

THE WHY.
THE HOW.
THE WHO.
AND THE
RESULTS.

**The Internet Watch Foundation
Annual Report 2019**

We are the Internet Watch Foundation

We're a child protection body. We use cutting-edge technology to find, remove, disrupt and prevent child sexual abuse imagery on the internet. We help to make the internet a safer place for children and adults across the world.

We're a not-for-profit organisation, supported by the internet industry, the European Commission and the generosity of ordinary people.

We work closely with police, governments and NGOs globally, who trust our work.

For 24 years we've given people a safe place to report imagery anonymously, now covering 30 countries.

We assess every report we receive. If it shows the sexual abuse of a child, we make sure the image or video is removed. To do this effectively, we develop technology-for-good and provide bespoke tools to our industry Members.

We care. No child should suffer repeated abuse and victimisation by having the recordings of their abuse shared time and time again.

Our work relies on compassionate and resilient staff members, who are highly trained and carefully looked after.

We encourage others to play their part, whether by reporting to us, funding us, or collaborating on the best technology and research.

The children in these pictures and videos are real. The suffering captured in this imagery and the knowledge that it could be shared can haunt a victim for life.

That's why it's our mission to eliminate this material for good. And to show every child there is someone out there who cares enough to help.

Contents

Forewords	4
1. Why we do this	7
Becky's story	10
Ana's story	12
2. How we do it	15
Rosa's story	20
Hotline case studies	21
How we process reports	22
Creating technology-for-good	24
Our policy work	26
Our reporting portals	27
3. Who we work with	31
Caring for our staff	34
UK Safer Internet Centre	35
Our Members	36
4. The results	39
Highlights and awards	44
Statistics and trends	46
Domain analysis	50
Geographical hosting of child sexual abuse images	52
Trends and patterns	54
Trend: Commercial child sexual abuse material	55
Trend: "Self-generated" content	57
Analysis: Child sexual abuse material by age	58
UK hosting of child sexual abuse imagery	68
Our key services to technology companies	70
Glossary of terms	74

Forewords

Welcome from our Chair

Welcome to our 2019 report. Once again, we've witnessed an increase in the number of child sexual abuse reports despite the number of expert analysts in our Hotline staying the same. We were able to do this because in 2019 we invested in building a strong internal team of technical experts who have developed new technology to help us fight the problem more effectively.

In 2019 the UK Government published its Online Harms White Paper, with the goal of making the UK the safest place in the world to be online. It proposes the introduction of a new Regulator, whose remit extends beyond the illegal content the IWF is concerned with, to wider online harms. Much of our year was spent in detailed discussions with government and companies to explore how we can work together to ensure children are protected without compromising the security and privacy of internet users.

As someone who places human rights at the heart of everything I do, it was important for me, as Chair, to ensure that the IWF's contribution to the debate was balanced and well-informed. Too often the public narrative is that the "household name" companies do very little to fight the problem. It's certainly true that everyone needs to do more. But we also need to have a broader, honest, discussion about who the bad actors are, even if they reside in territories outside of the UK and have little, or no, input in online safety discussions. The ecosystem is complex and magic bullet solutions don't, unfortunately, exist.

The mission of the IWF is to eliminate online child sexual abuse from the internet. I'm convinced that our role will be even more important in future years as we provide a trusted technically-proven solution to reporting and removing this content as well as providing a unique brokering role between the internet industry and the government and law enforcement.

Our work gives us important insights on how these illegal images are generated, hosted and accessed – information that enables us to play a pivotal role in finding solutions to what is a global problem.

We are also committed to working with our Members to be more transparent and accountable so that people are aware of what they, as companies, are currently doing – and what more they could do – to ensure that their platforms are free of online child sexual abuse. This may involve us in difficult conversations but we don't shy away.

Finally, in 2019 the Hotline operations of the IWF were independently audited and the team, led by Sir Mark Hedley, concluded: "We have observed a small efficiently-run organisation with a highly dedicated and skilled workforce doing a job that is both vital and very stressful. We were impressed by the good relationships between staff at all levels and the essential determination to maintain a high quality of work and relationships."

The IWF team do one of the most difficult jobs imaginable, and on behalf of the Board I want to thank and acknowledge the contribution of each and every staff member, led by Susie and her senior team.



Andrew Puddephatt OBE
IWF Chair

Welcome from our CEO

Nine years ago, I was appointed CEO of the IWF. In that time, we've grown from 16 staff to 45, our membership of technology companies has tripled and our services are deployed by the internet industry in every corner of the globe. Most importantly, we have removed more criminal content year-on-year, inching a little bit closer each day to our mission to eliminate online child sexual abuse imagery.

In 2019 we removed a staggering 132,700 webpages which included millions of images and videos of real children suffering real sexual abuse. To say it's a challenging task is an understatement. As more and more people get online access, so do new platforms for sharing this content. Yet, at the same time, we keep pace by developing and using new innovative technology, enabling us to take down more content, staying one step ahead of the perpetrators.

It would be easy to simply talk about the big numbers and the cutting-edge technology we use, but we must bring every conversation back to the abuse suffered by the individual children in the images. For their sake, we will never give up and we will continue to send a powerful message to the perpetrators that if you post this content online, we will find it and take it down. This is important, as every single time we remove an image or video we stop the revictimisation of that child and we give them hope that one day no one will be able to find images of them on the internet.

I also want to talk about the IWF team. Most people simply don't realise that even with the use of the latest technology, our Hotline team must still manually assess every single webpage before we remove it.

We have a dedicated team of highly skilled expert analysts who spend every working day viewing and assessing some of the most difficult and challenging content imaginable.

It doesn't matter how often the team sees this content, they never lose their humanity or fail to be shocked by the level of depravity and cruelty that some – a minority – engage in.

The team at the IWF do a job that very few people would be able to do, and they do this with relentless cheerfulness and a driving passion because they all believe in our cause.

We make sure we look after them properly and provide regular counselling and other support. We also have a team of supporting staff who work just as hard and are equally committed to the IWF mission and to making the UK one of the safest places in the world to be online.

I know I speak for the whole senior team when I say we lead the IWF with genuine pride. Whilst the content we are dealing with can be harrowing, every single member of the IWF team can go home every night knowing that they made a tangible difference. In how many jobs can you say that?



