NETCLEAN REPORT 2019

A REPORT ABOUT
CHILD SEXUAL ABUSE CRIME

INTRODUCTION

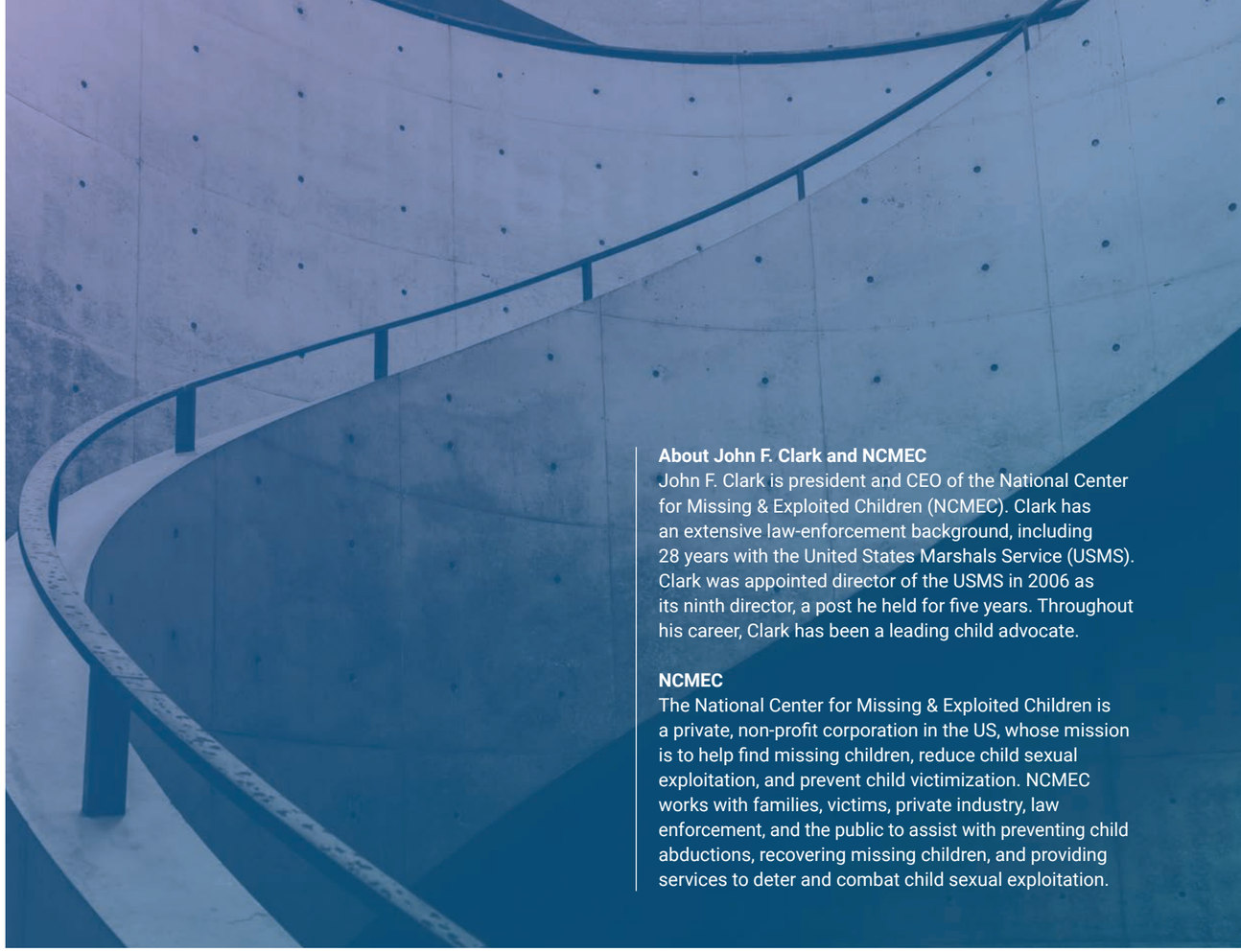
RESULTS

IN CLOSING

INTRODUCTION

BY USING TECHNOLOGY TO OUR ADVANTAGE WE CAN PREVENT CRIME AND SAFEGUARD CHILDREN

By John F. Clark, President and CEO
National Center for Missing and Exploited Children (NCMEC)



About John F. Clark and NCMEC
John F. Clark is president and CEO of the National Center for Missing & Exploited Children (NCMEC). Clark has an extensive law-enforcement background, including 28 years with the United States Marshals Service (USMS). Clark was appointed director of the USMS in 2006 as its ninth director, a post he held for five years. Throughout his career, Clark has been a leading child advocate.

NCMEC
The National Center for Missing & Exploited Children is a private, non-profit corporation in the US, whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation.

I am proud and honoured to have been given the opportunity to introduce the NetClean Report 2019. Child sexual abuse crime is a complex crime and sharing knowledge is key to both understanding and working to stop it. Over the past five years, the NetClean Report has contributed to a better understanding of child sexual abuse crime and the 2019 report adds yet more much needed insights.

As the central hub for cybertips from all US based platform providers, the National Center for Missing and Exploited Children (NCMEC) is acutely aware of the growing problem of child sexual abuse material across the globe. In 2013 the number of cybertip reports received by NCMEC was 1,106,072. In 2018 this had increased to 18,462,424 reports about online child sexual abuse.

Digital development has enabled offenders to produce and share child sexual abuse material at a previously impossible scale. In addition, the last decade's development of social media platforms and gaming platforms has enabled offenders to reach children directly, and abuse them over the internet without meeting them in person, adding a new dimension to this crime. Live-streaming services, examined closer in this report, has pushed this development further.

As is the case on all platforms, live-streamed child sexual abuse material is generated in several different ways – either voluntarily, by coercion or by force. However, live-streaming comes with its own challenges. The streaming takes place in real time, on encrypted channels and with no trace left afterwards unless someone records or takes screenshots of the stream.

Another problem that needs to be considered with the development of technology is on which platforms child sexual abuse is discussed and material shared. It is easy to assume that offenders leave old platforms and move with the latest technology and trends onto the latest fora for communication. However, it is not as simple as that. There is still activity on fora that were commonly used 15 years ago. Old spaces are not deserted because new ones come along, instead the problem and dissemination of online child sexual abuse expands and develops across all available platforms.

Similarly, as this report shows, child sexual abuse material is also stored across all available devices and spaces, from computers and laptops, to mobile phones, USB sticks and in online storage spaces such as cloud storage.

It is frequently said that technology is the driver of this problem. However, it is also a possibility and means to do something about it. By using it to our advantage we can prevent crime, safeguard children and stop offenders. Equally important to prevent this crime is building and sharing knowledge about all aspects of it.

What we are seeing today is encouraging. Instances of child sexual abuse, historical and current, are being discussed in the media and by decision makers across North America and Europe, shining a light on issues that we previously allowed to be ignored. The topic has moved higher up on the political agenda and awareness of the importance of dealing with it is increasing.

The NetClean Report is an important document and tool that adds to the knowledge base about this crime and helps create the awareness needed to keep this topic high up on the agenda. Not only does it gather and present insights from law enforcement professionals that work with these crimes every day. It is also unique in the focus that it puts on the business world's response to protecting their internal IT environments. This needs to be discussed more.

When employers ensure that their employees do not commit reprehensible crimes that might also physically affect children in their vicinity, they are also taking a tactical, moral and ethical step to protect the workforce of tomorrow.

We all need to collaborate. The online world belongs to everyone, and we must make it a safe space for future generations. I believe that initiatives like the NetClean Reports and other initiatives to understand child sexual abuse in the context of developing technologies are vital to ensuring a sustainable approach to stamping out child sexual abuse.

EXECUTIVE SUMMARY

The NetClean Report 2019 is based on two different enquiries. One with law enforcement as is always the case in the NetClean Reports, and one enquiry designed to understand businesses' response to the problem of child sexual abuse material in their IT environments. The report also includes a third section where we present an overview of technologies and methods available to businesses to stop child sexual abuse material.

In preparation for the NetClean Report 2019 we surveyed law enforcement officers to garner their opinions and insights into the problem of live-streaming. We also looked at trends, how child sexual abuse material is stored and how technology developments present both challenges and opportunities.

In the business part of the report we questioned companies with more than 5,000 employees, to see whether they have policies, action plans and technology in place that address the fact that their IT environment might be used to facilitate the consumption of child sexual abuse material.

Live-streamed child sexual abuse

The results showed that live-streamed child sexual abuse is increasing. However, opinion is split on whether this crime can be classed as frequently occurring, or uncommon.

Voluntarily and induced (through grooming or sexual extortion) self-produced live-streamed child sexual abuse were both reported to be common types of live-streamed material in investigations. However, distant live-streamed child sexual abuse, such as paid for webcam shows, were reported to be less common.

Victims and offenders

Both victims and offenders of voluntarily or induced self-produced live-streamed child sexual abuse were reported to come primarily from the US and Europe. Important to note is that a large proportion of the respondents are from the US and Europe, and that most police officers work primarily on cases close to where they are based. Therefore the result does not necessarily represent the global situation.

Victims of distant live-streaming were reported to come primarily from Asia (a majority from the Philippines), but also from Europe, Russia and the US. Offenders of distant live-streamed child sexual abuse were reported to come from North America and Europe, but also Asia, Russia, Australia and New Zealand.

There was a big difference in opinions as to whether there is an overlap between offenders who groom/extort children and offenders who order distant live-streaming, splitting the opinion of the surveyed police officers in half.

A large majority of respondents reported that it is common to find other types of child sexual abuse material in investigations that include evidence of live-streamed child sexual abuse.

Storage spaces

Laptops, mobile phones and USB sticks are the most common spaces to store child sexual abuse material, but it is also very common to store material on cloud services. Mobile phones are the type of storage space that is increasing the most, followed by USB sticks and external hard drives, and cloud storage.

The survey showed a wide spread of how much material is already known to the police when they start analysing a new case. In some cases all the material is previously unseen, in some cases all material is already known, with most cases landing in between these polarised findings.

Apps and services

A large number of apps and services are used for producing, sharing and storing child sexual abuse material. The surveyed police officers reported that Skype is the most common app used for live-streamed child sexual abuse. For cloud services, Dropbox and Google services were most frequently reported to be used for storing and sharing child sexual abuse material. Snapchat, Facebook and Kik were the most commonly mentioned social media platforms.

Encryption and AI

The biggest trends reported were an increase in cloud storage, encryption and smartphones. Encryption were reported to be the biggest challenge for law enforcement, but darknet and cloud storage were also frequently mentioned. The technological developments that were seen as most helpful to law enforcement in child sexual abuse investigations was Artificial Intelligence, but also different investigation software and sharing of data/intelligence.

Business policies and action plans

Nine in ten businesses reported having a policy in place that states that it is prohibited to handle child sexual abuse in the company's IT environment. Eight in ten reported having an action plan to deal with the discovery of child sexual abuse material in place.

Technology in place

Eight in ten businesses also reported having technology in place to comply with their policy. Six in ten use filter solutions, often as part of an employee monitoring tool. One in ten businesses reported using a detection solution. One in ten reported having found child sexual abuse material in the organisation's IT environment.

Comments on the findings

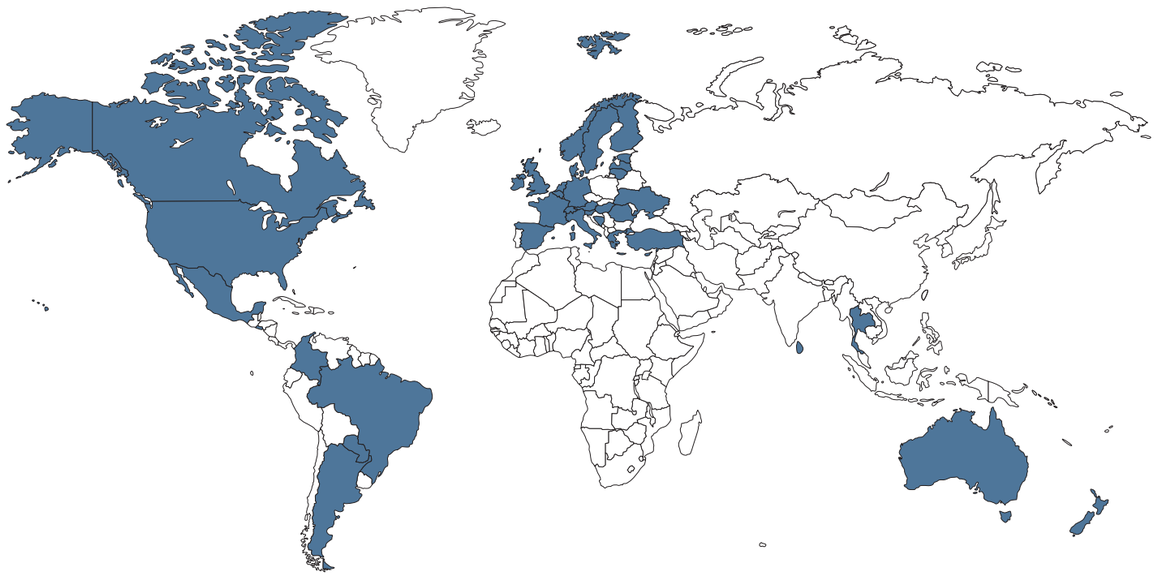
The NetClean Reports include insights by experts who work in different ways with the issue of child sexual abuse. You will find their comments after each different section in this report. Their observations add additional context and depth to the survey findings.

The result of the surveys provide an overview that helps us as a society to understand child sexual abuse crime better. As for NetClean's core clients (businesses and large organisations), it is important to us that we do not only say that it is important for businesses to protect their IT environment, but also comprehensively – why.

For more information about our knowledge building work, please read all our reports. Follow our work by reading our blog, and for an overview of technologies used to stop and detect child sexual abuse material see section three of this report and our blog series: Technical Model National Response. www.netclean.com

ABOUT THE NETCLEAN REPORT 2019

The NetClean Report 2019 is the fifth report in this series. The aim of the report is to ensure greater awareness of and more insight into child sexual abuse crime; to contribute to effective ways of stopping the dissemination of child sexual abuse material; and, ultimately, to reduce sexual abuse of children.



The data in this report is the result of two different enquiries: One with law enforcement, as is always the case in the NetClean Reports, and one enquiry designed to understand businesses' response to the problem of child sexual abuse material in their IT environments. The report also includes a third section where we present an overview of technologies and methods available to businesses to stop child sexual abuse material.

Part one: Law enforcement survey
Part one of this report is based on data collected from police officers across the globe who work on cases pertaining to child sexual abuse crime.

The respondents contributed by filling out a survey anonymously. The police officers are all users of Griffeye Analyze; a digital investigation platform used by law enforcement professionals to analyse large volumes of images and videos. Griffeye is NetClean's sister company.

The enquiry, an online survey, was undertaken between 29 April and 30 August 2019 and administered through Griffeye's user portal. 450 police officers from 41 countries participated in this year's survey. 50.4 percent of the respondents are from North America (of which 46.4 percent are from the US), and 40 percent come from Europe.

In this year's report we look at the following:

1. Live-streamed child sexual abuse – extent and development.
2. Location of victims of live-streamed child sexual abuse.
3. Offenders who consume live-streamed child sexual abuse.
4. How child sexual abuse material is stored.
5. Apps and platforms used for distribution of child sexual abuse material.
6. Emerging technologies – trends, challenges and opportunities.

These areas were selected based on intelligence gathered in previous NetClean Reports, and from conversations with police officers and other stakeholders about what they believe is currently relevant to the issue.

Part two: Business survey
Part two of the report is based on a survey conducted with one hundred businesses with 5,000 employees or more, all operating in the US.

The respondents were all IT/IT Security professionals who either operate as the primary decision maker in their company, or share equally in this role with others. The survey was conducted between 24–27 June 2019.

The survey was conducted as an anonymous online web interview. Partnering with Origo Group and Market Probe International utilising a proprietary specialty B2B panel and ITDM was targeted accordingly. With a non-profit recruitment method, C-Suite Executives, Directors, and Managers that have key decision-making authority were sourced.

In the survey, questions were asked about the following:

1. Whether the business has a corporate policy in place that states that it is prohibited to handle child sexual abuse material within the company's IT environment or on company devices.
2. Whether the business has technologies in place to detect or block child sexual abuse material in the business IT environment.
3. Whether the business has an action plan to deploy if child sexual abuse material is found in the organisation's IT environment.
4. Whether child sexual abuse material has ever been found in the business IT environment.

Part three: Mapping of technology
Part three of the report is an overview of technologies and methods available to businesses to stop child sexual abuse material. The texts are a revision and abridgement of the longer articles published on NetClean's website, which explain technologies and methods in more detail. More information is available on www.netclean.com/technical-model-national-response/

INTERVIEWS IN THE REPORT:
To contextualise the results of the study, we have conducted interviews with a number of distinguished experts in this field, listed here in the order in which they appear in this report:

John F. Clark
President and CEO, National Center for Missing and Exploited Children (NCMEC)

Cathrine Hagström Hägg
Head of Unit and Detective Inspector, Swedish Cybercrime Center, International Sexual Exploitation of Children, National Operative Department – Sweden

Eric Oldenburg
Law Enforcement Liaison, North America, Griffeye

Jim Cole
Supervisory Special Agent, Homeland Security Investigations, Special Agent in Charge Nashville, TN – USA

Anna Borgström
Chief Executive Officer, NetClean

Pat Gelsinger
Chief Executive Officer, VMware

LAW ENFORCEMENT SURVEY: 450 RESPONDENTS FROM 41 COUNTRIES
Argentina, Australia, Austria, Belgium, Bermuda, Bosnia and Herzegovina, Brazil, Canada, the Cayman Islands, Colombia, Cyprus, Denmark, El Salvador, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Mexico, Netherlands, New Zealand, Norway, Paraguay, Romania, Slovenia, Spain, Sri Lanka, Sweden, Switzerland, Thailand, Turkey, Ukraine, the United Kingdom, the United States and International organisations (e.g. INTERPOL or EUROPOL)

Geographic distribution of respondents:

USA	46.4 %
United Kingdom	17.3 %
Sweden	5.3 %
Australia	4.0 %
Canada	3.8 %
Others	22.6 %

EIGHT INSIGHTS INTO CHILD SEXUAL ABUSE CRIME

1 THE SPREAD OF LIVE-STREAMED CHILD SEXUAL ABUSE

- Split view on whether live-streamed child sexual abuse is common or uncommon.
- Voluntarily self-produced live-streaming is most common.
- Distant live-streaming is less common.
- Live-streaming is increasing.

