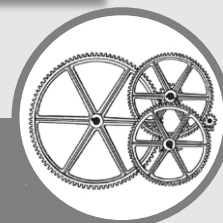
Live streaming of abuse or webcams: especially difficult to detect in real-time and leaving little or no digital trace.



'Sextortion' threat of publicising existing images unless additional images are produced.



Online 'cloud' storage reduces the need for offenders to hoard offline. Increased broadband speeds support the use of online-only services.



Encryption is now bundled with all phones, messaging applications and online services.

05.

Responses
to CSAI



“There is a misconception that tech can do anything - when actually, there are things that might be technically impossible.”

Expert Interviewee



RESPONSES TO CSAI

Law & Policy

The two central pieces of legislation on CSAI in the UK are Section 1 of the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988. Both of these acts stipulate offences for indecent photographs (or pseudo-photographs) of a child.

The 1978 Act establishes offences for taking, making, distributing, and possessing CSAI. This has been more commonly used in prosecutions than the 1988 Act, which concerns the possession of images only. Case law has established that 'making' images under the 1978 Act can include opening email attachments, downloading images to a computer, storing images on a computer, and accessing a website with 'pop-ups' - whenever this is done deliberately with the knowledge that there are (likely to be) indecent images of children (CPS). The Protection of Children Act 1978 has therefore afforded courts the ability to adapt understandings of this offence to reflect new technologies.

Downloading images hosted outside the UK remains an act of 'making' within the UK's jurisdiction.

The Sexual Offences Act 2003 changed the definition of a 'child' to include young people aged 18 years and lower, and also prohibits other child exploitation offences, including grooming.

Before the last election, additional measures were taken by the government to tackle CSAI. The Independent Inquiry into Child Sexual Abuse (IICSA) was announced in 2014 by then Home Secretary Theresa May. Alongside the inquiry, the government has supported the creation of the WePROTECT Global Alliance, the [Child Abuse Image Database \(CAID\)](#), and international cooperation by intelligence agencies. However, complications with the IICSA and the impact of Brexit and counter-terrorism on political priorities have moved the spotlight away from CSAI.

The CAID is discussed in detail below. It is a database containing known CSAI images, each of which has been given a unique 'hash' or ID.

Self Regulation

The IWF has an advantaged role in policing of CSAI in the UK. It is an independent, self-regulatory organisation. Experts within the IWF and external to it have argued that this approach has allowed the IWF to keep up with the pace of technological development over the past two decades, operating with greater agility than a legislative

approach might allow. The IWF currently publishes biennial audits, and points to the speed at which content is now removed and the large reduction in UK hosted content as evidence of their effectiveness.

A Memorandum of Understanding between the NPCC and the CPS formally recognises the work of the IWF and protects its employees from prosecution in the course of their legitimate search for illegal content. The IWF provides a hotline for reporting CSAI and since April 2014 itself has proactively searched for publicly-available images, including those hosted on the 'dark

net', which are reported to host country hotlines or law enforcement.

Since 2015, the IWF has also contributed to the CAID by assessing and categorising images for law enforcement, and will in the future contribute to the CAID directly.

Policing

The policing response to CSAI has been divided between local police forces, which tend to focus on pursuing less technologically sophisticated offenders, and CEOP, NCA and GCHQ, which investigate more complex cases, such as international rings, live streaming, organised crime, and CSAI on the dark net. According to experts, law enforcement has benefited from significant investment in technical skills in recent years, but in order to ensure a national response, continued investment will be

required to guarantee competence across police forces.

There is a clear correlation between CSAI offences and contact offences against children, but a causal relationship has not been established – we do not know whether CSAI satisfies or exacerbates the demand for contact abuse. CEOP has therefore recommended that CSAI offenders be viewed as potential contact offenders to some extent.