Susie Hargreaves OBE

IWF CEO and Director of the UK Safer Internet Centre



T T Y

T A T T T Y

WHY
WE DO
THIS

HY
DO
IS

HIS

RIGHT NOW,

THOUSANDS
OF CHILDREN
ARE BEING
EXPLOITED

IN NEW AND
HORRIFIC WAYS.





The internet has supplied people with the perfect tool to create, collect and share images of child sexual abuse and exploitation.

Right now, thousands of children are being exploited in new and horrific ways.

Images of past abuse circulate for years, destroying children's lives far into the future.

The youngest suffer. 87% of all images we see of babies and toddlers show the worst forms of abuse.

So for 24 years we've been fighting to make the internet a safer place for children and adults.

That's why.

Becky's story

Becky is about 10 or 11 years old. She sometimes styles her long brown hair in a plait or ponytail. We see her green eyes firmly fixed on the comments and messages being written to her at the bottom of her screen.

**She's still in primary school.
Cuddly toys are scattered on her bed and someone's adorned her bedroom walls with fairy lights.
We see her twice a day, every working day in our Hotline.**

Becky films herself in her family bathroom – which is clean and bright – and in her bedroom.

It's clear that she's being 'directed' by someone – or many people – on the other side of the live stream. She pauses to read comments or instructions before acting out what's asked of her.

It's clear Becky is not alone at home. She jumps at a noise outside the bathroom and her reaction is immediate – she looks nervous and quickly stops filming.

In a third of all the recordings we see of Becky, she's been encouraged to use everyday items from her bedroom and bathroom to insert into her vagina. In legal terms, this is category A penetrative sexual activity.

There are no clues as to where Becky is. In our Hotline, we wonder if it was one person grooming her online into producing the videos, or many? Is she aware of how widely they've now been shared across the internet? Is she scared her family or school friends will see the videos?

We doubt she knows that the live streaming was being recorded, copied and shared by those with reprehensible interests.

Whilst we find and remove this content from the internet, in 2020 we will launch a national campaign to help prevent the creation of this type of imagery.

We pieced together Becky's story over a three-month period by collecting and recording data every time we saw her. Names and some details have been changed to protect identities.



Self-generated child sexual abuse content

In this annual report, for the first time, we'll be grouping our data into age ranges. We'll also be separating the number of child sexual abuse URLs we've dealt with into two groups; where there was contact offending involved, and content that was created with no offender present in the room – something given the catch-all term “self-generated” child sexual abuse content.

The term self-generated covers imagery produced as a result of a range of behaviours.

This can include:

- Consensual sharing between peers as part of an age-appropriate relationship;
- Non-consensual onward sharing;
- Sexualised behaviour online in order to receive “likes” or validation; and,
- Coercion, grooming and even blackmail of a child by adults (or adolescents) to perform sexually over webcam or send explicit imagery, which may then be further shared online with others. *

** This paragraph has been informed by the Global Threat Assessment 2019, WePROTECT Global Alliance P30.*

Ana's story

We see Ana a lot. Every day at least. Sometimes twice a day. She's been groomed into taking part in sexual activities from a very young age with people who we think are her relatives.

We first see her aged seven. We stop seeing her when she's 11. Her long, tangled blond hair, green eyes and small frame being forced into things she shouldn't know how to do.

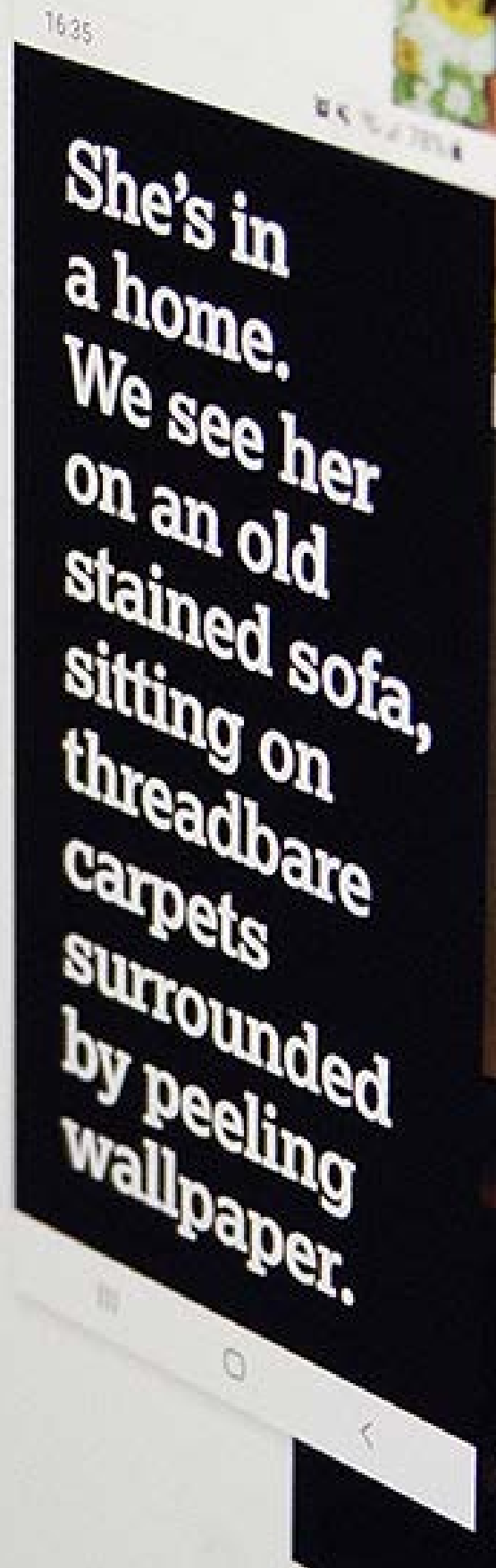
Most often she is with another little girl and an older boy. We guess they might be her brother and sister, but we don't know for sure. They're not playing. Not in the sense that children should be free to play. Sometimes we can see a man as well. Is this her father?

She's in a home. We see her on an old stained sofa, sitting on threadbare carpets surrounded by peeling wallpaper.

Ana has been made to pose provocatively and take part in several sexual activities. She's also raped.