2 VICTIMS OF LIVE-STREAMED CHILD SEXUAL ABUSE

- Many victims of voluntarily or induced live-streamed child sexual abuse come from the US and Europe.
- Victims of distant live-streamed child sexual abuse come primarily from Asia, but also from Europe, Russia and the US.

3 OFFENDERS WHO CONSUME LIVE-STREAMED CHILD SEXUAL ABUSE

- Offenders come from Europe and North America.
- Opinions differ as to whether there is an overlap between offenders who groom/extort and offenders who order webcam shows.
- Offenders in possession of evidence of live-streamed child sexual abuse material also collect other types of child sexual abuse material.

4 HOW CHILD SEXUAL ABUSE MATERIAL IS STORED

- Laptops, mobile phones and USB sticks are the most common storage spaces.
- Storage on mobile phones shows the biggest increase.
- There is both known and unknown material in most investigations.

5 APPS AND PLATFORMS ARE USED TO STORE AND DISTRIBUTE CHILD SEXUAL ABUSE MATERIAL

- Skype is the most common platform for live-streamed child sexual abuse.
- Dropbox and Google services are frequently used to store and share child sexual abuse material.
- Snapchat, Facebook and Kik are commonly mentioned social media platforms.

6 EMERGING TECHNOLOGIES – TRENDS, CHALLENGES AND OPPORTUNITIES

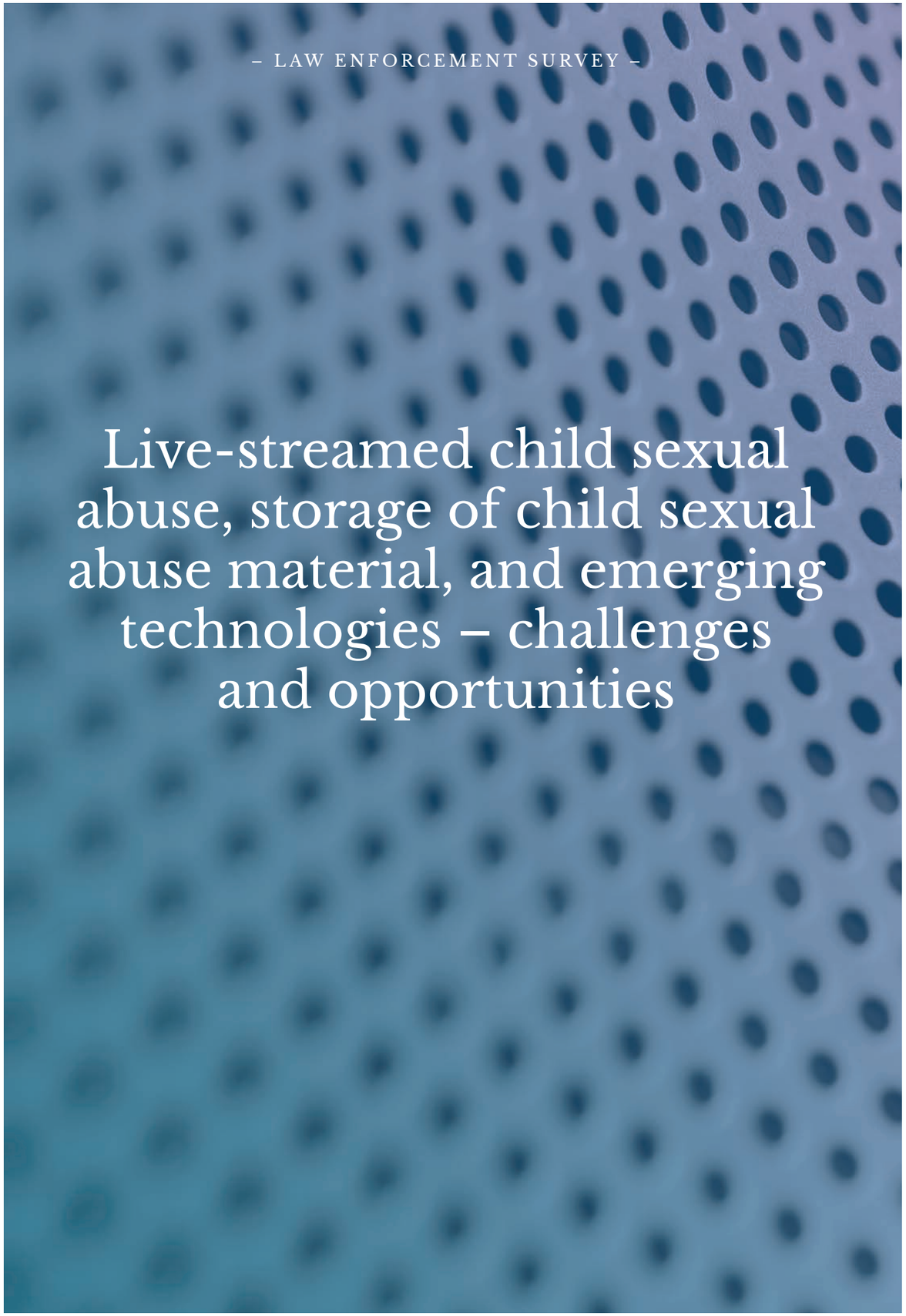
- Trend: Increase in use of cloud storage, encryption and smartphones.
- Encryption is the biggest challenge.
- Artificial Intelligence, investigation software, and sharing of data/intelligence is most helpful.
- One in five police officers have used AI tools in their investigations.

7 BUSINESSES' USE OF POLICIES AND ACTION PLANS TO PROTECT THEIR IT ENVIRONMENT FROM CHILD SEXUAL ABUSE MATERIAL

- Nine in ten businesses have a corporate policy in place.
- Eight in ten businesses have an action plan in place.

8 BUSINESSES' USE OF TECHNOLOGIES TO PROTECT THEIR IT ENVIRONMENT FROM CHILD SEXUAL ABUSE MATERIAL

- Eight in ten businesses have technology in place.
- Six in ten companies use filter solutions.
- One in ten companies have found child sexual abuse material.



– LAW ENFORCEMENT SURVEY –

Live-streamed child sexual abuse, storage of child sexual abuse material, and emerging technologies – challenges and opportunities

Topics covered in the NetClean Report 2019
The NetClean Reports cover current elements of child sexual abuse crime. In this year's report we look more closely at:

Live-streamed child sexual abuse
- Extent and development of live-streamed child sexual abuse
- Location of victims of live-streamed child sexual abuse
- Offenders who consume live-streamed child sexual abuse

Storage of child sexual abuse
- How child sexual abuse material is stored
- Apps and platforms that are used for distribution of child sexual abuse material

Emerging technologies
- Trends
- Challenges
- Opportunities

This part of the report is based on a survey with police officers across the globe who work on cases pertaining to child sexual abuse crime. 450 police officers from 41 countries answered this year's survey. They all answered anonymously, and provided invaluable information for a better understanding of this global problem. We would like to direct a big thank you to all of those who took the time to complete the survey.

1 The spread of live-streamed child sexual abuse

– Split view on whether live-streamed child sexual abuse is common or uncommon.
– Voluntarily self-produced live-streaming is most common.
– Distant live-streaming is less common.
– Live-streaming is increasing.

LIVE-STREAMING

Live-streaming is mentioned as a challenge and an increasing problem in the last three NetClean Reports. In the 2016 report live-streaming was one of four challenges most frequently mentioned by the surveyed police officers. In the 2017 report one in ten police officers said that live-streaming is increasing in chatrooms and chat applications. And in the 2018 report, live-streamed child sexual abuse was mentioned both in connection to trafficking and use of cryptocurrencies.

In the 2019 report, we look at how common live-streamed child sexual abuse is in general; different types of live-streaming; and how it is developing.

Live-streamed child sexual abuse

Live-streamed child sexual abuse is transmitted online in real time to the viewer. Unless the viewer deliberately records the live-stream, no material is saved. Therefore, what we look at here is evidence of live-streamed child sexual abuse; *captures* of the abuse in the form of images and videos.

Three different types

Live-streamed child sexual abuse takes on many guises, but we have chosen in this report to categorise it into the following three types:

1. Voluntarily self-produced live-streamed child sexual abuse
Voluntarily self-produced live-streaming features children or teenagers who voluntarily, with mutual consent, engage in live-streaming in which they are in a state of undress and/or engage in sexual behaviour. It might only be intended for a boyfriend/girlfriend, or posted via a game or app without sexual intent. Because of the sharing nature of the internet captures can find their way into investigations of child sexual abuse.

2. Induced self-produced live-streamed child sexual abuse
This is live-streaming that is a result of grooming or sexual extortion. In the case of grooming the child is coerced into live-streaming while they are in a state of undress and/or engage in sexual behaviour. In the case of sexual extortion they are threatened or forced into live-streaming the abuse.

3. Distant live-streamed child sexual abuse
Distant live-streaming is webcam shows that are ordered by an adult viewer. In the live-stream an adult is also present and is either physically involved in the abuse, or coercing or forcing the child into conducting sexual acts.

SPLIT VIEW ON WHETHER LIVE-STREAMED CHILD SEXUAL ABUSE IS COMMON OR UNCOMMON

Answers from the surveyed police officers show a split view on whether evidence of live-streamed child sexual abuse is common or uncommon in their investigations. Nearly four in ten (37.7 %) of the surveyed police officers reported that the material is common or very common in their investigations. However, just a few percent more (41.9 %) reported that it is uncommon or very uncommon. The rest, one fifth of the police officers, reported that it is neither common nor uncommon.

The added comments also showed their divided views:

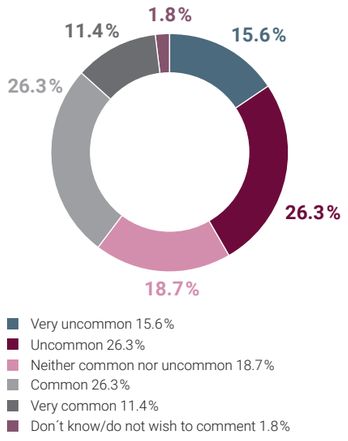
" The last two cases I had the videos were 70 percent or more live-streamed content that had been recorded."

" Last case I worked was 90 percent screen captures of live-streams."

" So far this year we have not had a live-streamed child sexual abuse case."

" I have not yet come across a live-stream sex abuse case."

FREQUENCY OF LIVE-STREAMED CHILD SEXUAL ABUSE IN POLICE INVESTIGATIONS



>>

1 THE SPREAD OF LIVE-STREAMED CHILD SEXUAL ABUSE

>>

VOLUNTARILY SELF-PRODUCED LIVE-STREAMING IS MOST COMMON

Somewhat contradictory to the results above, nearly seventy percent of the respondents reported that captures of voluntarily self-produced live-streamed child sexual abuse is common or very common in their investigations. More than half reported that this is the most common form of live-streamed material that they come across.

Several of the respondents commented that voluntarily self-produced material most often depicts teenagers.

" Teenagers are the most common that I have dealt with."

" I primarily see self-produced sexting videos by teenagers."

Several of the respondents added that it can often be very difficult to determine whether material is voluntarily produced or induced.

" 'Apparently' voluntarily self-produced material can sometimes be hard to distinguish from induced material. Teenagers (or younger) interacting with adults posing as much younger contemporaries is clearly commonplace."

" […] It is difficult to judge whether it is voluntarily or by grooming/threats."

Induced self-produced live-streamed child sexual abuse is common

Captures of induced live-streamed child sexual abuse is reported as slightly less common than voluntarily produced material. However, nearly sixty percent of the respondents answered that it is common or very common to come across evidence of induced live-streamed child sexual abuse material. More than one third of the respondents also reported that induced live-streamed child sexual abuse is the most common type of live-streaming in their investigations.

" The vast majority is live-streaming groomed victim videos."

" Often the videos appear to be of children responding to prompting from the screen they are visible in, eg such as via Skype, Omegle and this is being recorded by the suspect."

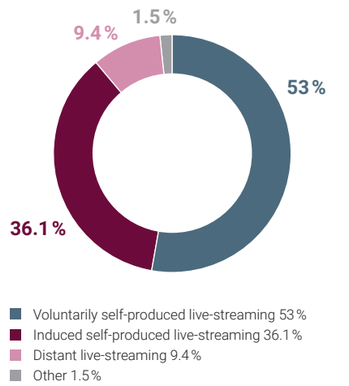
FREQUENCY OF DIFFERENT TYPES OF LIVE-STREAMED CHILD SEXUAL ABUSE

	Very uncommon	Uncommon	Neither common nor uncommon	Common	Very common
Voluntarily self-produced live-streaming	6.7 %	10.5 %	16.1 %	46.8 %	19.9 %
Induced self-produced live-streaming	6.2 %	14.8 %	17.7 %	46.8 %	10.5 %
Distant live-streaming	17.5 %	33.0 %	23.7 %	18.0 %	3.0 %
Other*	11.8 %	5.1 %	26.7 %	1.1 %	0.3 %

** Primarily secret filming, hacked cameras or already recorded child sexual abuse material being live-streamed.*

Respondents were not required to tick all categories, Therefore the total percentage does not add to a hundred percent in all categories.

MOST COMMON TYPE OF LIVE-STREAMED CHILD SEXUAL ABUSE



DISTANT LIVE-STREAMING IS LESS COMMON

In contrast to the two other categories, the respondents reported that distant live-streaming, such as paid for cam shows, is less common. Half of the respondents answered that distant live-streaming is uncommon or very uncommon, and nearly one quarter said that it is neither common nor uncommon.

However, this result might depend on the type of investigations that the respondents work on, as one in ten police officers reported that distant live-streaming is the most common form of live-streaming material in their investigations.

" We don't often see live-streaming but it is common to see remnants in case it occurred. Often paid for exchanges with south east Asian countries where the mother will expose children to the camera. If we are lucky (as an investigator) we will have screen recordings or similar which can be used as part of their prosecution and safeguarding of the children."

" […] I come across material when looking through illegal material and it is mostly recorded from the screen and from Asia."

Other forms of live-streamed child sexual abuse

Nearly half of the respondents also specified that there are other types of live-streaming, although they are less common. According to the surveyed police officers this is primarily material that comes from secret filming or hacked cameras, but it can also be already recorded child sexual abuse material being live-streamed to someone else.

" Hacked webcams streaming footage or cams when the IoT protocols of the device was not secure enough."

" Secret filming."

" Recorded video of child exploitation material streamed via live-streaming platforms."

LIVE-STREAMING IS INCREASING

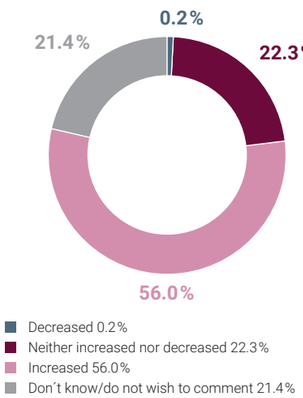
More than half of the respondents reported that live-streaming is on the increase. One fifth of the respondents answered that it is neither increasing nor decreasing.

" It is becoming an increasing problem."

" Uncommon at present in my experience, but appears to be on the increase when considering cases of colleagues in same office."

" Increased in the form of self-production live-streaming (example teenage girls live-streaming for what they believe is a teenage boy)."

WHETHER LIVE-STREAMED CHILD SEXUAL ABUSE HAS INCREASED OR DECREASED IN THE LAST THREE YEARS



2 Victims of live-streamed child sexual abuse

– Many victims of voluntarily or induced live-streamed child sexual abuse come from the US and Europe.
– Victims of distant live-streamed child sexual abuse come primarily from Asia, but also from Europe, Russia and the US.

The surveyed police officers were asked (based on their investigations) to specify from where victims of live-streamed child sexual abuse come, based on category of type of live-streaming.

MANY VICTIMS OF VOLUNTARILY OR INDUCED LIVE-STREAMED CHILD SEXUAL ABUSE COME FROM THE US AND EUROPE

Responses were similar for 'voluntarily self-produced live-streamed child sexual abuse material' and 'induced self-produced live-streamed child sexual abuse material'. Answers indicated that victims are primarily from North America and Europe. Nearly half of the respondents answered that victims come from the US (slightly lower for induced child sexual abuse), whereas one third answered that they come from Europe.

For North America most respondents answered that victims are from the US, but Canada and Mexico were also mentioned.

For Europe, the countries mentioned reflect where the respondents are from. Countries mentioned include the United Kingdom, Sweden, Denmark, Norway, Germany, Ireland, the Netherlands, Switzerland, Austria, Spain, Greece, France, Italy, Austria, Latvia, Romania, Slovenia, and Croatia.

The country where they operate

At first glance, the results showed that the victims come primarily from the US and Europe. However, when the results were matched against the location of the respondents, more than eighty percent listed their own country. This indicates that the results may be skewed to primarily reflect that the large majority of police officers work on investigations close to home, therefore not accurately painting a picture of the global situation.

It is therefore possible to conclude from the results that many victims of both voluntarily and induced live-streaming come from the US and Europe. But it is not possible to conclude what the frequency of this type of live-streamed child sexual abuse is in other parts of the world.

Eastern Europe, Russia and Asia

When looking at the countries that the respondents mentioned instead of or in addition to their own country, nearly a quarter still mentioned Europe and nearly one fifth answered the US. Some geographical areas and countries, from where there were no of very few respondents, were also repeatedly mentioned. These were primarily Eastern Europe, Russia and Asia.