(CEOP 2013)

TECHNOLOGICAL RESPONSES

Currently, tackling online CSAI in the UK is a collaborative effort involving policy-makers, law enforcement, technology companies, and civil society organisations. This is in large part due to the technical complexity involved in dealing with aspects of online material, which exceeds the capacity of law enforcement alone.

Child Abuse Image Databases (CAID)

In 2014, the Home Office developed a unified Child Abuse Image Database (CAID) to bring together all CSAI collected by all UK police and the National Crime Agency (NCA). Newly found images can be uploaded to CAID, which automatically compares them to the images hashed in the database and sorts them by level of severity. Thanks to this, law enforcement can more quickly identify any 'first generation images' (newly produced CSAI) and begin the victim identification process.

Internationally, Interpol supplements traditional investigative methods and image analysis with the International Child Sexual Exploitation (ICSE) image and video database. However, differences in countries' CSAI legislation means that Interpol must

adopt a lowest common denominator approach. This is the intention of the 'Worst of-list, which is a list of hashes that identify material that would be illegal in any country.

Efforts have been made to make this technology available to smaller hosts, for whom funding is limited. However, rollout has not taken place in the parts of the web where CSAI is most prevalent because hosts lack the capacity or interest in building preventative measures. One independent expert told us that there is a major problem with the 'long-tail' of providers: small companies that can't deal with the responsibilities of hosting, and may be inadvertently hosting illegal material but do not have the capacity or know how to monitor and remove it.

Website Blocking

The IWF provides a list of URLs known to contain CSAI. Updated twice a day, it can be used by network operators, social media companies and filtering providers to block access to these websites and search engines to stop indexing

them. The IWF also offers domain and payment brand alerts to companies wishing to quickly identify and remove illegal websites that are registered or receiving money through them.

Image hashes are unique 'digital fingerprints' assigned to known CSAI. There are different ways of assigning image hashes, such as PhotoDNA and SHA-2, meaning each image can have multiple different hashes, but two different images cannot share the same hash. New images can be checked against the hashes of known images by a computer, saving time and human resources.

A 'crawler' follows links on websites to discover new websites and stores this information.

Website blocking is seen as a preventative measure - the details of people who have been redirected away from known illegal domains are not typically retained or shared with law enforcement and accessing domains once (or even a few times) are unlikely to form the basis of a prosecution.

Earlier this year, the Canadian Centre for Child Protection launched a new tool called Project Arachnid, which is an automated 'webcrawler' that follows links from known CSAI websites across the clear and dark net. In an initial six-week trial of the crawler, it successfully scanned 230 million individual webpages, 5.1 million of

which were found to have child sexual abuse material. This is the fastest scanning tool yet developed and promises to hasten detection.

Similarly, the IWF internal software development team are currently building to further automate the search for child sexual abuse material on the 'dark net'. The 'Dark Web' crawler was created by Richard Franks of Simon University and has been working with the IWF Technical team to adjust the crawler to compliment the work the IWF already do online. Once the crawler is up and running, it will crawl hidden services for known child sexual abuse and alert analysts to new content.

Artificial Intelligence and Deep Learning

Deep learning is a kind of artificial intelligence (or AI) that allows computer programs to automatically learn and improve from experience.

Tools are being developed by technologists and in partnership with law enforcement to bring the power of AI and 'deep learning' to image recognition. Experts believe this technology has great potential, for instance, in identifying likely new CSAI before it is shared, or in automatically determining the age of a victim or severity of an abusive

act. This technology would greatly accelerate identification of CSAI and of victims, while easing the psychological burden on operatives tasked with classifying this data. However, the pace of technological development requires continued investment here.

Internet Company Responses

Most major Internet companies have taken steps to fight CSAI on their platforms. Facebook, Twitter, and Google use Microsoft's PhotoDNA image hashing system to tackle CSAI on their platforms. This may explain why the proportion of detected CSAI on social media platforms is reportedly low.