Ana's treatment is degrading and extremely cruel. Unfortunately, this is reality for the children we see in pictures and recordings in our Hotline.

We wanted to learn more about Ana's experience: Over three months we saw her 96 times. In two in every five occasions she was being raped or suffered some other kind of sexual torture. Other times she was suffering sexual abuse which didn't include penetration.



We don't always know if the children we see are ever rescued from their abuser. This is true of Ana.

We imagine that Ana – who might be in her late teens – has now realised that the horror of what she experienced was not “normal”, was not “an expression of love”, but instead was a ruthless and criminal exploitation of her innocence. It was multiple crimes committed over several years and instigated by those who should have been protecting and nurturing that innocence.

Ana may well wear the mental, and potentially physical, scars of the abuse she suffered for the rest of her life. If she is aware that the videos and photographs continue to be circulated online today with such prevalence, her suffering is likely only further compounded.

Ana is sadly one of many, many children we see every single day. A victim of grooming – robbed of her right to a carefree and innocent childhood.

We can only hope that she now has the support and care she deserves, but the sad truth is we just don't know.

You can hear more victim and survivor experiences in our podcast, [Pixels From a Crime Scene](#), launched in spring 2020.

We pieced together Ana's story over a three-month period by collecting and recording data every time we saw her. Names and some details have been changed to protect identities.



HO

HOW

HI
HWE

WDO

DO
D

OW

W

AT

HOW
WE
DO IT

DO IT


WE FIND, ASSESS
AND REMOVE
MILLIONS OF
CHILD SEXUAL
ABUSE IMAGES
AND VIDEOS
FROM THE INTERNET
EVERY YEAR.



We take reports from the public, police and technology companies as well as actively searching the internet.

We build bespoke tools for technology companies to keep networks safe and outsource our skills to others who need our help.

From the UK we operate a reporting hotline for child sexual abuse imagery covering 30 countries - with another 20 planned before the end of 2020.




We play a unique role, uniting technology companies, law enforcement, government and civil society to prevent the abuse of children online.

By analysing web hosts, payments and cryptocurrency abuse we work with our technology and police partners to tackle online sites and share what we've learned.

We see when offenders find new ways to sexually abuse children through new technology - and have the skills, the relationships and the technical expertise to respond immediately.

That's how.



FOR IMAGERY HOSTED
IN THE UK WE CAPTURE
THE EVIDENCE

TO HELP
SAFEGUARD
CHILDREN
AND PROSECUTE OFFENDERS



Rosa's story

“It’s a human issue, spread by technology like never before, and we have a lot of work to do”.

By Rosa, IWF analyst

“Imagine your darkest moments exposed to an unknown number of people. Then imagine strangers watching your pain for sexual satisfaction. That’s what happens for some of the children whose abuse images we see online. Each day I work as an analyst I question how people are so determined to abuse, coerce and exploit children sexually, let alone record it and pass it around.

I can’t step into a video or image and stop what is happening, but I can help stop it existing online, and that’s why I work as an analyst.

Sometimes a video or image will hit us harder than normal.

In one video, a little girl no older than six was being raped and filmed by an adult in a home setting. She looked tired and resigned, as though this had become her ‘normal’.

Sadly, I saw her images several times in the course of the same day. I remember wondering whether it would ever end for her.

Doing this job has made me realise just how big the problem of online child sexual abuse is. It’s a human issue, spread by technology like never before, and we have a lot of work to do.

Over the years I’ve spent a lot of time listening to survivors of childhood sexual abuse and hearing how that experience has stood in the way of their life so many times. Coming to work at the IWF meant I could make a practical difference. When people know that the images of their childhood suffering can – and will – be stopped from re-emerging, they can feel safer and stronger.

It feels good to know that we’re helping to make the internet a safer place.

The recruitment of our wonderful, resilient analysts is a strict process. And we put considerable thought into how we look after them. An independent inspection of our Hotline described our welfare programme as ‘exemplary’. Find out more on page 27.

*You can hear more about the work of our analysts in a behind-the-scenes podcast called *Pixels From a Crime Scene* launched spring 2020.*

Hotline case studies

A hacked Russian medical site

“We were contacted by the NCA with a request for assistance: they had been alerted to a website that appeared to be displaying links to criminal images of child sexual abuse, and asked if we could help.

“It was a legitimate business – a medical centre in Russia – but it had been hacked by criminals with the aim of sharing access to child sexual abuse images and videos. Due to the hacker’s methods of including lots of links to child sexual abuse content, this was painstaking work.

“It led us to a cyberlocker (online storage) site. There, more and more links were found. Each link in turn led to many more, all of which were hosting criminal content. Due to the overwhelming number of URLs, our whole team of 13 analysts was tasked with assessing and removing these images as a priority, as well as handling daily reports from the public as usual.

“For each cyberlocker file, a password was required to access the criminal content within, and we used our expertise in dealing with these types of sites to deduce what they were. Almost all of these files contained self-generated images of child sexual abuse, with category A images (the most severe) of girls aged seven to 13 appearing most frequently.

“In total, we processed over 3,000 separate URLs in just over five weeks as a direct result of those original links on the medical centre website. For each criminal image or video, we made an assessment, the hosting country was identified and our partner Hotlines in the USA, Romania, France and the Netherlands were notified immediately, so the images could be removed from the open web as quickly as possible.”

“As well as seeking to remove the child sexual abuse images from the cyberlockers, we worked in partnership with the Russian Hotline to remove the original links from the hacked medical centre website. Together, we made sure the site was cleared of all criminal content.”

Lucy, Internet Content Analyst

Girls safeguarded

“I was very proud this year when I learned my actions helped to safeguard two girls. I was assessing a video which captured their abuse via a live stream. One of the girls held up a sign with a profile name and so I got to work. I found a number of social media accounts and sent a Victim ID referral to our partners at the Child Exploitation and Online Protection Centre (CEOP). It helped narrow the search. We heard back from the police that actions to safeguard the girls were taking place. It’s great to know I’ve played a part in that.”

Henry, Internet Content Analyst.

Creating efficiency

“I am proud to have worked on some technical developments which enable our analysts to assess more reports, more quickly.