LOCATIONS OF VICTIMS OF VOLUNTARILY SELF-PRODUCED LIVE-STREAMED CHILD SEXUAL ABUSE AND INDUCED SELF-PRODUCED LIVE-STREAMED CHILD SEXUAL ABUSE

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse (webcam shows)
North America*	**45.8 %**	**41.7 %**	**8.5 %**
USA	43.1 %	36.6 %	8.1 %
Canada	2.8 %	2.3 %	–
Mexico	1.0 %	0.4 %	0.4 %
Europe*	**29.6 %**	**33.0 %**	**13.9 %**
Western European countries	24.3 %	18.5 %	6.3 %
Eastern European countries	5.9 %	8.0 %	5.4 %
Russia	**6.3 %**	**6.5 %**	**9.0 %**
Asia*	**3.8 %**	**3.3 %**	**42.2 %**
Philippines	–	–	18.4 %
Thailand	–	–	3.1 %
Cambodia	–	–	1.3 %
Australia and New Zealand	**4.2 %**	**3.3 %**	–
South America	**1.7 %**	**2.2 %**	**2.7 %**
Africa	–	–	**1.3 %**
All over the world	**5.9 %**	**5.0 %**	**1.3 %**
Other**	**1.7 %**	**2.5 %**	–
Don´t know/unable to answer	**1.0 %**	**2.5 %**	**21.1 %**

** Includes answers where respondents have answered North America, Europe or Asia without specifying a country or more specific region.*
*** Specification of other: Respondents have answered western or Caucasian.*

The respondents answered an open question and could provide many different answers.

"Everywhere, including UK, US, Russia, Europe etc as well as third world countries."

"UK, US, Russia, Eastern European countries."

"All over the world, UK, Eastern Europe, Asia, US."

VICTIMS OF DISTANT LIVE-STREAMED CHILD SEXUAL ABUSE COME PRIMARILY FROM ASIA, BUT ALSO FROM EUROPE, RUSSIA AND THE US

According to the surveyed police officers, victims of distant live-streamed child sexual abuse (webcam shows) are primarily from Asia. More than four in ten of the respondents mentioned Asia, and nearly one fifth mentioned the Philippines specifically. Other Asian countries that were mentioned were Thailand, Cambodia, Vietnam, Taiwan, Malaysia, Korea and India.

"Philippines, Taiwan, India, Cambodia."

"Asian countries."

"The cases we have seen are primarily from the Philippines."

Europe and Russia

In addition to Asia, fourteen percent of the respondents reported that victims of distant live-streamed abuse come from Europe. One in twenty police officers (5.4 %) specified Eastern European countries and one in twenty (6.3 %) mentioned countries in Western Europe. Nearly one in ten also reported that victims are from Russia and the US.

"Mainly seen to originate in the old Eastern block/Eastern Europe and Russia."

"I see these cases more common out of eastern Europe."

"Western Europe."

Different countries to their own

In contrast to the other two types of live-streamed child sexual abuse, more than seventy percent of the respondents answered a different country to their own when looking at distant live-streamed sexual abuse. A large majority answered Asia, followed by Europe (with a slight weight towards Eastern Europe) and Russia.

Unable to answer

Also in contrast to the other two categories, more than one fifth of the respondents answered that they did not know the answer to where victims of distant live-streamed sexual abuse are located. This is probably connected to the first question about live-streaming, where four in ten respondents answered that evidence of live-streamed child sexual abuse was uncommon or very uncommon in their investigations.

"As said previously these type of cases are uncommon."

"Have not encountered this type of case."

BREAKDOWN OF THE SHARE OF RESPONDENTS THAT ANSWERED EITHER THE COUNTRY WHERE THEY OPERATE, THIS COUNTRY IN ADDITION TO OTHER COUNTRIES, OR SOLELY OTHER COUNTRIES WHEN ASKED WHERE VICTIMS ARE FROM

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse (webcam shows)
Respondents who mentioned the country where they operate	56.2 %	56.2 %	18.7 %
Respondents who mentioned the country where they operate, but added one or more countries	26.2 %	26.4 %	6.5 %
Respondents who mentioned a different country to the one that they operate in	5.7 %	10.8 %	72.4 %
Respondents who answered that victims come from all over the world	7.6 %	6.5 %	2.4 %

COUNTRIES MENTIONED IN ADDITION TO OR INSTEAD OF WHERE THE RESPONDENTS OPERATE

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse
North America*	**18.6 %**	**18.9 %**	**4.9 %**
USA	12.9 %	12.4 %	2.4 %
Canada	1.0 %	1.6 %	–
Mexico	1.4 %	1.1 %	0.8 %
Europe*	**23.1 %**	**22.7 %**	**17.9 %**
Western European countries	21.9 %	15.1 %	8.1 %
Eastern European countries	6.7 %	7.6 %	9.8 %
Russia	**8.6 %**	**9.7 %**	**14.6 %**
Asia*	**5.7 %**	**5.9 %**	**74.8 %**
Philippines	–	–	33.3 %
Thailand	–	–	5.7 %
Cambodia	–	–	2.4 %
Australia and New Zealand	**1.9 %**	**1.6 %**	–
South America	**1.4 %**	**0.5 %**	**3.3 %**
Africa	–	–	**2.4 %**

** Includes answers where respondents have answered North America, Europe or Asia without specifying a country or more specific region.*

3 Offenders who consume live-streamed child sexual abuse

– Offenders come from Europe and North America.
– Opinions differ as to whether there is an overlap between offenders who groom/extort and offenders who order webcam shows.
– Offenders in possession of evidence of live-streamed child sexual abuse material also collect other types of child sexual abuse material.

Looking at each type of live-streaming, the surveyed police officers were asked (based on their investigations) to specify which countries offenders come from.

OFFENDERS COME FROM EUROPE AND NORTH AMERICA

Similar to the question about victims, responses about voluntarily self-produced live-streamed child sexual abuse material and induced self-produced live-streamed child sexual abuse material were very close in numbers. The respondents reported that offenders are primarily from North America (USA) and Europe (the same countries were mentioned when asked where victims are from). Four in ten (slightly less for induced child sexual abuse) reported that offenders come from North America, and more than one third that they come from Europe.

" All over, but primarily USA."

" USA and western Europe."

The country where they operate

However, again similar to the question about victims, a breakdown of the results showed that nearly nine in ten of the respondents answered their own country. The results most likely reflect the fact that the majority of police officers are working on cases close to home, and don't necessarily reflect what the global situation looks like.

As with the question about victims, this indicates that many offenders come from the US and Europe. However, it does not indicate that there are no offenders in countries not mentioned.

Asia and Russia

Other geographical areas that were mentioned by one in twenty police officers, or more, were Asia and Russia.

If Eastern Europe is removed from the European cohort, it shows five percent on its own. Asian countries/regions mentioned several times were China, Philippines, Malaysia, India, Pakistan and the Middle East.

" Asia, China, Philippines and other countries like Russia."

" Australia, USA, UK, Asian Countries."

" India, Pakistan, Greece."

LOCATIONS OF OFFENDERS WHO CONSUME VOLUNTARILY SELF-PRODUCED LIVE-STREAMED CHILD SEXUAL ABUSE, INDUCED SELF-PRODUCED LIVE-STREAMED CHILD SEXUAL ABUSE AND DISTANT LIVE-STREAMED CHILD SEXUAL ABUSE

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse
North America*	**41.0 %**	**38.7 %**	**22.4 %**
USA	36.9 %	33.8 %	21.1 %
Canada	2.5 %	1.8 %	0.6 %
Mexico	1.2 %	2.7 %	–
Europe*	**32.4 %**	**34.2 %**	**24.8 %**
Western European countries	21.3 %	23.0 %	15.5 %
Eastern European countries	4.9 %	5.4 %	4.3 %
Russia	**5.3 %**	**4.5 %**	**5.6 %**
Asia	**7.0 %**	**6.8 %**	**16.1 %**
Australia and New Zealand	**2.9 %**	**2.3 %**	**5.6 %**
South America	**1.6 %**	**1.8 %**	**1.9 %**
Africa	–	**0.5 %**	–
All over the world	**5.3 %**	**5.0 %**	**3.7 %**
Same country as victim	**0.9 %**	**0.9 %**	–
Unknown or unable to answer	**3.6 %**	**5.3 %**	**19.9 %**

** Includes answers where respondents have answered North America or Europe without specifying a country or more specific region.*

The respondents answered an open question and could provide many different answers.

Distant live-streaming

Responses regarding the location of offenders were more widely spread. More than one fifth of the respondents answered North America, nearly a quarter answered Europe. However, sixteen percent also answered Asia, more than five percent answered Russia, and just as many answered Australia and New Zealand. Similar to the question on victims, nearly one fifth of the respondents said that they don't know or are unable to answer.

" United States, Europe, Australia, New Zealand."

" USA, Germany, Norway."

" US, Russia, India and Asian Countries."

" Russia/Ukraine Philippines/ Thailand."

Different Asian countries mentioned

Although there were not enough answers to draw any firm conclusions, the survey results showed a slight discrepancy in the Asian countries mentioned in relation to location of victims and offenders. Countries mentioned in relation to victims were the Philippines, Thailand, Cambodia, Vietnam, Taiwan, Malaysia, Korea and India. For offenders, the countries mentioned were (in order of frequency) the Philippines, India, Pakistan, China, Thailand, Malaysia, and Indonesia.

The Middle East was also mentioned in the answers regarding offenders, but not regarding victims. The answers for both groups were similar with regards to Europe and North America.

>>

BREAKDOWN OF THE SHARE OF RESPONDENTS THAT ANSWERED EITHER THE COUNTRY WHERE THEY OPERATE, THIS COUNTRY IN ADDITION TO OTHER COUNTRIES, OR SOLELY OTHER COUNTRIES WHEN ASKED WHERE OFFENDERS ARE FROM

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse (webcam shows)
Respondents who mentioned the country where they operate	64.0 %	60.4 %	57.3 %
Respondents who mentioned the country where they operate, but added one or more countries	22.9 %	28.1 %	15.6 %
Respondents who mentioned a different country to the one that they operate in	5.9 %	4.3 %	20.8 %
Respondents who answered that victims come from all over the world	7.2 %	7.2 %	6.3 %

COUNTRIES MENTIONED IN ADDITION TO OR INSTEAD OF WHERE THE RESPONDENTS OPERATE

	Voluntarily self-produced live-streamed child sexual abuse	Induced self-produced live-streamed child sexual abuse	Distant live-streamed child sexual abuse
North America*	**16.4 %**	**23.2 %**	**7.3 %**
USA	12.4 %	10.0 %	7.3 %
Canada	2.0 %	0.7 %	–
Mexico	2.0 %	3.6 %	–
Europe*	**10.4 %**	**13.7 %**	**9.0 %**
Western European countries	5.2 %	4.3 %	4.2 %
Eastern European countries	2.6 %	7.6 %	5.2 %
Russia	**10.5 %**	**5.8 %**	**9.4 %**
Asia	**10.4 %**	**10.1 %**	**25.0 %**
Australia and New Zealand	**0.7 %**	–	**1.0 %**
South America	**1.3 %**	**2.2 %**	**2.1 %**
Africa	–	**0.7 %**	–

** Includes answers where respondents have answered North America or Europe without specifying a country or more specific region.*

3 OFFENDERS WHO CONSUME LIVE-STREAMED CHILD SEXUAL ABUSE

>> **OPINIONS DIFFER AS TO WHETHER THERE IS AN OVERLAP BETWEEN OFFENDERS WHO GROOM/EXTORT AND OFFENDERS WHO ORDER WEBCAM SHOWS**

The surveyed police officers were also asked whether they believe that offenders who pay for distant live-streamed child sexual abuse (webcam shows) are the same individuals who groom and sexually extort children on other platforms.

Their opinions on this differed greatly. One third of the respondents answered that they are the same individuals, and one third answered that they differ. One quarter of the respondents answered that they don't know or don't have enough experience of both types of crime to answer.

" No real correlation between offenders that live-stream and those that groom through other applications from what I have dealt with. While there are a variety of applications used in this crime, most of what I see revolves around an offender using the same means repeatedly. They seem to feel safe/comfortable with a specific app/software and will continue to use it until they feel it has been compromised.

" In my experience offenders tend to stick with one platform or the other, so if they are grooming and eliciting images and video from children on social media platforms, that is what they concentrate on."

" I don't believe they differ. I think there is a strong correlation with those who would live-stream, groom and extort children, and also move to hands-on offending."

" I would say that in my experience, that about half of the offenders I have investigated have sextorted children and also paid for abuse to be streamed."

Different offenders: Live-streaming is seen as more risky

The police officers who were of the opinion that it is different offenders who groom or sexually extort children and who pay for live-streamed webcam shows, reported different views on why this is so. Some commented that most offenders don't need or want to pay for the abuse, or that live-streamed child sexual abuse is seen as more of a risk than grooming.

" My experience is that those extorting are not paying for distant live-streamed, they know they can get it themselves."

" In my opinion if a suspect can get it for free they will always go that route first. I see more offenders trying to extort children personally online via webcam, or other means, than I see them paying for live streamed videos/webcam shows etc."

" […] The risk of paying for live streamed sexual abuse, I can only assume, is that the risk of detection is far too high for the low level offender, as most only appear to have basic technological knowledge and confidence in hiding their actions online."

Different offenders: Live-streaming is seen as less risky

In direct opposition, others said that live-streaming is seen as less risky than grooming, as there is more distance to the victim. Or that live-streaming is a stepping stone to committing hands-on child sexual abuse.

" There is, in my opinion, a desire for offenders to feel "safe", using distant pay to view sites offers a greater perceived safety than the offender making the approach to individual adults or children, perhaps in their own country, with a greater perceived risk of capture by law enforcement."

" The contact the people are having [in distant live-streaming] is adult-to-adult. They are not involved in the child and generally don't interact with the child. I believe this distances themselves from the situation and are different to those who intentionally converse with children."

" I believe that it is more rare that the same types of individuals engage in both activities. I believe that the people that pay for streaming services are those who have not necessarily reached the point of committing hands-on offences yet."

Same offenders

Police officers who answered that the offenders who will pay for webcam shows and those who groom and sexually extort children are the same, commented that this may be for several different reasons.

Several said that offenders will use any means available to access child sexual abuse material and sexually abuse children, and will act on any opportunity that they are given. Some likened it to an addictive behaviour.

" I think anyone with that mind-set and sexual interest will take part in any related forms of deviant behavior if given the opportunity."

" In my opinion and the offenders that I've dealt with personally. Offenders will do what ever it takes to get their "fix" any way that they can. They act in much the same ways that a person who is addicted to an illicit substance does."

Other respondents commented that offenders will use both paid live-streamed child sexual abuse and material acquired from grooming or sexual extortion as a means of payment or access to "climb" in organised forums of offenders (where you only get access to certain "levels" if you upload new and unseen material to the forum).

" In my experience the people who pay/access these kinds of services play an active role in grooming activities. They may be trying to get new videos/pictures to share with their community and climb in this way in their pyramidical structure."

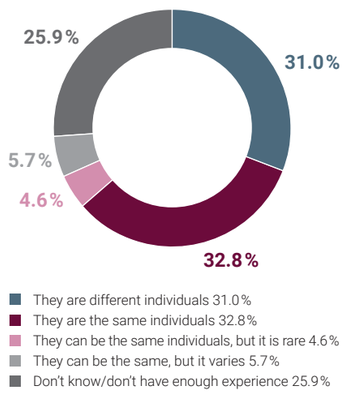
Perceived anonymity

The respondents who answered that offenders move between grooming/ extorting victims and paying for distant live-streamed child sexual abuse (web shows), but mentioned that it is less common, commented that this is as a result of perceived risks with anonymity, and a perceived distance to the child.

" Given an opportunity and understanding of the different platforms offenders can move between them but I believe it too less common. We have found that those using live-stream appear to be more reluctant or even confident to directly engage with children. They appear to be of a mentality that their webcam offending has a higher degree of anonymity due to the fact the victims are often in poor and remote locations with less chance of Law Enforcement Agency involvement."

" I have seen that offenders are not easily convinced to send payment over the Internet for fear of being identified, but that if they feel they are anonymous they will groom and extort children online at every opportunity."

WHETHER THERE IS AN OVERLAP BETWEEN OFFENDERS WHO GROOM/EXTORT CHILDREN ON ONLINE PLATFORMS AND OFFENDERS WHO PAY FOR DISTANT LIVE-STREAMED CHILD SEXUAL ABUSE (WEBCAM SHOWS)



>>

3 OFFENDERS WHO CONSUME LIVE-STREAMED CHILD SEXUAL ABUSE

>> OFFENDERS IN POSSESSION OF EVIDENCE OF LIVE-STREAMED CHILD SEXUAL ABUSE MATERIAL ALSO COLLECT OTHER TYPES OF CHILD SEXUAL ABUSE MATERIAL

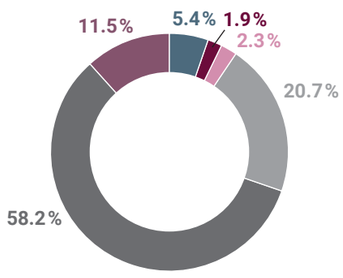
To further try to understand offenders who possess evidence of live-streamed child sexual abuse material, the surveyed police officers were asked whether these offenders also collect or store other types of child sexual abuse material, or if they only engage in live-streamed child sexual abuse.

Eight in ten of the surveyed police officers reported that it is common or very common to find other types of child sexual abuse material in investigations that include evidence of live-streamed child sexual abuse. Less than one in ten (7.3 %) answered that it is uncommon or very uncommon to find other types of material.

" Pretty much guaranteed."

" They are almost always in possession of other child abuse material."

WHETHER OFFENDERS WHO ARE IN POSSESSION OF EVIDENCE OF LIVE-STREAMED CHILD SEXUAL ABUSE ALSO HAVE OTHER TYPES OF CHILD SEXUAL ABUSE MATERIAL



- Very uncommon 5.4%
- Uncommon 1.9%
- Neither common nor uncommon 2.3%
- Common 20.7%
- Very common 58.2%
- Don´t know/do not wish to comment 11.5%

All types of material

According to the surveyed police officers, nearly all types of child sexual abuse material is commonly found in investigations that also include evidence of live-streamed child sexual abuse material.

Hands-on child sexual abuse material produced by another offender

The most common type of child sexual abuse material found in the investigations is hands-on child sexual abuse material produced by another offender. This is the material that is most often referred to when speaking about child sexual abuse material in general terms. More than six in ten respondents answered that this is *the most common* type of material found, and nine in ten of the surveyed police officers answered that this type of material is common or very common.