In August 2017, the IWF, in partnership with Microsoft

launched a new service – VideoDNA. VideoDNA utilises custom software and PhotoDNA algorithms to hash stills of child sexual abuse images within videos. With this technology, reviewing and categorising videos takes a few minutes rather than hours to complete and with less risk that a reviewer might identify some small parts of the video incorrectly.

Google has introduced changes to its search algorithms to limit results for CSAI queries, as well as restricting access to known websites through its Chrome browser. Both the IWF and Thorn (a US-based NGO) have also worked with the search engines to redirect potential offenders towards help based on their search queries. Facebook also restricts searches for certain keywords across its services.

In 2006, service providers formed the Technology Coalition to jointly fight online CSAI and develop new tools. In partnership with the US National Center for Missing and Exploited Children (NCMEC), they made over 8.1 million reports of suspected CSAI in 2016 alone. However, NCMEC does not publish a breakdown of these figures so it is

not known where this material is most commonly found.

Despite having adopted Terms of Service and technical tools that tightly restrict illegal and even 'grey area' content, social media companies remain under pressure. The volumes of content on these websites, numbered in the billions of photos, comments and messages, make policing the platform difficult. Provision of messaging platforms also provides a channel between offenders and victims, a tool exploited by online groomers. Finally, they provide an environment in which young people, and parents or friends of young people, are encouraged to share images. Despite privacy warnings, these are often public, and used as material by offenders.

International Investigations

In 2014, a joint Australian-Europol investigation gained access to Playpen, a website distributing CSAI. The FBI was able to unmask users accessing the site. When it was shut down in February 2015, there were over 215,000 users and 23,000 images and videos. There have been some 900 arrests and investigations continue.

The UK is frequently seen as the global benchmark for combating CSAI. The IWF, CEOP, GCHQ, the NSPCC and other charities, and law enforcement, have formed a strong national network of cooperation. Nonetheless, experts did note that even greater levels of cooperation could be achieved.

Major successes in investigating CSAI distribution rings have tended to rely on two pillars: international cooperation and forensic detective work.

Europol, Interpol, the FBI, and national enforcement around the world have worked together on

some of the largest operations in the last decade.

Formed in 2015, the WePROTECT Global Alliance emanated from a merger of the Global Alliance Against Child Sexual Abuse Online (led by the US Department of Justice and EU Commission) and the UK's WePROTECT initiative, and represents the most comprehensive global initiative to establish coordinated and comprehensive national responses to CSAI. Other initiatives include INHOPE, an international network of hotlines to report illegal content online.



“The problem is the “long tail” of providers - small companies hosting material that can’t deal with the responsibilities that come from hosting. The big players can’t do everything.”

Expert Interviewee



05.

Preventing
Online CSAI

PREVENTION

Efforts to address online CSAI have largely focused on the detection and prosecution of offenders and protection of victims, but far less has been done in the realm of prevention. Experts across the board have highlighted the need for a different approach to prevention, including the NSPCC, which stated last year that 'it is a focus on prevention that will make the long-term difference.'

(Jütte 2016)

Currently, the main source of help for potential offenders in the UK is the Lucy Faithfull Foundation, which provides the Stop It Now! Helpline (0808 1000 900) and Get Help website (get-help.stopitnow.org.uk) for abusers and those at risk of abusing. The Specialist Treatment Organisation for the Prevention of Sexual Offending (StopSO) also supports potential offenders by helping them find trained therapists and providing training for professionals. Despite the work of these organisations, support pre-offence is limited in its reach and scope. For example, the Stop It Now! helpline estimates that it misses around 1500 calls each month due to lack of resources.

(Beier & Loewit 2013)

(Beier et al. 2014)

(Moj 2017)

Better public understanding might encourage potential offenders to seek help sooner and avoid offending. Germany's Dunkelfeld Prevention Project (www.dont-offend.org) has led the way in prevention internationally. The project began in 2005 as a large-scale media campaign advertising free confidential medical treatment to paedophiles who wanted clinical help.