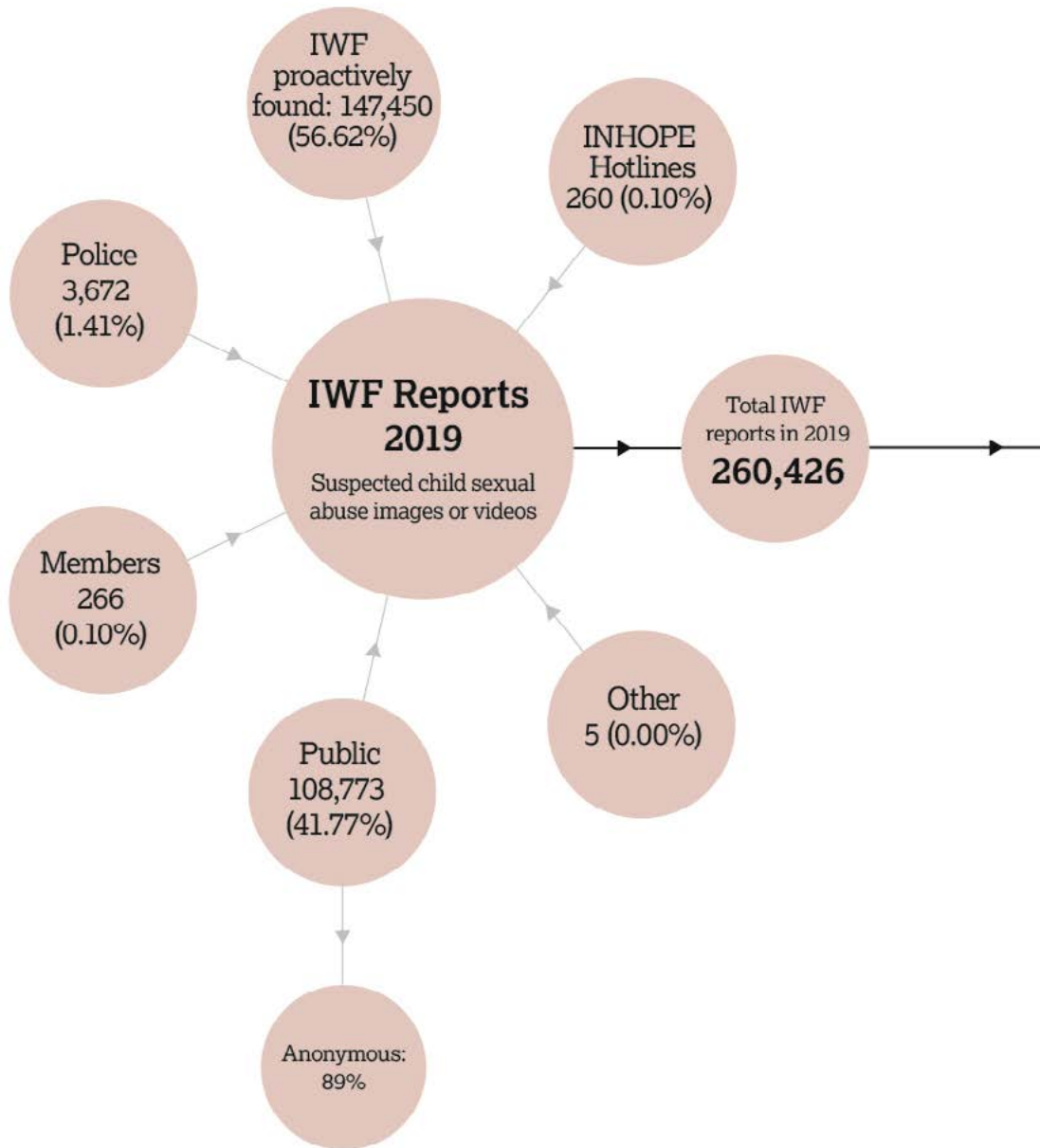
“I developed some new features within our Report Management System that support bulk operations on a number of tasks, helping to make our Hotline more efficient.

“There’s now less for the analysts to remember, and some reports can be completed in a fraction of the time. It also means we can provide a better service to our Members.”

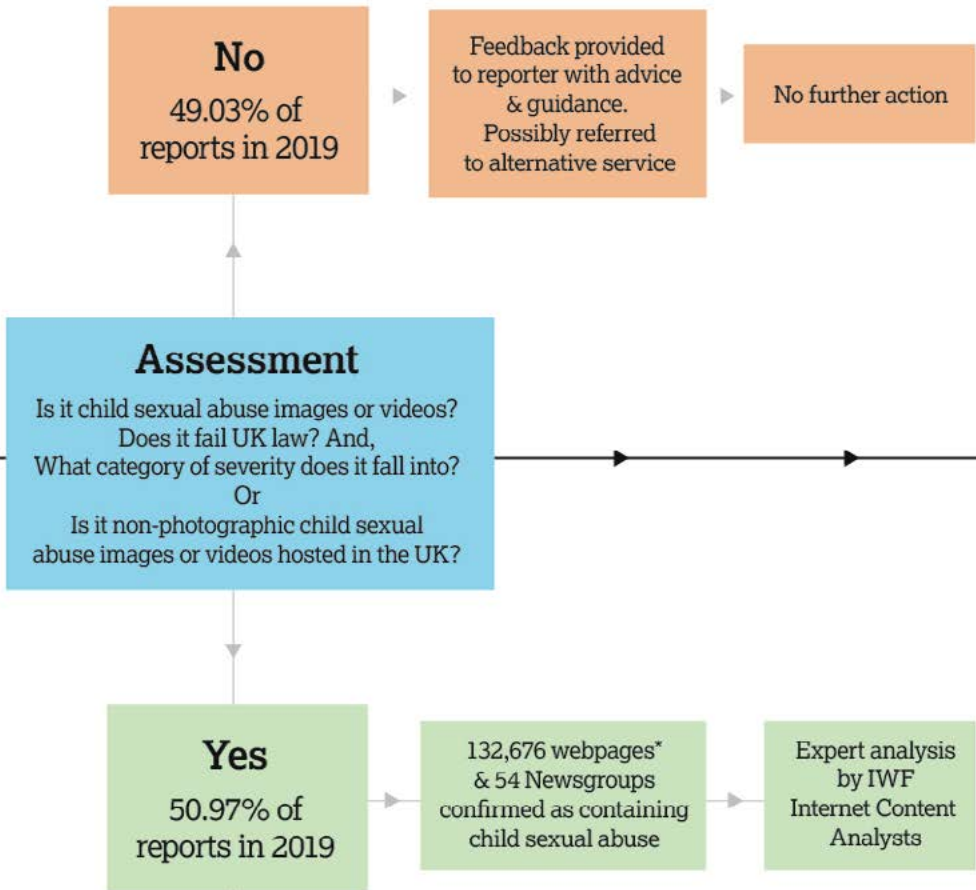
Bino Joseph, Systems Support and Developer