Voluntarily self-produced material

Voluntarily produced child sexual abuse material was reported as nearly as common, more than eight in ten reported that such material is common or very common. However, only one in ten of the surveyed police officers reported this as the most common type of material.

" 50/50 between voluntary and child sexual abuse images."

Innocent, grooming, sextortion and hands-on material

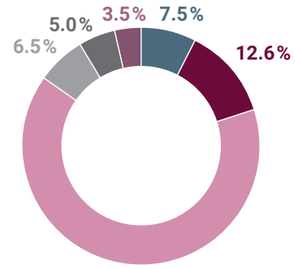
More than six in ten of the surveyed police officers also reported that it is common or very common to find innocent material or grooming material. They reported that it is slightly less common to find sexual extortion material or hands-on child sexual abuse material produced by the suspect themselves.

" It can be hard to tell sometimes if the materiel is from grooming/ sexual extortion if there is no chat from messaging services such as snapchat, kik and skype."

" Hands-on offending does happen but the majority of suspects are image collectors and while possible would place hands-on if the situation presented itself many are not actively seeking one."

It is, although less common than the other types, interesting to note that one in three police officers answered that it is common or very common to find hands-on child sexual abuse material produced by the suspect themselves. Another third of the respondents answered that this is neither common nor uncommon.

MOST COMMON TYPES OF CHILD SEXUAL ABUSE MATERIAL THAT POLICE OFFICERS COME ACROSS IN INVESTIGATIONS THAT INCLUDE EVIDENCE OF LIVE-STREAMED CHILD SEXUAL ABUSE



- Innocent images 7.5%
- Voluntarily self-produced material 12.6%
- Child sexual abuse images and videos 64.8%
- Grooming material 6.5%
- Sexual extortion material 5.0%
- Hands-on child sexual abuse images or videos 3.5%

FREQUENCY OF OTHER TYPES OF CHILD SEXUAL ABUSE MATERIAL, THAT POLICE OFFICERS COME ACROSS IN INVESTIGATIONS THAT INCLUDE EVIDENCE OF LIVE-STREAMED CHILD SEXUAL ABUSE

	Very uncommon	Uncommon	Neither common nor uncommon	Common	Very common
Innocent images (for example holiday images that have ended up in collections of child sexual abuse material)	0.5 %	10.1 %	21.6 %	44.2 %	21.1 %
Voluntarily self-produced material (images or videos that for example teenagers take themselves, but that end up in collections of child sexual abuse material)	–	3.0 %	11.1 %	58.8 %	24.6 %
Grooming material (images and videos that children have been coerced into producing as a result if being groomed for sexual purposes)	1.5 %	7.5 %	23.6 %	49.7 %	16.1 %
Sexual extortion material (images or videos that children have been forced to produce as a result of being threatened)	1.5 %	21.6 %	32.2 %	31.7 %	9.0 %
Hands-on child sexual abuse material by another offender (images or videos of hands on sexual abuse that has been produced by someone else and downloaded by the suspect)	1.0 %	1.5 %	7.0 %	44.2 %	46.2 %
Hands-on child sexual abuse images or videos (that have been produced by the suspect himself/herself	7.0 %	27.1 %	28.6 %	23.6 %	6.5 %

Respondents were not required to tick all categories, Therefore the total percentage does not add up to a hundred percent in all categories.

CATHRINE HAGSTRÖM HÄGG
Head of Unit and Detective Inspector, Swedish Cybercrime Center, International Sexual Exploitation of Children, National Operative Department, Sweden

LIVE-STREAMING IS ON THE INCREASE

My unit works exclusively with international sexual exploitation of children, so I can only comment on distant live-streamed child sexual abuse, and not on the other types of live-streaming mentioned in the report.

We saw our first case of live-streaming in 2010. This type of crime is on the increase, still, we have only handled approximately forty cases so far.

Western countries
We only investigate Swedish offenders, however countries that are often mentioned in the context of offenders are the US, the UK, France, Germany and Australia – large Western countries with, in general, well-to-do populations.

Adult facilitators
The victims come primarily from the Philippines, but we have also seen indications of victims coming from Colombia, South Africa and Romania. Our biggest case to date featured a Swedish man who subjected twenty-five children in the US to sexual abuse online through live-streaming. In this case the children were groomed and threatened by the offender himself.

Cases from the Philippines always involve adults who facilitate the abuse. Contact often starts on Philippine dating sites for adults, from where the conversation moves to private channels, primarily Skype, but also Messenger and WhatsApp, where the conversation moves on to children. These are also the channels where the abuse takes place.

There are several reasons why this crime is especially prevalent in the Philippines. It is a poor country, and one where the population communicates well in English, making international communication easy. There is a well-established sex-industry, limited police resources, a developed IT-infrastructure, cheap mobile phones, and simple ways of making international money transactions. The big difference between the Philippines and other South East Asian countries is probably the common use of the English language.

Other types of child sexual abuse material
In all our cases, offenders have been in possession of other types of child sexual abuse material. However, except for the US case, we have not found evidence that they have themselves groomed or threatened children. Only in one case have we found images of hands-on abuse by the offender himself.

Our sample is too small to draw any conclusions, but the question that this type of crime raises is if distant live-streamed abuse is a substitute for sex tourism. According to colleagues in other countries this does not seem to be the case. Consumption of live-streamed child sexual abuse rather seems to further the addiction and fuel a desire to travel to participate in hands-on abuse.

A lot of investigative challenges
This type of crime presents a long list of challenges. The biggest challenge is to detect the offence and the offenders in the first place. It is difficult to establish whether payment for a show has been for an adult sex show or for abuse of children.

Working across borders is difficult – people are not registered in the same way everywhere, and in order to interview a child one needs to make a request for international assistance, which can be a lengthy procedure. It can also be difficult to get information from platform providers in other countries. There is also the fact that these types of cases contain enormous amounts of material made up of lists of calls, chat logs, screenshots and evidence of payment, which all need to be investigated and matched.

“ In all our cases, offenders have been in possession of other types of child sexual abuse material.

4 How child sexual abuse material is stored

– Laptops, mobile phones and USB sticks are the most common storage spaces.
– Storage on mobile phones shows the biggest increase.
– There is both known and unknown material in most investigations.

To understand how to find and tackle child sexual abuse material it is important to understand how it is stored and collected, and if the methods for storing material is changing with developing technologies.

LAPTOPS, MOBILE PHONES AND USB STICKS ARE THE MOST COMMON STORAGE SPACES

Pretty much all possible storage devices are commonly used to store child sexual abuse material, according to the surveyed police officers. Nearly half of the respondents answered that they come across child sexual abuse material on almost all storage spaces.

Physical devices

More than nine in ten of the surveyed police officers answered that they find child sexual abuse on computers, laptops and mobile phones. Nearly as many answered USB sticks or other portable devices. This makes computers/laptops, mobile phones and USB sticks the most common storage devices that child sexual abuse is found on in police investigations. When not only asked what they find, but also what is most common, these three types of storage were also clearly rated as the most common by the surveyed police officers.

> " Computers/Laptops, Mobile Phones, USB or other portable devices."

> " Portable devices become more common if the computers or laptops are shared."

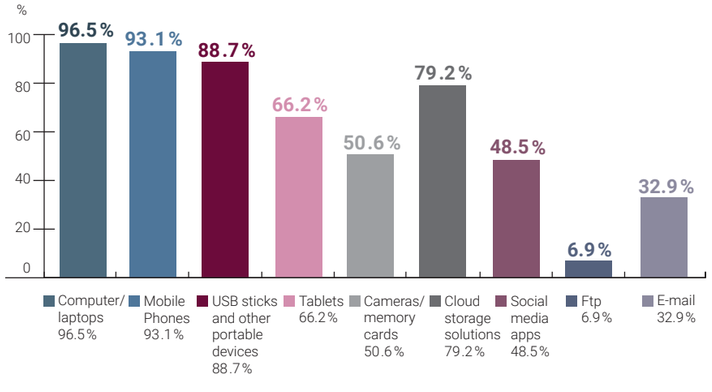
> " I wouldn't put much space between these - I think mobile is really on the rise, but USB devices that can go from mobile devices to PC/Mac as well."

More than one in six also answered that they find child sexual abuse material on tablets and half of the respondents answered that they find it on cameras and memory cards.

Online storage

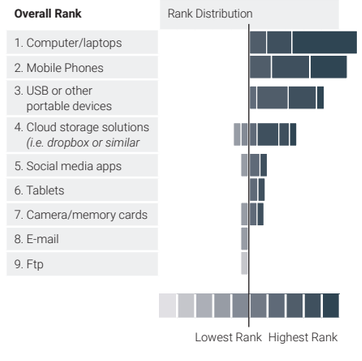
Eight in ten respondents answered that they find child sexual abuse material on cloud storage solutions, which makes cloud storage nearly as common as USB sticks and other portable devices. This was also rated as the fourth most common type of storage space by the surveyed police officers.

DEVICES AND OTHER STORAGE SPACES THAT ARE USED TO STORE CHILD SEXUAL ABUSE MATERIAL



The respondents were able to tick several answers.

DEVICES AND OTHER STORAGE SPACES, THAT ARE USED TO STORE CHILD SEXUAL ABUSE MATERIAL, THAT POLICE OFFICERS RATE AS MOST COMMON



Respondents were asked to grade the three most common storage spaces that they come across.

> " Cloud storage seems to be coming more prevalent with offenders sharing links to cloud storage, rather than risk sending / receiving images."

> " Most cases the offender has imagery stored on computer related device. However more often larger quantities of images are stored within the cloud. This makes it difficult to trace."

Half of the surveyed police officers answered that they find child sexual abuse material on social media apps. One third answered that they also find it stored in e-mails.

STORAGE ON MOBILE PHONES SHOWS THE BIGGEST INCREASE

More than eight in ten of the surveyed police officers answered that storage on different types of devices has increased in the last three years.

When asked which devices have increased, one third answered storage on mobile phones. One fifth answered that computers and laptops, cloud storage, and USB sticks and external hard drives have increased.

> " Phones and cloud storage have both increased significantly."

> " Computer hard drives and portable storage devices."

> " Cloud based trading. Offenders commonly use chat programs to share links where there are buckets and buckets of illegal materials in the folders."

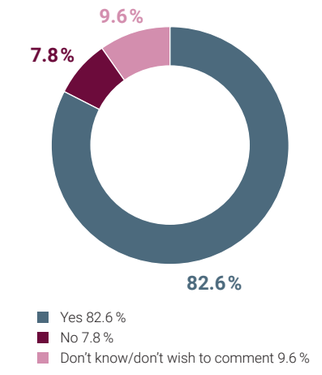
Nearly sixteen percent answered that it is the increase in storage capacity on all types of devices, such as larger hard drives, that has driven the increase in different types of storage spaces.

> " Pretty much every type of device has increased its storage size."

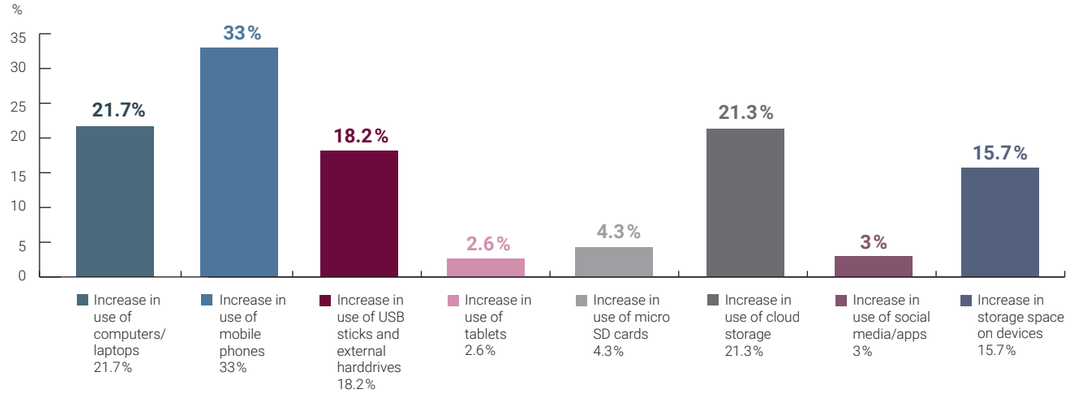
> " Storage capacity in all devices has increased."

>>

WHETHER THERE HAS BEEN AN INCREASE IN TYPES OF DEVICES / STORAGE SPACES TO STORE CHILD SEXUAL ABUSE MATERIAL OVER THE PAST THREE YEARS?



INCREASE IN TYPE OF DEVICE OR STORAGE SPACE, USED TO STORE CHILD SEXUAL ABUSE MATERIAL, OVER THE PAST THREE YEARS



The respondents answered an open question and could provide many different answers.

4 HOW CHILD SEXUAL ABUSE MATERIAL IS STORED

>> THERE IS BOTH KNOWN AND UNKNOWN MATERIAL IN MOST INVESTIGATIONS

The police officers were also asked to quantify how much material is known and already classified as child sexual abuse when they start on a case. This is important for many different reasons. One is to understand how much old material is in circulation, and to know how much new material is produced. Another reason is to understand the caseloads that law enforcement professionals are dealing with, and the amount of work that they have to undertake when analysing child sexual abuse cases.

The respondents were asked to first report how much material was already known in their latest case. If they did not know this, they were asked to estimate their "average" case. Sixty-four percent of the respondents answered the first question, thirty-six percent answered the second.

Latest case

There is a fairly even spread in the answers to how much material was already known or classified from the start of the police officers' latest investigations.

Four in ten of the respondents answered that *more* than fifty percent of their latest case consisted of already known material. One in twenty answered that as much as hundred percent of their latest case consisted of known material, and nearly one in ten said that more than ninety percent was already known. In contrast, nearly six in ten answered that *less* than fifty percent of their latest case consisted of already known material. Nearly one in ten said that their latest case contained no previously known material at all, and one in ten said that only up to ten percent was known before.

Average case

Of the respondents who estimated their average case, half reported that fifty percent or more of their cases normally contain already known material, whereas the other half reported that their average case usually has less than fifty percent known material.

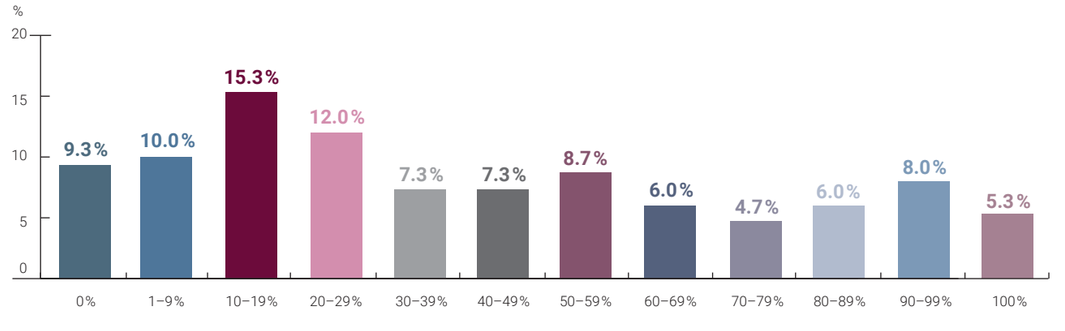
No clear trend

The numbers don't present a clear trend of how much material is generally unknown or known in a case. This indicates that there is both a lot of known material in circulation, but also that a lot of new material is being produced.

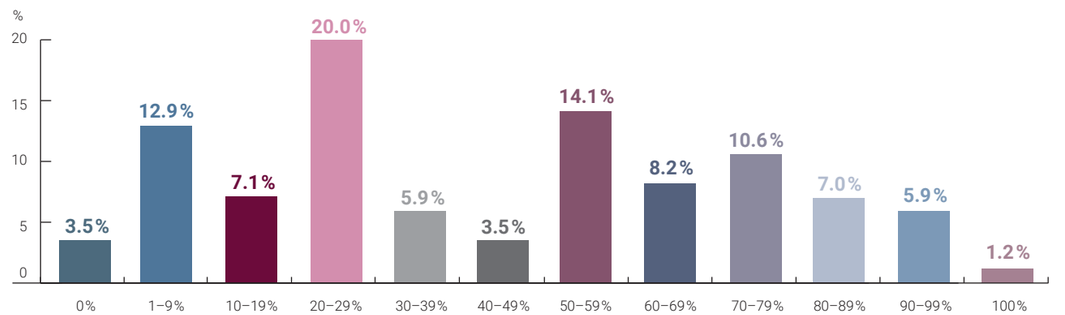
In nearly all cases there is unclassified, previously unseen child sexual abuse material, and in many these unknown images and videos are a large share of the case. These images do not only need to be classified for the future, they are also important in the work to identify and safeguard child victims.

Simultaneously, the numbers show that in many cases a large share of the images and videos are already known, pointing to the help law enforcement can get from being able to filter images out so that they do not have to look through all the material.

SHARE OF CHILD SEXUAL ABUSE IMAGES AND VIDEOS THAT WERE ALREADY KNOWN/CLASSIFIED IN THE RESPONDENTS LATEST CASE



SHARE OF CHILD SEXUAL ABUSE IMAGES AND VIDEOS THAT WERE ALREADY KNOWN/CLASSIFIED IN THE RESPONDENTS AVERAGE CASE (IF THEY WERE UNABLE TO SPECIFY THEIR LATEST CASE)



5 Apps and platforms are used to store and distribute child sexual abuse material

– Skype is the most common platform for live-streamed child sexual abuse.
– Dropbox and Google services are frequently used to store and share child sexual abuse material.
– Snapchat, Facebook and Kik are commonly mentioned social media platforms.

In a number of different questions, the police officers were asked which apps and online services are used to store and distribute child sexual abuse material. In the case of live-streaming the services are used to distribute the abuse itself rather than the material.

SKYPE IS THE MOST COMMON PLATFORM FOR LIVE-STREAMED CHILD SEXUAL ABUSE

The surveyed police officers were asked which applications, services or technologies they come across in their investigations of live-streamed child sexual abuse. They mentioned a wide range of social media platforms and chat apps with live-streaming technology, video call apps and video meeting services, live video apps, web-based chat apps and chat apps for gamers. In total sixty-four different apps, platforms and services were mentioned by name.