For instance, the campaign slogan was:

"You are not at fault for your sexual feelings, but you are responsible for your sexual behaviour! There is help available! Don't offend!"

Over 8000 people have sought help through the project since its inception and some 260 people are currently in therapy. Treatment consists of cognitive behavioural therapy and optionally medication to either reduce sex hormones or their effect. The Dunkelfeld project has been a source of much-needed information on non-offending paedophiles and early academic assessments of its effectiveness are positive.

The second approach adopted in the UK has been to help convicted offenders refrain from re-offending. Reoffending rates for sexual crimes are actually relatively low – in the UK, it is around 15 per cent (compared to 40 per cent for theft, for example) – further reinforcing the view that interventions must take place prior to the first offence. In prison, CSAI offenders can take part in Sex Offenders Treatment Programmes (SOTP), including one programme specifically focused on Internet crimes. Evaluations of these programmes have been largely positive, finding significant decreases in pro-offending attitudes. However, there is anecdotal evidence that many CSAI offenders in the UK do not receive long enough prison sentences to take part in these programmes while serving their sentences.

Outside of prison, Circles UK offers support for ex-offenders to reintegrate into the community. Circles brings together several volunteers from the community who meet regularly with the ex-offender to help reduce their social isolation, develop pro-social behaviours, and follow any treatment programmes. In 2015/16, there were 137 ex-offenders in the programme. However, there have been no systematic studies of the effectiveness of the Circles.

As well as programmes for offenders and potential offenders, there are also programmes to educate potential victims. The

leading example of this in the UK is the CEOP's Thinkuknow curriculum and related teaching resources, which was estimated in 2009 to have reached 14 per cent of UK children. The programme has been shown to children's likelihood of reporting threatening online experiences, but did not affect their propensity to share personal information or interact with strangers. It is likely that Thinkuknow has improved in effectiveness since this review, as resources have been developed that are more targeted to different age groups and using more varied teaching styles, but no evaluations have been conducted since.

(Davidson et al. 2009)

06.

Recommendations

We conclude there are seven areas in which government, tech companies and the media might improve in combating CSAI.

Improve Measurements of Online CSAI

Better estimates for the amount of content circulating on the Internet, and the numbers of UK users viewing it, are vital. Law enforcement reports should distinguish between 'contact abuse', online crimes, and CSAI specifically. Technology companies should, where accurate data is available, be more transparent about the volumes of material found on their platforms.

Focus on the Top of the 'Pyramid'

If indeed the number of adults engaging with CSAI is as high as predicted, and the goal is to minimise harm to children, it is right that law enforcement must focus on dismantling the top of the 'pyramid': contact abuse and those producing CSAI. This is not being 'soft on paedophiles', but rather a sensible way of targeting limited resources.

Invest in Technology

Although technology is not a silver bullet, it is vital that law enforcement can keep pace with technological change. Advances in technological solutions have been widely hailed by experts in enforcement and prevention, and the development of future tools in areas such as image categorisation and biometric victim identification must be supported.

Facilitate Sharing and Cooperation

Designing new technology, improving existing technology and adopting new tools in the fight against CSAI requires the legal sharing of highly sensitive data. This must be carefully facilitated: without access to data, it is more difficult for researchers to develop tools, and without access to tools, websites are not able to implement them to curtail CSAI.

As the vast majority of CSAI is stored outside of our borders, international cooperation will be the key to combating it. In the wake of Brexit, ensuring close collaboration between international police forces must be prioritised.

Educate

We strongly believe that digital life skills should be part of the PSHE curriculum, and that the pitfalls of sharing content online, including sexual content, should form part of the syllabus. As the amount of self-produced illegal content continues to increase, stopping this at its source is the only sensible response. Education is needed to support potential victims and perpetrators of sextortion and peer-on-peer abuse, a growing problem.