How we process reports

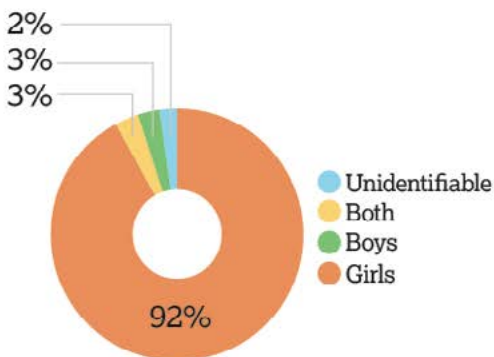
Step 1: Where reports come from



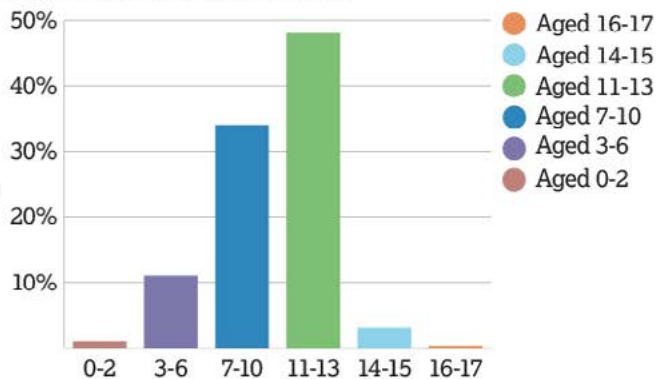
Step 2: Assessment



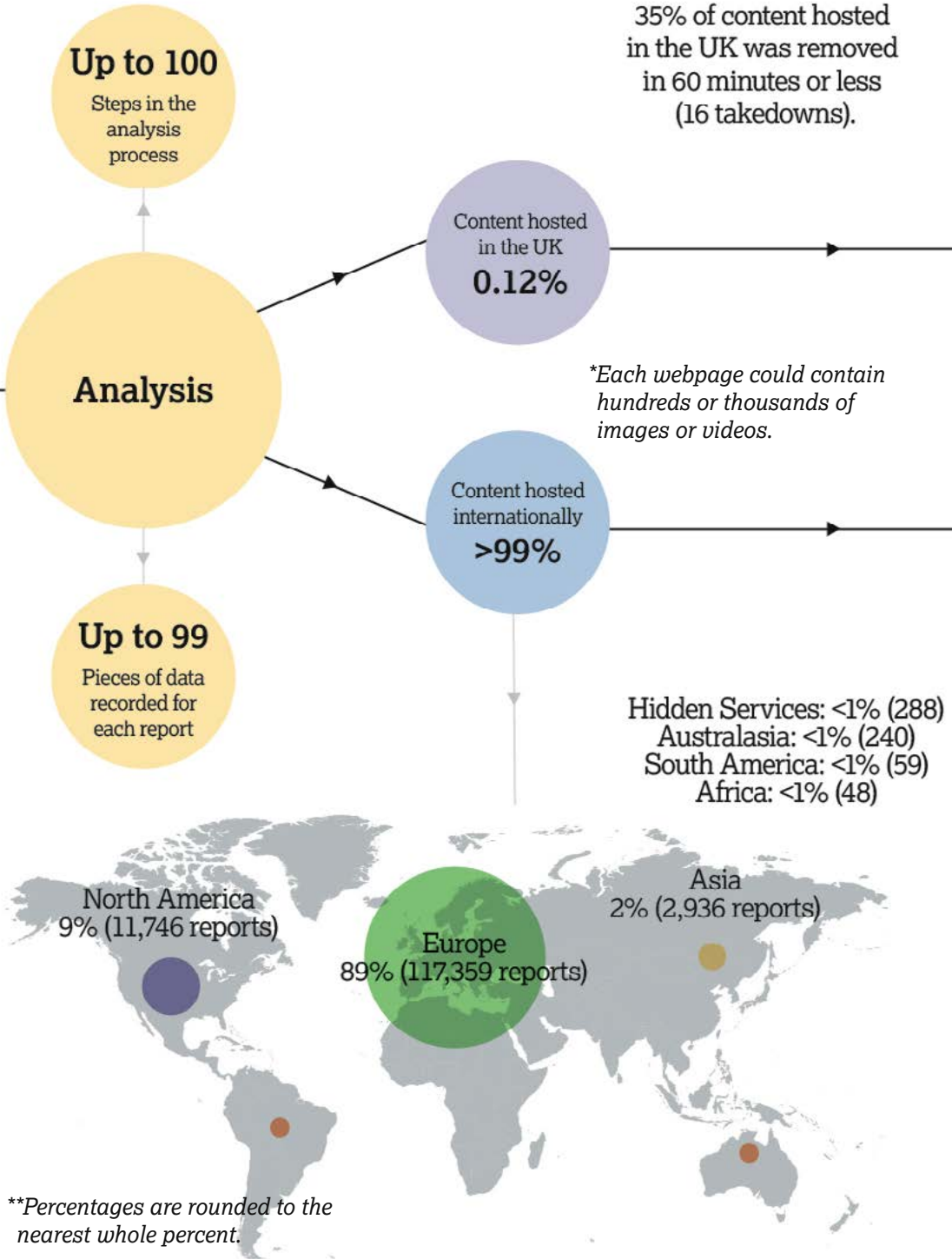
Sex of the victims in 2019**



Age of the victims in 2019



Step 3: Analysis



Step 4: Our actions

NCA & Regional
Police Force
notified for
investigation and
permission.