The most commonly mentioned apps/platforms were Skype followed by Snapchat, Facebook, Kik and Omegle. WhatsApp, TikTok, LiveMe, Instagram, Zoom and Periscope were also frequently mentioned.

" Skype is by far the biggest one. There is no protection on that platform. Contact is usually made on some other social media platform such as Facebook, Instagram, KIK, MYLOL, etc ... but then moved to Skype to record the video stream."

" Skype is the predominant platform used. Also used is KIK and Snapchat etc."

" Any of the hundreds of private chat sites like ooVoo and Zoom. These private chat apps are exploding in use."

" Omegle, LiveMe, TikTok."

" Kik, Instagram, WhatsApp, Discord, Snapchat, Facebook Messenger."

The results show that all possible platforms are used for live-streamed child sexual abuse, and that it is a problem for all platform providers. It may also indicate that the bigger the platform, and the more users, the bigger the problem.

DROPBOX AND GOOGLE SERVICES ARE FREQUENTLY USED TO STORE AND SHARE CHILD SEXUAL ABUSE MATERIAL

The police officers were asked which cloud storage services they come across in their investigations into child sexual abuse material. Forty different services were mentioned in total. The large majority of respondents, eight in ten, answered that they come across child sexual abuse files stored on Dropbox. Nearly half mentioned Google Drive or Google Photos, one quarter mentioned Mega and one quarter mentioned OneDrive.

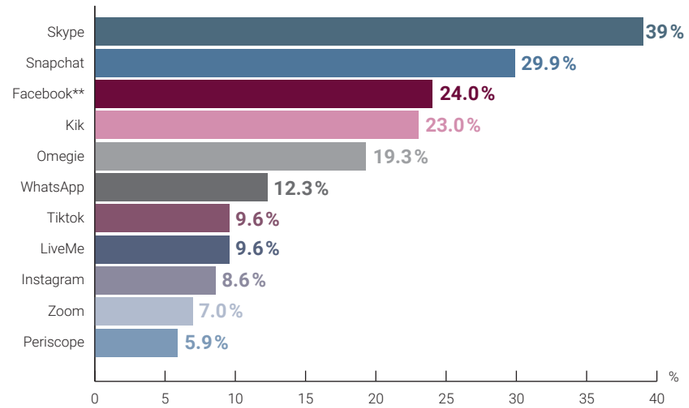
" Dropbox has become the main cloud storage app we have been finding."

" iCloud and Google drive are the most common."

" Dropbox, iCloud, MEGA, Google Drive."

" Dropbox and Google Drive; However both of these cloud servers have sent us CyberTips whenever hash values are matched."

MOST FREQUENTLY MENTIONED APPS, PLATFORMS AND TECHNOLOGIES, THAT POLICE OFFICERS REPORTED SEEING IN THEIR INVESTIGATIONS OF LIVE-STREAMED CHILD SEXUAL ABUSE. SHARE OF RESPONDENTS THAT NAMED THE SPECIFIC APP/PLATFORM*



** Other apps mentioned several times were Facetime, Yahoo Messenger, Twitter, Youtube, Discord, Oovoo, Wickr, Stickam, Younow, Viber, Chatroulette, Chaturbate, ChatAvenue/KidsChat and Chatstep.*

*** (incl. Facebook messenger and Facebook Live)*

The respondents answered an open question and could provide many different answers.

SNAPCHAT, FACEBOOK AND KIK ARE COMMONLY MENTIONED SOCIAL MEDIA PLATFORMS

The police officers were asked which social media platforms and chat apps they come across in their investigations into child sexual abuse material. Forty-nine different platforms and apps were mentioned in total. Half of the respondents mentioned Snapchat, Facebook and Kik. A third of the respondents mentioned Instagram and WhatsApp.

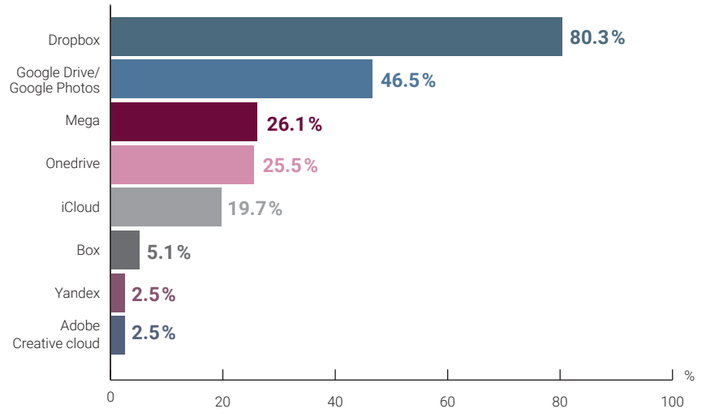
" SnapChat predominantly, also Kik, WhatsApp, Hangouts, HeyNow."

" Kik, Snapchat, Instagram, Facebook."

" Kik, Snapchat, WeMe ... pretty much any video/chat app."

" Facebook, Instagram, Snapchat."

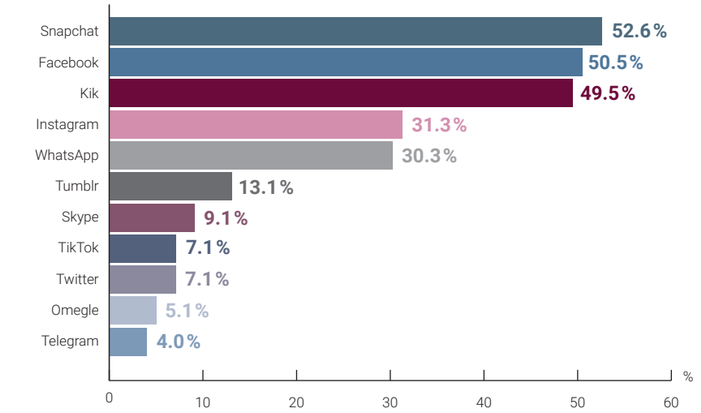
MOST FREQUENTLY MENTIONED CLOUD STORAGE SERVICES, THAT THE POLICE OFFICERS REPORTED SEEING IN THEIR INVESTIGATIONS OF CHILD SEXUAL ABUSE MATERIAL. SHARE OF RESPONDENTS THAT NAMED THE SPECIFIC CLOUDSTORAGE SERVICE*



Other services mentioned several times include Flickr, Amazon Cloud, SkyDrive, Imgsrc, File.io, DropFile, pCloud, DL-Free and a number of other cloud storage solutions provided by operators.

The respondents answered an open question and could provide many different answers.

MOST FREQUENTLY MENTIONED SOCIAL MEDIA PLATFORMS AND CHAT APPS, THAT THE POLICE OFFICERS REPORTED SEEING IN THEIR INVESTIGATIONS OF CHILD SEXUAL ABUSE MATERIAL. SHARE OF RESPONDENTS THAT NAMED THE SPECIFIC SOCIAL MEDIA PLATFORM OR CHAT APP*



** Other services mentioned several times include Reddit, Discord, LiveMe, MeWe, Mega, VK, WeChat, Chatstep and Mylol.*

The respondents answered an open question and could provide many different answers.

THE PROACTIVE PLATFORMS

It is important to note, that being among the most commonly mentioned apps or platforms does not automatically mean that they have the biggest share of the crime. In some cases the platforms that do most proactive work on this issue and report found material to law enforcement, show up more in investigations. The results should therefore be seen to indicate that the mentioned platforms are commonly used for child sexual abuse crimes. However, the results should not be seen as an indication that the platforms that are not mentioned are not used to share/stream child sexual abuse material.

ERIC OLDENBURG
Law Enforcement Liaison, North America, Griffeye

EASY PRODUCTION AND SHARING DRIVES THE SPREAD OF CHILD SEXUAL ABUSE MATERIAL

Child sexual abuse material is today stored on all possible devices and shared in all sorts of fora on the internet. The nature of sharing information follows the development of technology which throws up new challenges for law enforcement.

The ease of sharing links

Online storage, like cloud storage, presents a different challenge to law enforcement than physical devices do. Sharing a large collection of files on a hard drive, or sharing all images on a phone requires a lot of effort and is difficult to do. Cloud storage, however, makes it possible to share an entire mass of material by just sharing a link on a forum, social media platform or through direct messaging. Duplicates of millions of images can reach more people much quicker than they ever could before. I believe this ease of access and facility to quickly share material is one of the main drivers behind the sharp increase in the spread of child sexual abuse material.

Slower and more complicated investigations

Cloud storage has also made investigations slower and more complicated. With material on hardware the police can seize and get immediate access to a computer or USB stick. Working to gather information from cloud storage demands that law enforcement identify where the material is located in the world, get a search warrant for that place, and wait for the platform provider to respond and deliver the data in a safe way. This causes delays that makes it more difficult to safeguard victims in a timely manner.

Mobile phones

Mobile phones and mobile apps are other examples of ease of access driving the spread, and also production, of child sexual abuse material. Nearly everyone has a mobile phone, and they are cheap, have good cameras, and feel very private and secure as people always carry them with themselves. Using mobile apps it is also very easy for offenders to access collections of material.

I believe that the increasing numbers of mobile phones seen in investigations is also linked to the increase in self-produced material by children and teenagers themselves. Whether they produce material voluntarily or as a result of grooming or extortion, they typically use their mobile phone.

Known images vary depending on investigation

The quantity of child sexual abuse material known at the beginning of an investigation varies widely depending on the type of investigation. For example, on a peer to peer undercover investigation most images and videos will probably be known. On the other hand, in a self-production case, most images will probably be new. Overall though, my experience is that known files typically outweigh new material.

The number of known images at the beginning of an investigation is also entirely dependent on the intelligence and databases of known hashes that each law enforcement professional has access to. That is why it is so important to collaborate and share intelligence. The consequence of not sharing is that law enforcement professionals risk duplicating the efforts of others and wasting time that could be used to identify victims.

This is also important to address from a mental health point of view. Working on child sexual abuse investigations, constantly exposed to child sexual abuse material, is psychologically very difficult. Being able to filter out already known material not only reduces risk of duplicating work, it also reduces exposure and trauma. The less time law enforcement professionals spend looking at unnecessary child sexual abuse material, the longer they will have the mental strength to keep doing the job.

“I believe this ease of access and facility to quickly share material is one of the main drivers behind the sharp increase in the spread of child sexual abuse material.

6 Emerging technologies – trends, challenges and opportunities

– Increase in use of cloud storage, encryption and smartphones.
– Encryption is the biggest challenge.
– Artificial Intelligence, investigation software, and sharing of data/intelligence is most helpful.
– One in five police officers have used AI tools in their investigations.

INCREASE IN USE OF CLOUD STORAGE, ENCRYPTION AND SMARTPHONES

The police officers reported that major technology trends that affect methods for production, storage and distribution of child sexual abuse material are increased use of cloud storage, encryption of a range of devices and online storage spaces, and the development and spread of smartphones.

An increase in use of cloud storage was mentioned by more than one third of the surveyed police officers.

Increases in encryption and smartphones were mentioned by one fifth of the respondents. This includes encryption of apps, mobile phones and computers as well as encryption of cloud services.

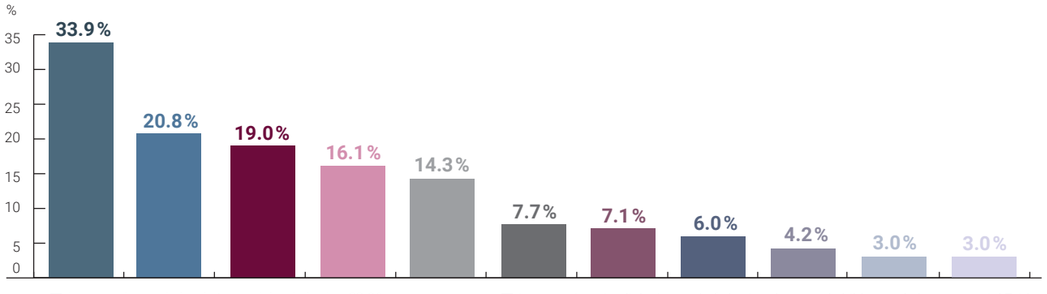
Darknet, social media and online gaming

More than one in ten respondents answered that increased use of TOR/darknet (16.1 %), and social media and online gaming (14.3 %) being used to produce and share child sexual abuse material are major trends.

Apps, link sharing and P2P

Other trends mentioned were development of mobile applications, and an increase in offenders sharing links to online spaces (often cloud storage) or websites where child sexual abuse material can be downloaded, rather than sharing the material itself directly. Increased use of P2P networks was also mentioned.

MOST FREQUENTLY MENTIONED EMERGING TREND IN TECHNOLOGIES THAT ARE USED TO PRODUCE, STORE AND DISTRIBUTE CHILD SEXUAL ABUSE MATERIAL*



** Other trends mentioned several times include the use of virtual machines, NAS Networks, self-produced child sexual abuse material, deepfakes, organised forums, and forensically cleaned devices.*

The respondents answered an open question and could provide many different answers.

“ Use of cloud storage appears to be increasing year on year with offenders storing and sharing links. Devices are often forensically cleaned making detecting offences more difficult.”

“ Distribution of links which lead to cloud storage accounts containing child sexual abuse material.”

“ Cloud storage is quickly going to overtake mobile phone storage (if it hasn't already). Every case seems to have a Dropbox, Drive, or Mega connection to it.”

“ The use of cellular devices to store and distribute child sexual abuse material across a myriad of Apps and the storage of that material in third party cloud storage companies.”

“ Apps that allow covert and encrypted communication between offenders and children.”

“ Live-streaming, being recorded using DU recorder or ITube. Then shared via encrypted chat plaforms like WhatsApp and Telegram between offenders. Still large use of Dropbox links being shared on chat groups.”

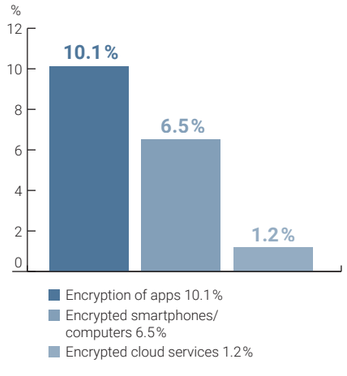
“ Cellular/mobile devices and tablets/laptops are loaded with encryption by default which makes processing the device as well as their backups increasingly difficult.”

“ Devices that automatically encrypt data. Devices that auto-lock down and require passcodes to gain entry, such as smartphones. Apps that have "My Eyes Only" type secure vaults to hide content, such as what Snapchat uses.”

“ Production is made easy by the use of smartphones and distribution is, in my experience, made easy by the use of TOR.”

“ Cloud sharing. Perpetrators are locating victims through gaming apps a lot more these days.”

BREAKDOWN OF THE TYPES OF ENCRYPTION SPECIFICALLY MENTIONED IN THE SURVEY



>>

6 EMERGING TECHNOLOGIES – TRENDS, CHALLENGES AND OPPORTUNITIES

ENCRYPTION IS THE BIGGEST CHALLENGE

Nearly half of the surveyed police officers reported that encryption is the biggest challenge they face in child sexual abuse investigations. Fourteen percent (14.4 %) of the respondents specifically answered that encrypted and locked smartphones and computers are particularly challenging.

Darknet and cloud storage

Nearly one fifth of the respondents mentioned TOR/darknet and cloud storage as technologies that are particularly challenging. In relation to cloud storage, several respondents specified that the major challenge is jurisdictional issues, for example when the cloud host is based in another country. Other challenges mentioned were live-streaming and apps that don't store content, VPN, ISPs that don't track IP addresses and store information, and apps with user anonymity.

> "The problems associated with storage on international servers and the legal challenges associated with that. Also, I have seen a lot of sharing via anonymous file sharing websites, especially on the 'dark web'."

> "The standard use of hardware encryption on smartphones and computers."

> "Encryption/password protection Apps that store very little data on the device i.e. Snapchat."

> "VPN services are a particular challenge as they mask the true location where someone is accessing data from."

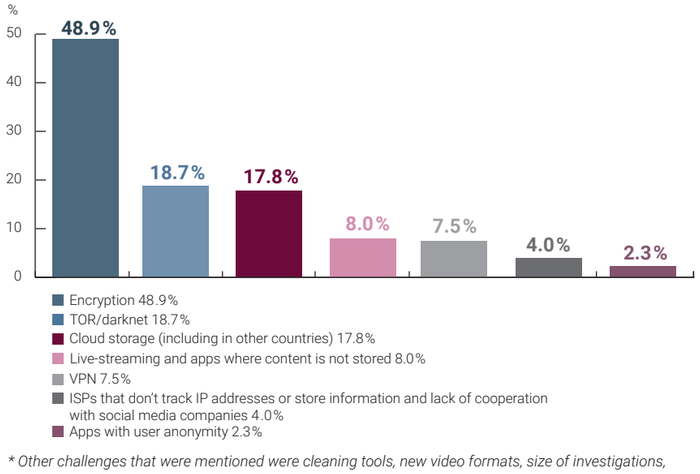
> "The vast amount of programs that enable a user to show live videos and keep no records has allowed offenders a larger group of children to groom and exploit."

> "The biggest hurdle outside of encryption are ISPs which do not retain the needed data to identify subscribers. Many cellular providers do not maintain records of session and login activity. Those that do may only keep them for 60–90 days, which is often outside the range of the abuse when reported."

> "That is the co-op with the social media platforms. They are not that willing to help the police, and that is a big problem. Use things like letters rogatory/MLAT*, and that result in months and months of waiting, and then the evidence is gone."

> "The biggest challenge is that the use of the DarkNet is constantly rising and that using mobile applications makes it harder for us to track and search for these kind of material."

TECHNOLOGY DEVELOPMENTS THAT POLICE OFFICERS SEE AS PARTICULARLY CHALLENGING TO CHILD SEXUAL ABUSE INVESTIGATIONS. SHARE OF RESPONDENTS THAT HAVE ANSWERED A SPECIFIC CHALLENGE*



** Other challenges that were mentioned were cleaning tools, new video formats, size of investigations, increasingly tech savvy suspects, virtual machines.*

The respondents answered an open question and could provide many different answers.