A Greater Focus on Prevention

The NSPCC advised in their 2016 report that it would not be possible to “arrest our way out” of the problem, a sentiment echoed by every expert we interviewed. Estimates of the number of individuals who may have viewed CSAI range from 50,000 to over 500,000; even taking the lowest estimates, locking up all perpetrators is not a viable option.

More funding could be made available to charities dealing with preventing contact paedophilia like the Lucy Faithfull foundation. Awareness of their work, and helplines for people concerned about their own feelings, should form a part of media coverage.

Report Responsibly

It will not be possible to ensure informed public debate around online CSA without responsible reporting practices on this issue. Four preliminary guidelines are suggested as good practice reporting tips:

First, images should be referred to as either ‘indecent images of children’ (IIOC) or ‘child sexual abuse images’ (CSAI). The term ‘child pornography’ is misleading: pornography is material that is produced and consumed by consenting adults, which cannot include children. Referring to child abuse material as ‘pornography’ minimises the necessarily abusive way in which material is produced.

Second, reports should give details of sources of support for both victims and potential offenders. This can encourage victims to come forward and potential offenders to seek help. The purpose of potential abusers charities is not to defend paedophiles, but protect children, in a similar way to other crime prevention interventions.

Third, broader context should be given. According to the NSPCC, in 90 per cent of cases, offenders have a close connection (such as family, neighbour, or teacher) with their victims. In addition, a significant proportion of material is generated by children and young people themselves. Reports on incidents of abuse should help provide this context to better equip children and their guardians.

Fourth, caution should be exercised when referring to the methods of abuse, including grooming, and sharing and storage of images. Details of the methods used may inform other offenders. Lessons should be learned from the success of the Samaritan’s guidelines for reporting suicide.

FOR MORE INFORMATION

To report child abuse to the police in the UK, call 999 or 101. More information is available at www.gov.uk/report-child-abuse.

If you are worried about a child's safety, you can also call the National Society for the Prevention of Cruelty to Children (NSPCC) on 0808 800 5000 or go to www.nspcc.org.uk.

To learn about and contribute to the Independent Inquiry into Child Sexual Abuse (IICSA), go to www.iicsa.org.uk.

To report online child abuse images and learn about the Internet Watch Foundation (IWF), go to www.iwf.org.uk.

To find help for offenders or potential offenders in the UK, go to the Lucy Faithfull Foundation (www.lucyfaithfull.org.uk) or the Specialist Treatment Organisation for the Prevention of Sexual Offending (StopSO) (www.stopso.org.uk). For resources overseas, go to helplinks.eu.

For educational materials on CSAI, go to CEOP's Thinkuknow programme www.thinkuknow.co.uk.

EXPERT INTERVIEWEES

Eric King, Former Deputy Director at Privacy International
Katie O'Donovan, Public Policy Manager at Google UK
Elena Martellozzo, Senior Lecturer at Middlesex University
Jonathan Baggaley, Chief Executive of the PSHE Association
Fred Langford, Deputy CEO of the Internet Watch Foundation
David Gray, National Online CSE Coordinator for England & Wales Police
Jacqueline Beauchere, Chief Online Safety Officer at Microsoft
Brooke Istook, Strategy and Operations Director at Thorn
Yiota Souras, Senior Vice President, General Counsel at NCMEC
John Shehan, Vice President, Exploited Children Division at NCMEC
Novi Quadrianto, Associate Professor at University of Sussex
Julie de Baillencourt, EMEA Safety Policy Manager at Facebook

We would also like to thank the experts who contributed to the research but who did not wish to be named in the briefing paper. Demos is committed to gathering input from a wide range of organisations and experts on this issue. Due to time constraints, some organisations may not have been contacted during the research period. However, we continue to invite suggestions and contributions.

CONTRIBUTORS

Alex Krasodowski-Jones
Alex.Krasodowski@demos.co.uk

Camille White
Dominic Eccleston
Oliver Marsh

DEMOS

www.demos.co.uk