1

Notice sent to
hosting provider to
preserve evidence
and remove content.

2

Images collected,
graded & hashed.
Images & hashes
added to CAID.

3

Webpage
monitored until
content removed.
Report closed.

4

Report submitted
to INHOPE
or direct contact with
international
hotline or
relevant agency.

1

Images collected,
graded & hashed.
Images & hashes
added to the Child
Abuse Image Database.

2

Webpage added
to IWF URL
List to prevent
accidental
access before
removal.

3

Webpage monitored
until content
is removed.
Overdue content
chased directly
by IWF team.

4

Webpage
removed from
the IWF URL List
after removal.

5

Creating technology-for-good

Technology is a wonderful and powerful human invention. However, it has made it easier to harm children. While technology empowers the abuse, it can also stop it. We're building technology-for-good and putting it in the hands of our expert – human – analysts.



IWF Tech Team



**Fred Langford Deputy
CEO & CTO**

Automation

We're building a stack of classifiers. These will help us to triage public reports, helping to identify those most likely to show new child sexual abuse material, versus duplicate images which we've seen and assessed before, and other, off-remit content.

Our goal is to automate parts of the assessment procedure, whilst ensuring that human verification still sits at the heart of what we do.

Our classifiers will empower our analysts to have an even greater impact: their time and skills will be more focused on reviewing new child sexual abuse imagery and the imagery which requires finer judgements, and their wellbeing will be better safeguarded by not having to see the same child sexual abuse imagery on multiple occasions. The children depicted in the duplicate images will have greater privacy as our analysts will no longer need to see their suffering over and over again.

Nominet grant building tech-for-good

IWF has been awarded £100,000 as part of Nominet's public benefit programme to counter online harm. The Nominet Tech Innovation Fund is designed to ensure simple and rapid access to the funds to invest in projects that look ahead and pre-empt emerging threats.

Collaborative engineering community

Strong partnerships are at the heart of everything we do. We're implementing a system to enable our in-house technical team to collaborate more effectively with external partners from across the globe.

The IWF DevOps Community will enable engineers and developers from a wide range of organisations to help us create new tech-for-good.

So far, this has allowed us to streamline our own in-house improvements. We can now roll out our technical developments more swiftly, it's easier to scale them up and we can integrate everything with our bespoke Report Management System.

Criminals are often the first to abuse new technology; our DevOps Community means we can keep pace, and even out-pace, the offenders.

Transatlantic Hash Sharing

We signed a landmark data sharing agreement with the USA's National Centre for Missing and Exploited Children (NCMEC). This allows us to pool our hashes of child sexual abuse imagery, making them available to internet companies in the United States and beyond.

This represents a huge step forward in providing internet companies with the tools to prevent the uploading, sharing and storage of this abuse on their platforms. Each time one of our expert analysts identifies an image or video of child sexual abuse, they "hash" it for our database – giving it a "digital fingerprint" which allows it to be identified if it's re-shared or re-uploaded. Sharing hashes allows technology companies to help prevent the repeated trauma of countless children.

The NGO Sharing Platform now contains more than 3.5 million hashes of known child sexual abuse imagery.

High standards revealed by Hotline Audit

Every two years our Hotline undergoes an independent inspection, led by Sir Mark Hedley, a High Court Judge.

In 2019, his team comprised Dr. Edward Humphreys, a retired Professor of cyber security, Martin Clabon, a former career police officer with experience in the investigation of child sexual exploitation and currently the National Auditor of the Child Abuse Image Database, and David Trickey, a consultant clinical psychologist.

The full report is published unredacted at iwf.org.uk. It found that the IWF is an "efficiently run organisation with a highly dedicated and skilled workforce doing a job that is both vital and very stressful." It commented that there was a "determination to maintain a high quality of work and relationships". Our welfare programme to look after all staff, but particularly our analysts, was praised as "exemplary" and also an "absolute necessity".

Regarding our assessments of child sexual abuse imagery, the inspection team was "satisfied that reasonable judgements to consistent standards were being made" and that this was "kept under proper review". Additionally, induction training for new analysts was described as "outstanding".



Sir Mark Hedley
High Court Judge

Our policy work

Online Harms agenda:

The UK Government published its Online Harms White Paper in April and IWF responded to the public consultation following discussions with Members, law enforcement and Government.

The IWF is supportive of new regulation to combat online harms including child sexual abuse.

We believe future legislation should:

- Build on existing effective regulatory solutions and complement the voluntary work undertaken by companies;
- Ensure that any legislation is developed in partnership with industry and it is essential that technical experts are involved;
- Involve the UK Government working collaboratively with international stakeholders to tackle what are ultimately, international issues.

Independent Inquiry into Child Sexual Abuse (IICSA)

Our CEO Susie Hargreaves, and Policy and Public Affairs Manager Michael Tunks, spent two weeks at IICSA as Core Participants in their Internet Investigation.

We emphasised our track record of reducing UK hosting of child sexual abuse material from 18% in 1996 to less than 1% since 2003. We also called for a national prevention campaign aimed at 18-24 year old men and underlined the importance of the public having somewhere to report.

The inquiry considered three key areas:

1. Government policy related to the protection of children from sexual abuse facilitated by the internet.
2. The relevant statutory and regulatory framework applicable to ISPs, online platforms and other relevant software providers.
3. The response of ISPs, online platforms and others to child sexual abuse facilitated by the internet.

The inquiry's report was published in March 2020.

DNS over HTTPs:

Nineteen of the IWF's Parliamentary Champions signed an open letter, published in the Sunday Times in August, calling on DCMS Secretary of State, Rt. Hon. Nicky Morgan MP, to address the issues the new form of encryption posed to the safety of children and the effectiveness of the IWF's URL List.

IWF and the European Union:

In June our Policy and Public Affairs team attended a European Commission consultation on the effectiveness of blocking. We also attended the Safer Internet Forum, a European Commission consultation on the Better Internet for Kids programme and conducted a new outreach campaign to expand IWF's reach beyond the UK delegation of MEPs.

Internationally:

The IWF has been involved in updating the ITU's Child Online Protection Guidelines, the development of the Broadband Commission Guidelines and has developed a response to a call for evidence from the UN Rapporteur on the sale and sexual exploitation of children.