** MLAT stands for Mutual Legal Assistance Treaties. Letters rogatory and MLAT are treaty-based mechanisms for seeking foreign law enforcement cooperation. See comment by Jim Cole at end of insight 6 for further explanation.*

ARTIFICIAL INTELLIGENCE, INVESTIGATION SOFTWARE, AND SHARING OF DATA/INTELLIGENCE IS MOST HELPFUL

Artificial Intelligence

Half of the surveyed police officers answered that different types of technology developments, such as Artificial Intelligence (AI), Face Recognition, PhotoDNA[1] for video and forensic tools for breaking locked smartphones are most helpful to child sexual abuse investigations. Most of those, one fifth of the respondents, answered that AI is helpful.

> "AI for image detection."

> "Facial recognition, AI."

Software and sharing data/intelligence

One third of the respondents named specific software for investigative work and analysis. One quarter mentioned the importance of sharing data and growing different intelligence sources like databases of hashes, and work done by NCMEC[2], Project VIC[3] or CAID[4].

> "Continued growth of MD5[5] hash sets of known material. More importantly the growth of PhotoDNA of Known Images. Most important the use of Photo DNA on movies so that non matching MD5 values on movies can be addressed."

> "Hash databases that are contributed globally."

> "NCMEC/CVIP[6] are very helpful."

> "CAID/Project VIC."

Platform and service providers

One in ten answered that it would be helpful if ISPs and social media platforms collaborated more with law enforcement. Just over three percent of the surveyed police officers said that they were helped by just that, improved help from social media companies.

> "Online storage and businesses that monitor online storage for known hashes."

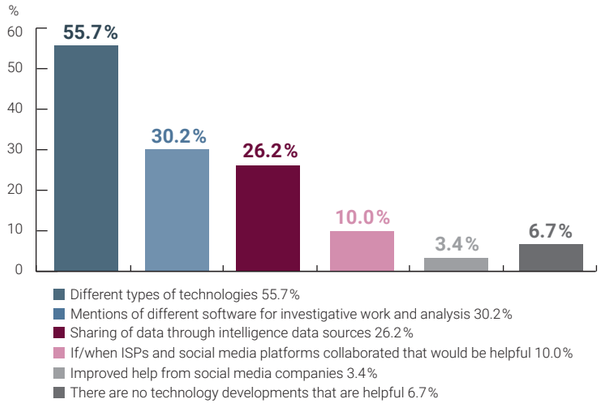
> "The implementation of any tools used by any ISP/ESP that recognizes child exploitation from the get go and is then reported to the appropriate jurisdiction."

> "Constant cooperation between law enforcement and internet service providers."

No helpful developments

Nearly seven percent of the respondents said that they didn't feel that there were any technological developments that are helpful to child sexual abuse investigations.

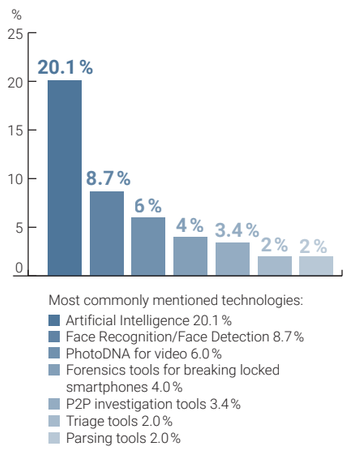
TECHNOLOGY DEVELOPMENTS THAT POLICE OFFICERS SEE AS PARTICULARLY HELPFUL TO CHILD SEXUAL ABUSE INVESTIGATIONS. SHARE OF RESPONDENTS THAT HAVE ANSWERED A SPECIFIC TECHNOLOGY THAT IS HELPFUL*



** Other helpful technologies mentioned included text recognition, location services in apps, decryption tools, cybertips from platform and online storage providers, and more possibilities to use online undercover investigations.*

The respondents answered an open question and could provide many different answers.

BREAKDOWN OF TECHNOLOGIES LISTED AS HELPFUL IN THE SURVEY



[1] *PhotoDNA is robust hashing technology used to identify child sexual abuse material. See section three of the report for a description of PhotoDNA.*

[2] *NCMEC (National Center for Missing and Exploited Children) is the US' national clearing house for reports on child sexual abuse material for US based platform providers*

[3] *Project VIC is a global partnership between law enforcement and the private sector. It promotes data sharing between domestic and international law enforcement agencies working on cases pertaining to sexual exploitation of children.*

[4] *CAID (Child Abuse Image Database) is a national system to enable collaboration between law enforcement agencies working on child sexual abuse cases in the UK.*

[5] *MD5 is a type of binary hash. Read more about binary hashing in section three of this report.*

[6] *CVIP (National Child Victim Identification Program) is a database of child sexual abuse material maintained by the United States Department of Justice and NCMEC.*

6 EMERGING TECHNOLOGIES – TRENDS, CHALLENGES AND OPPORTUNITIES

>> **ONE IN FIVE POLICE OFFICERS HAVE USED AI TOOLS IN THEIR INVESTIGATIONS**

One fifth of the surveyed police officers answered that AI is helpful in child sexual abuse investigations. This number is also reflected in how many of the respondents reported having used AI in their investigations. The large majority, nearly eight in ten of the surveyed police officers, however answered that they have not used AI in their investigations. Several respondents commented that they would like to.

" I would like too but haven't taken the time to learn the technique."

" Would love to try AI in my cases."

Triage and locate material

Of the respondents that used AI classifiers in their investigations, eight in ten reported that they were useful.

The majority of those (46.2 %) reported that the primary gain is that the AI classifier helps to triage or filter material, to locate where to look in the caseload or highlight material that is likely to be child sexual abuse material.

" Due to the immense amount of digital evidence, the use of AI […] allows examiners to target potential images first. This provides both a benefit in efficiency as well as a mental boost because it allows the user to sort out the most likely media files first."

" Everything identified by AI still has to be manually reviewed however pre-categorization of child abuse images or vetting of known system files speeds processing time greatly.

" The image classifiers can surface potential child pornography images more quickly."

" It can be used as a triage tool to decide if a device needs to be deeper examined or not."

Needs to mature

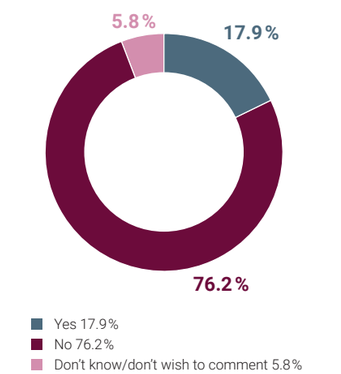
Those who reported that AI technologies are not useful, commented that the technology still needs to mature, but will be beneficial in the future, or that they had just started using it and needed to get more experience.

" Technology doesn't seem mature enough yet....Getting better but still a way to go."

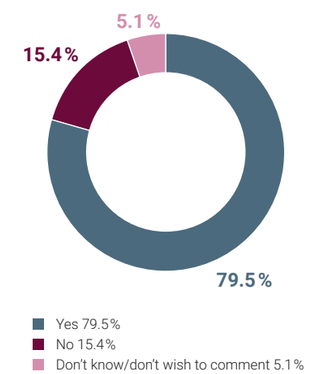
" Will be more beneficial as the technology develops."

" I have only barely started trying to apply AI/machine learning in my cases but I'm excited to find ways to make it useful."

SHARE OF RESPONDENTS WHO HAVE USED ARTIFICIAL INTELLIGENCE TECHNOLOGY/ CLASSIFIERS IN THEIR INVESTIGATIONS



WHETHER RESPONDENTS WHO HAVE USED ARTIFICIAL INTELLIGENCE TECHNOLOGY/ CLASSIFIERS IN THEIR INVESTIGATIONS FIND IT USEFUL



JIM COLE
Supervisory Special Agent, Homeland Security Investigations (USA),
Special Agent in Charge Nashville, TN

ARTIFICIAL INTELLIGENCE WILL BE A MAJOR GAME CHANGER

The technological development that is having the single most impact on child sexual abuse investigations is Artificial Intelligence (AI). I have used AI for many years now and in the past two or three years there have been some incredible developments.

The future of AI

The future of AI is exciting, and we are still only in the beginning of where AI can take us, but it is clear that visual analytics will change beyond our imagination.

An example of current really interesting work is a research project that aims to marry the human brain's neural networks with AI neural networks. The human brain has an amazing capability to understand context, something machines are terrible at. In this project images are shown to a person (police officer) at a faster pace than the brain can cognitively register. The brain still reacts to the content of the image, and violent content elicits a heightened stimulus. By reading a brain's EEG, AI can use those reactions to group images together. In the future this could be used during the first sift through of case data, to help law enforcement go through material faster.

There is also work on AI being used for text analysis to detect certain text sequences in chats and messaging apps to push content for review. That could be used in both child sexual exploitation and terrorism investigations.

Another future use is resource intensive undercover operations where a detective chats with suspects. With some human monitoring, that could probably be AI driven instead. Or when doing a house search, images from the premises could automatically be matched to see if the location matches unsolved child sexual abuse series that we have.

These are just some examples; I think that we will see AI move into areas that we are far from contemplating now.

Investigative leads

We are still some way from the future I've painted above, but AI can already be very useful. It is already a good indicator and provider of investigative leads.

Instead of just looking at a vast pool of data in a case, image classifiers can help us group together images with visual similarity and highlight images that might be of particular interest. This makes the data both easier and faster to review, making investigations more efficient.

Expectations vs capability

The challenges that we face with AI right now, is the general poor knowledge level and people's expectations of it. In the general police community there is a lack of understanding of how AI works, and how the algorithms "learn" and there is a tendency for investigators to rely too heavily on the result from the computer.

As a result, expectations are exceeding the capabilities of the technology. There is a belief that AI classifiers will find all child sexual abuse material in a case, and that it will find everything correctly – which it doesn't. It is not a result that can be trusted without review or that can be used in court, it still needs to be manually validated and investigated.

Therefore, we need to make sure that we train people in the police community to understand the strengths and limitations of AI, so that they use its potential efficiently and correctly.

Automate manual work

I don't think there will be a time during my career nor lifetime where we can blindly rely on computers and algorithms. However, in the not too distant future we might be able to automate up to ninety percent of what we today are doing manually. This will cut down on the time and resources that we have to spend reviewing images and will free up time for people to work on more new cases.

JIM COLE
Supervisory Special Agent, Homeland Security Investigations (USA),
Special Agent in Charge Nashville, TN

ACCESSIBILITY TO TECHNOLOGIES HAS CHANGED THE PLAYING FIELD

The results in this report mirrors my own understanding of the situation. The technologies mentioned are not new, but what has really changed over the past years is the accessibility to, for example, encryption and cloud storage.

Built in encryption
Previously only used by people with thorough technological know-how, encryption is now everywhere, in apps and devices, and as with everything this presents both positives and negatives. In order to protect privacy and data, encryption is a good thing, however it also facilitates crime that uses digital technology, not only child sexual exploitation, but also financial crime, narcotics and terrorism.

In the past we could submit devices to mobile phone manufacturers, like Apple, to access data on phones. Apple have now moved to a system where they cannot decrypt the phones that they produce even if they wanted to. And we are seeing more companies following suit – Facebook, for example, has announced that they will deep encrypt Facebook Messenger. This is a major challenge to child sexual exploitation investigations.

Automatic cloud storage
Similarly, in the past cloud storage had to be actively sought out as an add-on. Now every device comes with automatic and easily accessible cloud storage, and there are several challenges to this. The first is that we don't get access to cloud storage when we execute a residential search warrant. For that we need a second search warrant and another court process, which delays access.

Another issue is legal challenges to accessing data stored outside of US borders. An example of this is when Kik was based in Canada. We could get subscriber information by drafting a US subpoena and going through the Royal Canadian Mounted Police. However, to get communications or images from an account, we needed a Canadian search warrant. To get this, we would need to go through letters rogatory/MLAT (Mutual Legal Assistance Treaties) which is an incredibly long and drawn out process. This process could at best take nine months, but often up to three years. After that long the information is often gone, or the MLAT is rejected because legal requirements have changed during that time. It ends up being a futile waste of time and effort.

Darknet is the biggest challenge
I think one of the biggest challenges is still darknet and TOR, where child sexual abuse crime still goes largely undetected. Methods on darknet and encrypted communication means offenders can establish a type of trust. This was previously difficult to do, and it gives offenders opportunity to engage in really extreme behaviour.

Even though many police officers are aware of the problems with darknet, few are investigating it. One reason is that most law enforcement agencies around the world are only tasked to work on cases that fall within their own jurisdiction. It is often not possible to determine who's operating on the darknet or where they are, and this produces a problem for traditional police work.

This is the conundrum that we are dealing with – technology is making our jobs more difficult and informing us at the same time. The law enforcement community needs to adopt to these challenges, and we need to be willing to try to learn new technology. We have to be willing to work cases that may not be in our own jurisdictions. We have to work better together, and we have to be willing to do things differently to what we have done before.

“ This is the conundrum that we are dealing with – technology is making our jobs more difficult and informing us at the same time.

Protecting business IT environments against child sexual abuse material – Use of policies, action plans and technologies

Following up on child sexual abuse material in the business environment

In last year's NetClean Report (2018) we interviewed businesses and organisations that have NetClean ProActive (software that detects child sexual abuse material in organisations' IT environments) installed on their computers and in their IT environments. The results showed that 1 in 500 employees use their work computer to view child sexual abuse material, often on a laptop, outside of business hours and using USB sticks.

This year we surveyed large corporations from a more general selection, not only NetClean's own customers, to see how businesses respond to the problem of child sexual abuse material in their IT systems. We surveyed one hundred businesses with 5,000 employees or more, all operating in the US. The respondents were IT/IT Security professionals that are either the primary decision maker in their company, or share equally in the decision-making with others. The survey was conducted as an anonymous online web interview.

This section of the report looks at the following four areas:

Whether the businesses have a corporate policy in place that states that it is prohibited to handle child sexual abuse material within the company's IT environment or on company devices.

Whether the businesses have an action plan in place to deploy if child sexual abuse material is found in the organisation's IT environment.

Whether the businesses have technologies in place to detect or block child sexual abuse material in the business IT environment.

Whether child sexual abuse material have ever been found in the businesses' IT environments.

7 Businesses' use of policies and action plans to protect their IT environment from child sexual abuse material

– Nine in ten businesses have a corporate policy in place.
– Eight in ten businesses have an action plan in place.

NINE IN TEN BUSINESSES HAVE A CORPORATE POLICY IN PLACE

Company policies are important frameworks for businesses as they define core values and strengthen company culture. They are designed to define and reinforce acceptable and unacceptable behaviour and conduct in the workplace, and the standards that employees are expected to meet. They also give an organisation leverage to act, providing opportunity to terminate employment where serious policy breaches have occurred.

Nine in ten of the surveyed businesses reported that they have a company policy in place that states that it is prohibited to handle child sexual abuse material in the company's IT environment or on company devices.

Nearly one in ten companies reported that they do not have such a policy in place.

EIGHT IN TEN BUSINESSES HAVE AN ACTION PLAN IN PLACE

A plan of action outlines a procedure to follow if child sexual abuse material is found in the business IT environment. It provides the organisation with a framework for steps to take and actions to be executed, to ensure that the situation is handled in a way that the company considers most correct.

Eight in ten businesses reported that they have an action plan in place to deploy if child sexual abuse material is found in the business IT environment.

More than one in ten businesses stated that they do not have an action plan of this sort in place.

Notification of law enforcement and internal reporting are most common actions

When the respondents were asked to describe the action plan, notification of law enforcement, internal reporting, securing of evidence and suspension and/or termination of employment were mentioned most frequently.

Notification to law enforcement

Nearly half of the total number of respondents (60 percent of those who have an action plan in place) reported that their action plan prescribes notifying law enforcement.

" After the discovery we immediately include the authorities and collaborate with the investigation."

" We contact the correct authorities immediately."

" All the data that we find are immediately sent to the authorities."

" Report to police and ensure we keep the evidence."

Internal notification

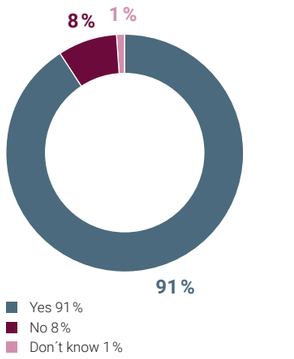
One third of the surveyed businesses reported that they notify someone internally, most commonly this was HR (nearly one in five), but it could also be the Executive Team, Head of Department, Local IT department or other.

" We immediately have human resources respond."

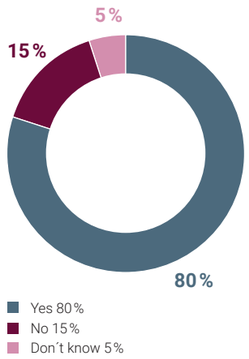
" It is reported to HR and CTO."

" Manager escalates to Department Head, Department Head alerts Human Resources, HR informs me and CIO to engage background check."

SHARE OF BUSINESSES THAT REPORT HAVING A CORPORATE POLICY IN PLACE THAT STATES THAT IT IS PROHIBITED TO HANDLE CHILD SEXUAL ABUSE MATERIAL WITHIN THE COMPANY'S IT ENVIRONMENT OR ON COMPANY DEVICES



SHARE OF BUSINESSES THAT REPORT HAVING AN ACTION PLAN IN PLACE TO DEPLOY IF CHILD SEXUAL ABUSE MATERIAL IS FOUND IN THE ORGANISATION'S IT ENVIRONMENT



One in twenty of the surveyed businesses reported that their action plan includes notification of the employees' supervisor or manager.

" If they somehow get around the filter we notify their manager."

" IT Staff tips off HR and Manager."

" IT Group notifies executive team, CHRO is contacted. Supervisor of employee is contacted."

Action to secure evidence

One in five of the businesses stated that their action plan includes instructions to secure evidence.

" We would isolate the equipment immediately and remove it from the network. We would then call in an incident response team to investigate."

" We immediately freeze the user account and do a 48-hour investigation."

" Ensure proof of violation, see how they were able to get around the filter, and report it."

" Record the dates, times and facts of the incident, report to HR, and authorities."

Two of the responding companies specifically answered that they review the material before reporting to law enforcement.

" After this is found, we review it and then send to the police."

" This material is reviewed after being discovered and sent to the authorities."

Suspension and termination of employment

One in ten of the surveyed companies reported putting the employee on suspension while the case is being investigated, and one in five reported that any employee found in possession of child sexual abuse material will have their employment terminated.

" We gather all documentation, person is put on suspension, authorities are contacted."

" Immediately notify law enforcement and place the suspected violator on a leave of absence for the investigation."

" Follow appropriate steps by notifying HR, contacting the authorities, and placing them on suspension until we can confirm their involvement which will result in termination."

" Immediate termination and reports to the Police."

" To fire that offender and alert police."

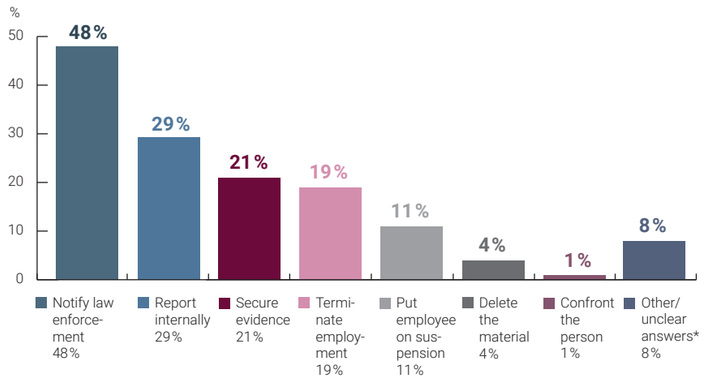
Deletion of suspected material

One in twenty of the surveyed businesses answered that the only action outlined in their plan is to delete the illicit material.

" We delete the images and other stocks of proof."

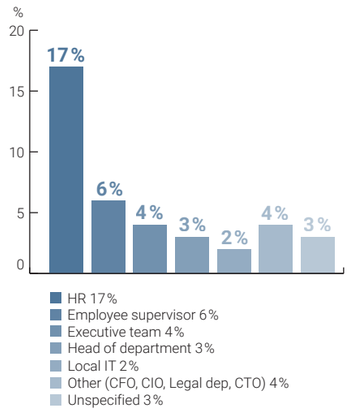
" We detect it then take it down and delete the software."

BREAKDOWN OF THE DIFFERENT REPORTED ACTIONS OUTLINED IN THE ORGANISATIONS' ACTION PLANS



* Includes general answers such as tighter control of child sexual abuse material, handling things cautiously and effectively fight the spread of child sexual abuse material.

POSITIONS TO BE REPORTED TO INTERNALLY ACCORDING TO THE ORGANISATIONS' ACTION PLANS



The respondents could identify several different job titles to be informed after child sexual abuse material had been found in the organisation. Therefore the numbers in this graph add up to more than the total number of those that report to someone internally (29 %).

8 Businesses' use of technologies to protect their IT environment from child sexual abuse material

– Eight in ten businesses have technology in place.
– Six in ten companies use filter solutions.
– One in ten companies have found child sexual abuse material.

EIGHT IN TEN BUSINESSES HAVE TECHNOLOGY IN PLACE

There are different technologies available to prevent child sexual abuse material being viewed, stored or distributed in the business IT environment or on company devices. These include different blocking tools (often in filter solutions) and detection tools. An overview of technologies used to detect and stop child sexual abuse material is outlined in section three of this report.

More than eight in ten businesses stated that they have technology in place to detect or block child sexual abuse material in the business IT environment.

SIX IN TEN USE FILTER SOLUTIONS

Six in ten of the surveyed businesses reported that they use some kind of filter solution to protect their IT environment from child sexual abuse material.

" Various blocking and filtering technologies."

" Internal firewall, software to block browser sites."

More than one third specified that they use filter solutions as part of an employee monitoring tool, such as Hubstaff, Teramind, BrowseReporter or SentryPC. Employee monitoring tools are used to track employee web or application use, monitor chats and keystrokes, and to also filter and make specific types of online content inaccessible.

One in ten use detection solutions

More than one in ten of the surveyed businesses stated that they use detection technologies to protect their IT environment from child sexual abuse material.

" Technologies that detect this type of material and alert us, so we can react properly."

Other solutions

One in twenty of the respondents reported that they use antivirus solutions. One in twenty also responded that they use different kinds of physical protection instead of IT solutions (such as surveillance cameras, microphones or physical law enforcement protection present).

" Cameras, Microphones, etc."

Nearly one in ten of the respondents gave unclear answers, such as enterprise resource planning (ERP) systems or protocols that are used when children go physically missing.

One in ten have no technology in place

More than one in ten of the surveyed businesses reported that they don't have technology in place to detect or block child sexual abuse material. When asked why, they primarily answered that they are unaware of technology that can detect or block child sexual abuse material, that it can be done manually or that they are of the opinion that this kind of material does not appear in business networks, and that they therefore do not need to protect their IT environment.

" I am not aware of such technologies."

" It can be done manually."

" Because we don't think that this happens on company networks."

ONE IN TEN COMPANIES HAVE FOUND MATERIAL

One in ten businesses reported that they have found child sexual abuse material in the business IT environment. They reported having found the material in a wide variety of ways; by IT specialist in different check-ups or IT scans, by someone else reporting it to IT, or with the help of technology.

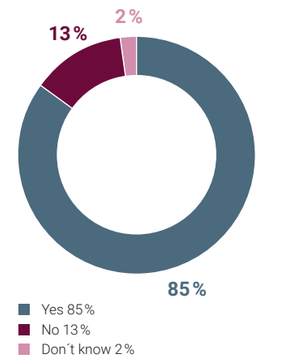
Nearly nine in ten respondents reported that they have not found child sexual abuse material in their IT environment.

Important to note is that it is customary in organisations to keep information about cases where an employee has been found to handle child sexual abuse material to a very tightly defined and limited group. Therefore, the results most likely reflect whether child sexual abuse material has been found in the particular region and during the time that the respondent has been in his or her current position.

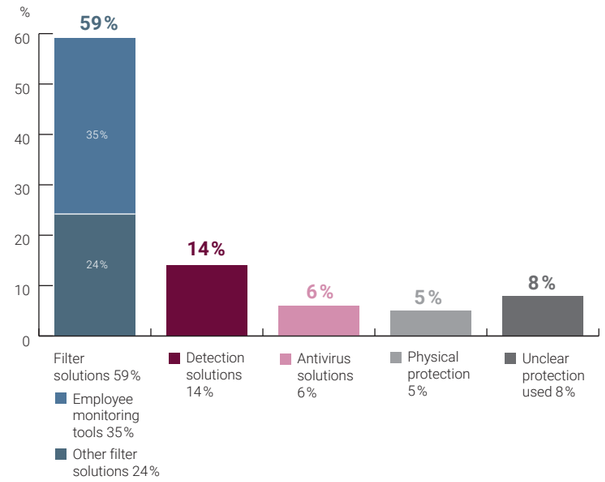
Law enforcement was notified and employee fired

In cases where child sexual abuse material had been found in the respondents' organisations, the surveyed businesses answered that they handled it by notifying law enforcement, conducting an internal investigation, and firing the employee.

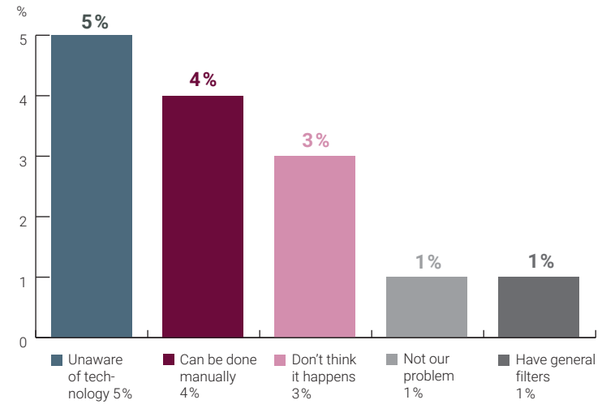
SHARE OF BUSINESSES THAT REPORT HAVING TECHNOLOGY IN PLACE TO DETECT OR BLOCK CHILD SEXUAL ABUSE MATERIAL IN THE ORGANISATION'S IT ENVIRONMENT



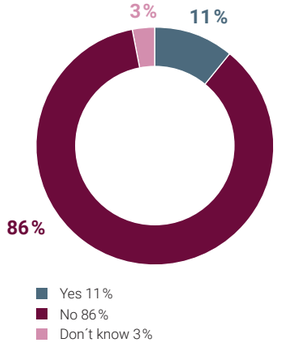
BREAKDOWN OF THE DIFFERENT TECHNOLOGIES THAT BUSINESSES REPORT USING TO DETECT OR BLOCK CHILD SEXUAL ABUSE MATERIAL



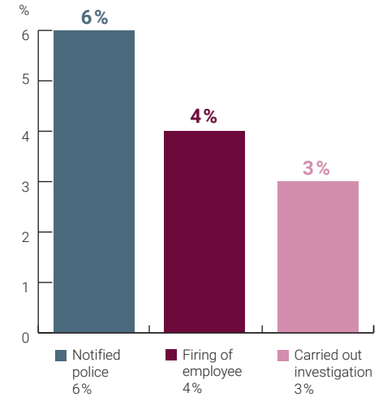
BREAKDOWN OF THE DIFFERENT REASONS REPORTED FOR WHY TECHNOLOGIES ARE NOT BEING USED TO DETECT OR BLOCK CHILD SEXUAL ABUSE MATERIAL



SHARE OF BUSINESSES THAT REPORT HAVING FOUND CHILD SEXUAL ABUSE MATERIAL IN THE ORGANISATION'S IT ENVIRONMENT



BREAKDOWN OF HOW THE SITUATION WAS HANDLED BY THE ORGANISATION



ANNA BORGSTRÖM
Chief Executive Officer, NetClean

THE WILL TO ACT NEEDS TO BE FOLLOWED UP WITH EFFECTIVE TECHNOLOGIES

It is gratifying to see that so many of the surveyed businesses have policies and action plans in place to stop employees from consuming child sexual abuse material. This must be followed up by effective policy compliance.

Action plan
Child sexual abuse material poses a risk to IT environments. It is therefore vital that businesses have an action plan in place to secure evidence correctly, ensure the welfare of any employee who might have seen the content, and to manage the offender who has downloaded the abuse material to the IT environment. Next, notifying law enforcement is crucial. It is only when the incident is investigated that more material is found, and children can be safeguarded.

Handling information
The human factor needs to be considered carefully in these types of cases, and information about discoveries need to be kept to a very small group of people. One reason is that other employees might find it difficult to continue working with a suspected colleague while evidence is gathered, which could risk alerting the suspect.

While securing, timestamping and recording evidence is helpful to the police, freezing or restricting access to networks or devices, or confiscating equipment also risks alerting the suspect. As a result the individual might delete material kept on other devices at work or at home.

It is also important to note that the child sexual abuse material itself should be handled as little as possible. As it is illegal to possess, it should not be saved, copied or shared.

Effective technologies
Most of the surveyed businesses report that they have filter technologies in place to protect their IT environment from child sexual abuse material. Although many filter technologies offer different kinds of measures to stop inappropriate content – often adult pornography – child sexual abuse material is normally not a prioritised threat. In addition, they rarely find child sexual abuse material on an image content level. As a result their effectiveness is limited*. Antivirus solutions have even more limited capabilities to find and stop child sexual abuse material.

It is encouraging to see that fourteen percent of the businesses report using detections tools, which are arguably much more effective in this case. These technologies detect on image content level, and are specifically designed to find child sexual abuse material.

Why detect?
The NetClean Report 2018 showed that 1 in 500 employees use their work computers to consume child sexual abuse material. Therefore, this year's result showing that only one in ten businesses had detected child sexual abuse in their IT environment was surprising. One possible explanation for this discrepancy is that incidents are usually kept within a very small group of people and that the survey respondent was not aware of all cases.

It is also very possible, as shown by the statistics on what type of technologies are applied, that businesses are not effectively protecting their IT environment against child sexual abuse material. Companies believe their solutions are efficient, but child sexual abuse material is still going undetected, and remains a hidden problem.

** Read more about filter technologies and detection technologies in section three of this report.*

COMMENT TO INSIGHT 7 AND 8

PAT GELSINGER
Chief Executive Officer, VMware

BUSINESS INTEGRITY AND ETHICAL LEADERSHIP

Today is the fastest day of technological evolution for the rest of your life; today is also the slowest day of technological evolution for the rest of your life. This provides us with incredible possibilities.

Will we expand the life of every human on the planet and eradicate diseases that have plagued mankind? Can we ensure modern education for every child on the planet, lift the remaining 10 % of the planet out of poverty, and reverse the implications of climate change? While we cannot predict the future, we can say that technology will play a significant role in these efforts.

Technologies also amplify human behaviour, both the good and the bad. This is why it is critical that we act responsibly in relation to the technologies that we create and the services that we provide; shaping them so that they are used in the way that was intended.

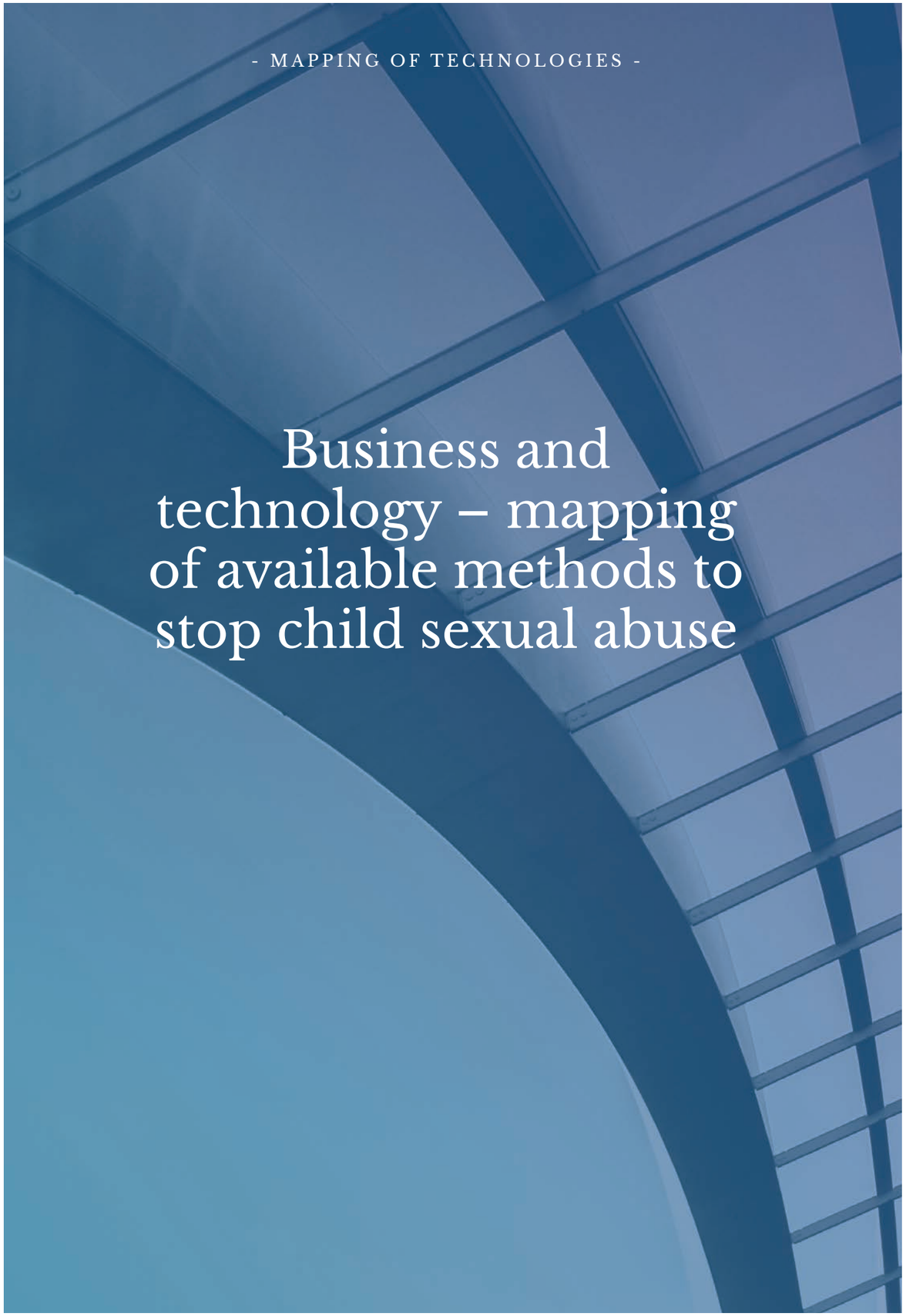
Drivers like the UNs' Sustainable Development Goals highlight the fact that companies must act in the interest of the future of the planet and humanity. One of the goals, SDG 16.2 – End abuse, exploitation, trafficking and all forms of violence against and torture of children, is to secure a prosperous future for all children, and all businesses have a great stake in this.

Child sexual abuse is a problem that has migrated online with the development of technology, and we must ensure that the dissemination of child sexual abuse material is disrupted in all services that we provide. Companies must act swiftly, responsibly and demonstrate leadership and integrity to ensure that we are doing everything we can to safeguard children.

At VMware, we use our own products and technology to solve our most critical challenges — the same ones faced daily by every IT organisation. A great example of this is our approach to build security intrinsically into our platform to eliminate a host of cyber threats and security complexity.

Now more than ever, the tech community has an individual and collective responsibility to engage and act. This applies not only to our own businesses but also to shaping global policy and regulatory frameworks to ensure that technology serves the greater good. At VMware, we strive to be a force for good.

VMware is a leading innovator in enterprise software. The company's cloud, networking and security, and digital workspace offerings, provide a dynamic and efficient digital foundation to over 500,000 customers globally, aided by an ecosystem of 75,000 partners. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough innovations to its global impact.



- MAPPING OF TECHNOLOGIES -

Business and technology – mapping of available methods to stop child sexual abuse

Overview of technologies and methods available to businesses to stop child sexual abuse material
The internet is a complex multi-layered place which provides many ways for offenders to share child sexual abuse material. Therefore, there is no one technology or solution that alone can police the internet against online child sexual abuse material. To effectively fight the spread of child sexual abuse material, different technologies must be applied by all who use the internet and have an interest in making it a safe space for future generations. This includes viable business planning.

If all businesses and organisations in the world – billions of computers and networks – took appropriate action, the opportunity to find and disrupt the spread of online child sexual material would increase infinitely.