Our reporting portals

We're working with countries and territories around the world to provide a tool for people to report online child sexual abuse images and videos. It's simple, low cost, and all reports are then assessed by our world-class analysts in the UK. Reporting Portals are webpages that can be customised to suit the host country or nation and which can be found through links from national organisations and agencies. This helps to make portals a trusted reporting system specific for each nation.

Since 2013, we've helped to set up **29 IWF Reporting Portals** in **4 continents**, providing **1.667 billion people** with a dedicated site to report instances of child sexual abuse imagery online. Thanks to the support of the Global Fund to End Violence Against Children and others, 50 nations worldwide will be provided with this IWF reporting mechanism.

Key milestones of the Reporting Portals project – 2019:

9 roundtable meetings held:

Comoros Islands, The Gambia, Ghana, Madagascar, Mongolia, Pakistan, Senegal, Sierra Leone, Ukraine.

4 Reporting Portals launched: Comoros Islands, The Gambia, Liberia, Nepal.

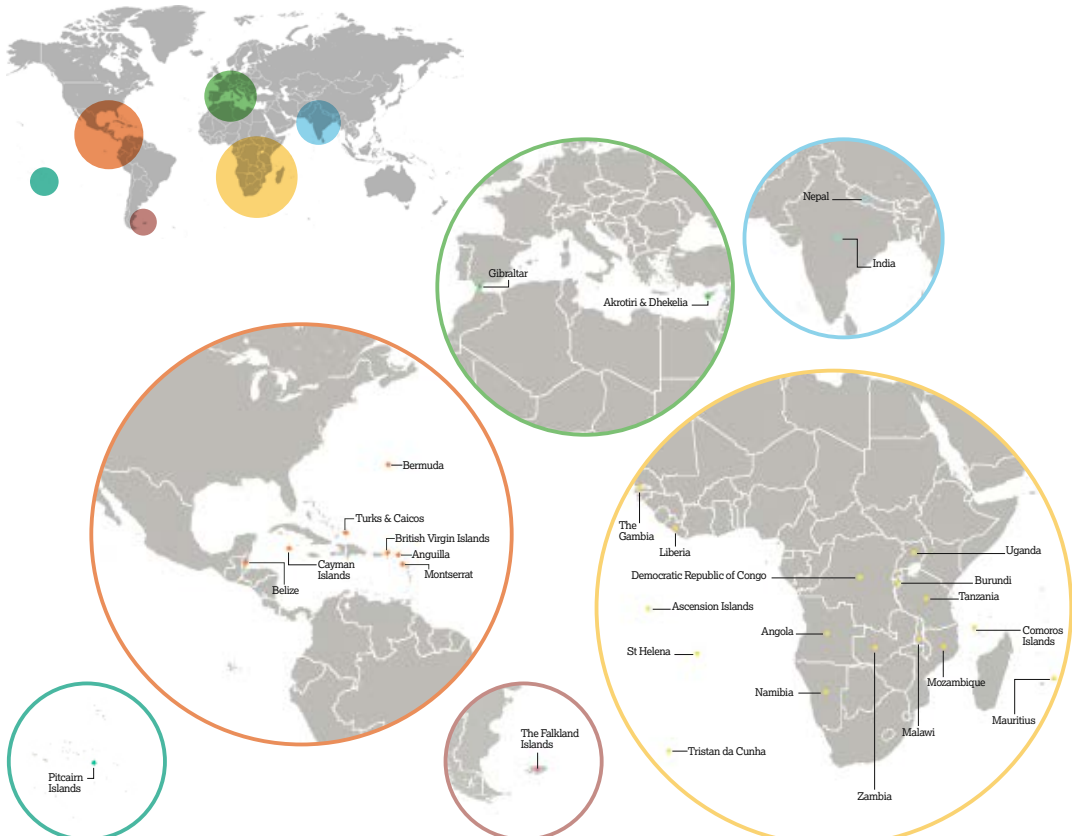
9 languages featured: English, French, Hindi, Lingala, Nepali, Portuguese, Spanish, Swahili, Urdu.

4 continents with IWF Reporting Portals: Europe, Africa, Asia, Americas.

1.667 billion people now have a dedicated IWF Reporting Portal.

The 29 portals are incorporated into the INHOPE network.

IWF Reporting Portal locations



Nepal

The Nepali Portal launched as a joint initiative of the IWF and a consortium of three organisations: Forum for Digital Equality, the Internet Society Nepal, and the Centre for Law and Technology and Delta Law. The Online Child Safety website, launched as part of this partnership to host the portal, also provides psychological counselling, and technical and legal assistance for online child abuse cases.

It was thanks to the peer support of Aarambh Initiative, the portal host in neighbouring India, that Nepal launched its portal in record time. The expedited launch reflected an urgency to tackle child sexual abuse in the country, and the IWF was chosen as a key partner because it is internationally recognised as a leader in this field.

Since the launch, the Nepali Telecommunications Authority has been working on Online Child Safety Directives and the three host organisations have been involved in the draft proposal. A police cybercrimes unit has also been created to combat these crimes.

Despite the infancy of online child protection measures in the country, the timely launch of the portal has been crucial to showing the country's commitment to tackling these crimes. Drawing experience from neighbouring partners has also meant that Nepal is rapidly creating a strong safety environment that will undeniably help protect all Nepali children.

“The Reporting Portal launched in Nepal by Online Child Safety Initiative, a consortium initiative led by Forum for Digital Equality, and the IWF not only provides courage, inspiration and a solution to report and fight against the online abuse of children, but has also become a great platform for sharing knowledge, enhancing capacity and building trust among all stakeholders.”

Babu Ram Aryal

Executive Director, Forum for Digital Equality.



Nepal launch: IWF CEO Susie Hargreaves, Coordinator of the Online Child Safety Initiative and the Treasurer of Forum for Digital Equality Kamala Adhikari, Executive Director Forum for Digital Equality Babu Ram Aryal, and IWF Policy and Public Affairs Manager Michael Tunks.

Liberia

Launching on Safer Internet Day, the Liberian Reporting Portal was the result of a partnership between the IWF, the Liberian government, Liberia's Defence for Children International (DCI) and GSM service providers Orange Liberia. The Liberia National Police (LNP) and the Liberia Telecommunications Authority (LTA) are also supporters of the initiative.