Child sexual abuse crime is a complicated crime, one that is not easy to understand nor fight, but what is clear is that specialist technologies must be applied to stop the dissemination online.

There are a number of technologies that can be applied by businesses, and in this last section of the report we present an overview of technologies and methods available to businesses to stop child sexual abuse material. The articles are a revision and abridgement of longer and more technically detailed articles published on NetClean's website.

More information is available on www.netclean.com/technical-model-national-response/.

HASHING TECHNOLOGY/DIGITAL FINGERPRINTING

Binary Hashing

Binary hashing is used to fingerprint and discover online child sexual abuse material on a content level, i.e. it identifies the actual images and videos depicting child sexual abuse. Hashing technology is a secure, fast and reliable technology that is used in various ways, e.g. in detection tools, digital investigation tools and crawlers. It is used by law enforcement, NGOs, businesses and platform providers. When new child sexual abuse material is found, the image or video is classified as illegal and given a hash value, a unique digital fingerprint. These fingerprints are added to databases that are used in different kinds of software used to identify child sexual abuse material.

THE TECHNOLOGY

A binary hash is created by a mathematical algorithm that transforms the data of a file, whatever size it may be, into much shorter fixed-length data, a hash value. The hash value acts as the file's fingerprint, allowing software to find and identify it.

The conversion is arbitrary, however the algorithm always transforms the same input data into the same output data. The output data cannot be reversed or traced back to the original input data. This secure feature means that an image cannot be recreated from a hash value.

ITS USE

Hash values are produced by law enforcement agencies and select NGOs that work to combat child sexual abuse. When unknown material is found, a hash value is calculated and added to a database. Specialised software can then run matches against these databases and look for exact copies of the material on for example social media sites, and in IT environments that are protected by detection software.

Law enforcement agencies use hashes to find pertinent material in investigations and for evidence authentication, while some NGOs and social media companies send out web crawlers to actively search out known material and take actions to remove it. Businesses and organisations use detection software to safeguard their IT environment, to comply with policies and ethical values and work towards the Sustainable Development Goals. Detection software is also used to protect employees, especially IT professionals, from the risk of being exposed to child sexual abuse material.

STRENGTHS AND LIMITATIONS

Binary hashing is efficient and reliable. Binary hashes are non-reversible and as they will only detect classified material and identical files, the risk that technologies using binary hashing will flag the wrong material is extremely low.

The technology also works very fast. Typically, binary hashing matches are almost instant, and detection takes up limited processing power. This is crucial for businesses and organisations with IT environments where speed and processing power are of the outmost importance.

The limitation of binary hashing technology is the same as its strengths: That it can only detect already known and indexed material. Although this limits the scope for detection and removal of images, it guarantees accuracy as only material that has been classified by law enforcement professionals, and nothing else, is detected.

HASHING TECHNOLOGY/DIGITAL FINGERPRINTING

Robust Hashing

Like binary hashing technology, robust hashing is used to fingerprint and discover online child sexual abuse material on a content level. In contrast to the binary system, robust hashing technology looks at the actual visual content of an image rather than just the binary data of the image file. A widely used hashing technology is PhotoDNA. It was developed specifically to detect child sexual abuse material, and is used today by law enforcement, NGOs, businesses and platform providers.

THE TECHNOLOGY

Robust hashing ensures that the input data produces a hash value that will match any image with the same visual content. Like binary hashes, the PhotoDNA hash value cannot be reversed into an image.

Whereas two copies of the same image in different file formats will produce completely different binary hashes, robust hashing technology can detect the image even if a slight alteration, such as resizing or change of file format, has been made. This is because the recognition is based on the visual content of the image, rather than the binary file data.

ITS USE

As with binary hashing, PhotoDNA classification is made by law enforcement and a number of NGOs. The hashes are added to databases, which can be used to match and detect known child sexual abuse material.

Law enforcement use PhotoDNA hashes in the same way that they use binary hashes, and web crawlers use both binary hashes and PhotoDNA hashes when trawling the net.

Unlike binary hashes, robust hashes are more frequently used in environments where detection in real-time is not of critical importance. Social media platforms are one example of this. Another is that businesses can deploy a secondary and wider robust search in their IT environment after binary hashing technology has made a match. The robust search then scans nearby lying files to search for nearly identical material.

STRENGTHS AND LIMITATIONS

As with binary hashing, robust hashing technology detects only already known and indexed material. However, the robust technology is also able to detect images that have been slightly altered, which widens the search.

The choice of technology always depends on the context and purpose of the search taking place. The reason why robust hashing is not always used instead of binary hashing is that it, although it is very fast, is slower than binary hash matching. Instead of an instant match, the complete image has to be analysed for a PhotoDNA match, which takes more processing power. Therefore, depending on the search, one or the other, or the technologies combined, might be most effective.

Artificial Intelligence/ Machine learning

Artificial Intelligence, AI, and machine learning is increasingly being used in child sexual abuse investigations, by helping to recognise, categorise and triage material. It is a rapidly developing technology, which shows a lot of promise for this type of investigative work. Unlike hashing technologies, AI classifiers have the potential to recognise new and previously unclassified child sexual material.

THE TECHNOLOGY

One machine learning technique is artificial neural networks (ANN), which are based on efforts to model information processing in the human brain. The adage is that Artificial Intelligence is learning without instruction or programming.

ANN are adaptive systems that change based on external or internal information that flows through the network, i.e. the system is learning, and the networks infer functions from this learning. This is important in systems where the complexity of the data or task makes the design or function by hand difficult.

ANN learn and adapt through assessing data, and in order to draw the right conclusions they must train on high volumes of quality data. An AI application is only as good as the data on which it has trained. If the data is flawed the system will draw the wrong conclusions and become inefficient, or unhelpful. This is why, for optimum results (output) it is crucial to have high quality data and to structure the training in such a way that the system draws the right conclusions.

ITS USE

AI shows great future potential for finding, analysing and removing child sexual abuse material online.

AI classifiers are being developed at speed to assist with law enforcement investigations, and aside from law enforcement, industry is also developing AI applications to detect child sexual abuse material. One example is Google's AI classifier that can be used to detect child sexual abuse material in networks, services and on platforms.

There is also a clear case for businesses and organisations to use this technology. When a child sexual abuse image is detected in an IT environment, other files on the device can be searched with the help of an AI classifier. It is also possible to schedule these types of searches in the IT environment.

STRENGTHS AND LIMITATIONS

AI classifiers are unique in that they have the ability to detect previously unknown material. This increases the scope for detection, and identification and safeguarding of previously unknown victims. The technology is developing fast, and will continue to revolutionise the fight against online child sexual abuse exploitation.

However, an AI classifier is not a hundred percent reliable, and it will make mistakes. It is, in essence, only as good as the data that it has been provided with. If the data is flawed or too limited, the AI will draw the wrong conclusions, and even with the most high-quality data, it will still make mistakes. Hence, it still relies heavily on human verification to ensure that the AI classification is right.

Another limitation is that when an AI classifier makes mistakes, it is usually very difficult, if not impossible, to backtrack why it has made a particular mistake.

Keyword Matching

Keyword matching is widely used in everything from search engines to online advertising campaigns to media monitoring tools. In the search for child sexual abuse material, its function is to match words or phrases, in filenames or in text, that have been listed as suspicious and worth investigating.

THE TECHNOLOGY

Keyword matching in its simplest form is lists of words, phrases or groupings that match directly against for example filenames, chatlogs, documents or websites, to identify if they are relevant or not.

In addition to exact matching, matches can also be case invariant. This means, for example, that even if capital letters are used, the match will still be made.

Next level is fuzzy matching, which will match even if there are variations, made by mistake or on purpose. This includes simple spelling mistakes, letters being switched around, double letters, the letter A swapped with 4, or E for 3 etc.

The match can be further refined by attaching different values to different words, and different words in relation to each other.

Although not classified as keyword matching, further development of textual analysis with AI algorithms is used to analyse larger volumes of text for semantic summaries, translations, and correction of spelling to name a few examples.

Keyword matching relies on the quality of the keyword lists, how words have been combined and how relationships between words have been scored.

ITS USE

Files containing child sexual abuse material are often named in specific ways, hence the importance of keyword matches to filenames. They are often combinations of words, scrambled words or very specific terms used by offenders to describe certain types of material.

Lists of known keywords can be used by law enforcement to triage and identify pertinent material, and by platform providers and businesses to highlight suspected files.

Modern web filters, which are used by most businesses, also use keyword matching in a number of ways to look at content and produce a probability score to determine how likely it is that a site contains certain content, and whether it should be blocked or not.

STRENGTHS AND LIMITATIONS

Keyword matching is fast and takes up very limited processing power compared to analysis of images. It is also quite easy to get started. Even a limited keyword list will provide value from the start, and the process to refine and build lists to make them better is straight forward.

However, keyword matching is also highly complicated. The quality and value of keyword matching is directly related to the quality of the list that is used. This makes intelligence and deep knowledge of the subject necessary, and that much time is needed to maintain a list in order for it to be effective. As child sexual abuse material is rarely a prioritised area, this means that many lists are lacking.

Also important to note is that a match does not automatically mean that the file contains child sexual abuse material, it is only an indication, yet the file still needs to be reviewed.

Filter Technology

Filter technologies are used to protect businesses' and organisations' IT environments from cyber threats and other harmful traffic. There are different types of filtering options, but as a basic rule all filter technologies look at web traffic that passes in and out from IT environments to decide what can pass through. These methods work at different layers of a network, which determines how specific the filtering options can be.

THE TECHNOLOGY

Filtering technologies look for suspect behaviour, surf patterns, links, known "bad" domains or specific patterns in different ways.

Large corporations can have a million DNS requests every second. Looking in detail at all that traffic would require enormous data power. Therefore, instead of one solution trying to do it all, companies install different solutions that work in layers and look at different parts of the traffic.

DNS Filtering

DNS filtering checks website requests against a database of prohibited addresses/domains and either allows the requested webpage to be displayed or refuses the request.

URL filtering

URL filtering is a more sophisticated and granular technology that can be used to block access to specific websites or parts of websites known to contain malware.

The four most common ways in which a filtering solution prevents web pages from being loaded onto a user´s device are:

Blacklists. Lists of websites known to contain malware and viruses. When a request to visit a website matches a blacklisted website, the request is denied.

Category. Blocks websites that belong to a certain group of websites, such as pornographic sites or gambling sites.

Content filtering. Prevents access to items within, for example, an e-mail or website. The request is allowed, but the response is inspected at the proxy server to determine if it contains anything meeting configured criteria. It is used to block for example viruses, e-mail attachments, advertisements etc.

Keyword filtering. Blocks access to specific content by keyword without necessarily blocking access to an entire category of websites.

ITS USE

Most, if not all, businesses and organisations take steps to secure their IT environment against a multitude of threats with the help of filter technologies. However, whereas blocking of child sexual abuse is often included in one way or another in filter solutions, it is rarely, if ever, the focus of the technology.

STRENGTHS AND LIMITATIONS

Filter technologies are only as effective as the intelligence put into the solutions – such as the lists of keywords, or of domains or URLs known to contain harmful material. Keeping those lists up to date requires a lot of work and continuous updates.

Traditional filter solutions focus on security threats such as business intelligence, service disruptions, ransomware, fishing etc, and unfortunately, child sexual abuse material comes far down the list. As a result, filter technologies are used to block child sexual abuse material, but they are less effective than they could be.

Blocking Technology at the ISP Level

Blocking technologies are built to pick up and block domains and URLs that are known to contain online child sexual abuse material. It can take place on the Internet Service Provider (ISP) level of the internet, where content travels through providers' networks. In business' networks, blocking normally takes place through different filter solutions. Even though blocking on an ISP level does not fit in with standard business precautions when protecting IT environments, it is an important practice in the fight against online child sexual abuse material.

THE TECHNOLOGY

There are five main different blocking technologies for provider networks. The majority operate using lists of sites known to contain child sexual abuse material. These are compiled by different stakeholders, among others INTERPOL and the Internet Watch Foundation. If the blocking solution matches a search for a web address against the information it has on its list, the request will be blocked.

Domain Name Server (DNS) blocking:

A DNS filtering solution is a specific type of web filter that operates as a middleman between a client computer and the web server that it is trying to access. DNS technology is cost effective, but comes with the drawback that it is easy to circumvent. Further, most businesses use their own DNS and not the ISPs, with the consequence that most traffic from businesses is not picked up by DNS Blocking. As it blocks on domain level, there is also a risk of overblocking.

Deep Package Inspection (DPI):

This technology has the capability of looking at the actual content rather than URLs, and at all the traffic that flows through the ISPs networks. It is also very difficult to get around. The drawback, and the reason why it is not used much, is that it is expensive and can slow down traffic through the networks significantly. The technology also raises questions about the users' integrity and how the internet should or shouldn't be policed.

URL blocking solutions:

This is a hybrid of the technologies mentioned above. Instead of analysing all data, this technology looks at specific pages that have been put on a blocking list. The technology is scalable, more difficult (although not impossible) than DNS to get around and blocks URLs rather than whole domains, allowing for a less heavy-handed approach.

Proxys and firewalls:

Blocking lists can also be held in proxy servers or firewalls. This is a technology that is frequently used by businesses. The disadvantage to this technology on ISP level, is that the quality of traffic will be heavily reduced, and it is expensive as it is difficult to scale down the volume of data that is being looked at.

Blocking technologies in the operators' router:

A cheap and simple solution is the possibility of operators blocking IP-addresses directly in their own routers. This is a heavy-handed solution, as it will block all pages on the IP-addresses, leading to heavy over-blocking. As a result it is hardly ever used.

ITS USE

Blocking technologies are built to pick up and block domains and URLs that are known to contain online child sexual abuse material. DNS is the most commonly used technology, used by many ISPs around the world to protect their networks from being used for criminal purposes. Although this is a start, there is much more work to be done in this area to make sure that all ISPs block child sexual abuse in their networks, and do it using the most effective technology.

STRENGTHS AND LIMITATIONS

Blocking on a general level is a somewhat blunt tool as it does not detect new material or bring new intelligence to law enforcement.

However, blocking is needed because large amounts of child sexual abuse material is still stored, shared and distributed through the open internet and on unencrypted websites.

Blocking covers a large part of the internet, and is very important to stop spread of online child sexual abuse images, and the revictimisation that happens every time an image or film is shared.

CONCLUSION

TECHNOLOGY – A DRIVER OF BOTH PROBLEM AND SOLUTION

Anna Borgström, Chief Executive Officer, NetClean

Technology has developed at an unprecedented speed over the past couple of decades. Large parts of the globe have access to the internet, mobile phones are ubiquitous, and there is an infinite amount of ways to communicate across the web. The possibilities for what we can accomplish online are mind-boggling.

As with everything else, technology has also moved child sexual abuse online. Live-streamed child sexual abuse is one development, and an increasing problem which we had not heard of a decade ago. We frequently think about it as a crime that happens far away, but this report shows that is happening everywhere, also so right where we are. Children across the world are being subjected to sexual abuse online, and their vulnerability when it comes to live-streamed offences is great.

Technology is now the driving factor behind how material is produced, distributed and stored. All mobile phones have a camera, a factor which has markedly influenced how material is produced, and the almost infinite ways of communicating online drives the dissemination of the material. Phones, USB sticks, laptops and external hard-drives are capable of storing increasingly large amounts of data, and in addition there is the possibility to store data online.

Technology also plays a pivotal role in police investigations. Examples of that are challenges following E2E encryption and built-in encryption, and the difficult nature of investigations on darknet/TOR.

However, technology is not just a driver of the problem, it also presents solutions to fight it. It is, for better or worse, a double-edged sword. Prior to moving online, child sexual abuse was far less discussed and largely confined to the dark and murky places of humanity. Today we have the possibility to detect the crimes and safeguard children.

There are many different tools to aid this work. There are tools designed specifically to block child sexual abuse material in Internet Service Provider networks, and technology that can detect how material is shared in P2P networks. NetClean specialises in technology designed to detect child sexual abuse material on laptops and IT systems belonging to employers of every size. The police have access to tools ranging from forensic programmes that extract data from devices, to programmes that sort and analyse the large quantities of images and videos that occur in criminal investigations.

Artificial Intelligence is opening up a whole new world of possibilities, and will be a game changer in the fight against child sexual abuse. However, as with all technology it is not in itself a holy grail. To be truly effective, we have to also scale already existing technology on all fronts so that we can meet the challenges of today and tomorrow in a comprehensive way.

And while technology is continuing to be refined and developed, the crime of child sexual abuse and the welfare of future generations is also gaining more importance on political agendas across the world. This means more recourses, more involvement, and more tangible desire and knowledge to generate real action and efforts to stop child sexual abuse. Technology, knowledge and collaboration is the key to achieve this.

3,707

CHILDREN SAFEGUARDED FROM SEXUAL ABUSE DURING 2018

The police officers who participated in the survey were asked how many children their unit had safeguarded from sexual abuse in 2018. Together they had rescued 3,707 children.

ACKNOWLEDGEMENTS

We would like to extend our gratitude to the 450 police officers who participated in our research and took the time to share their knowledge and expertise with us. The work that they do is invaluable and life changing for each of the 3,707 children that they safeguarded in 2018, and for all children rescued prior to that.

We also want to direct a big thank you to our sister company Griffeye, for asking their customers to participate in the survey on our behalf.

We would like to thank the businesses that answered our survey in the US, for taking the time to answer the survey and for providing us with a better understanding of how child sexual abuse material is tackled in large organisations.

Finally, we would like to thank all individuals that commented on the report. Your insight and expertise provide us with the opportunity to contextualise and bring further meaning to our research.

Thank you!

READ AND DOWNLOAD THE NETCLEAN REPORTS

The NetClean Report 2019 is the fifth annual report about child sexual abuse crime produced by NetClean. All the reports can be read and downloaded on www.netclean.com.

About NetClean
NetClean develops world leading technology solutions to fight child sexual abuse. Our solutions are used worldwide in business IT environments, by large and medium sized businesses, government agencies and public sector organisations. The technology reacts when it detects the digital fingerprint of an image or video that law enforcement has classified as child sexual abuse, to keep workplaces free from child sexual abuse material.

NetClean.