It is the first reporting system on children's issues in West Africa and a pioneering initiative in a country where 95% of children now use the internet, and where almost 44% of the population is under 14 years old. The second most common crime in Liberia is sexual abuse, of both children and adults, but mainly children.

The promotion of the portal on social media produced over two million impressions and reached 425,000 people, while the media reach of this historic event was 2.8 million people across different Liberian media. These activities were complemented with an SMS campaign led by Orange and LoneStar Cell MTN, who sent a message to customers with information about the portal. Liberia has a mobile penetration of approximately 75%. The initiative was inspired by the successful nationwide SMS campaign trialled in the Zambian Portal launch last year.



Liberia portal launch with legal officer at DCI-Liberia Joseph M. Tegli, IWF Development Director Emma Douglas, Executive Director Defence for Children-Liberia Foday M. Kawah, IWF Development Manager Will Few.

“I think it is a good thing for the children of Liberia, owing to the fact that 95 percent of children in Liberia are online users, their protection matters, and we are glad that this is coming to Liberia. At the level of the children’s parliament, we have come across several cases of online abuse.”

Jutomue Doetein

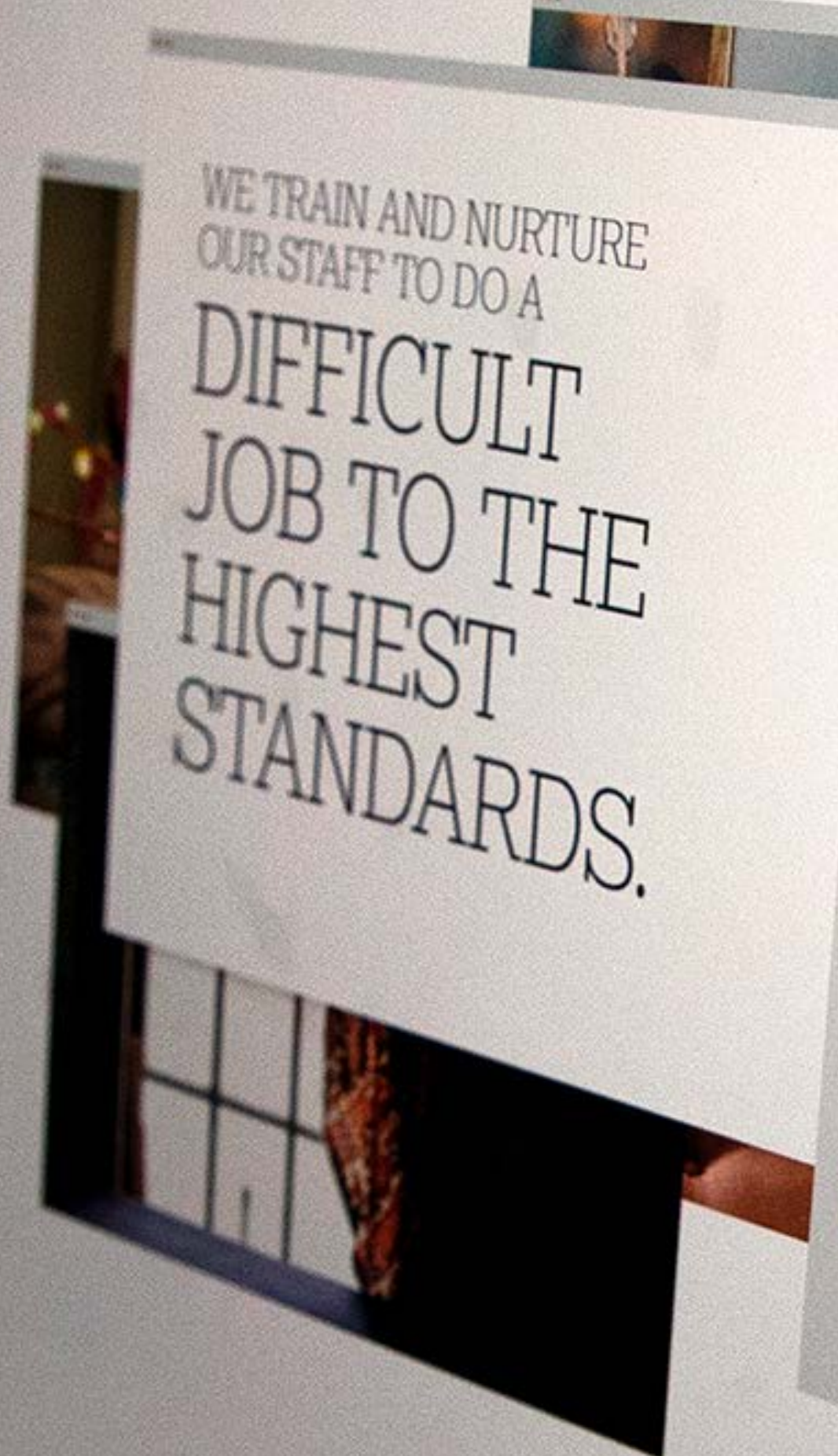
Speaker of the Liberian Children’s Parliament

“In more instances, children are the victims of internet abuse. Child offenders take advantage of the internet to exploit children around the world which Liberia is no exception.”


Foday M. Kawah

Head of DCI





WE TRAIN AND NURTURE
OUR STAFF TO DO A
DIFFICULT
JOB TO THE
HIGHEST
STANDARDS.



Our Members include hundreds of technology companies who value our unique independence – our tools and services can be used with confidence by all.

We work closely with the National Crime Agency and local police forces to provide training and datasets to alleviate the burden of assessing child sexual abuse imagery.

Our worldwide portals help countries with fewer resources to access our technology and advice. That's who.

Caring for our staff

At the IWF, people are at the heart of everything we do. So we give them the best care we can.

IWF may operate in a highly advanced technological world, but it's the expertise and experience of our analysts that sets us apart. They see more distressing images in a day than most see in their lifetime. It takes a special person to be able to view these images without losing their compassion and concern.

Just 13 analysts assessed more than 20,000 reports each in 2019. Whilst they're highly trained to identify criminal imagery, they're exposed to all sorts of hideous content they often don't expect to see, and images that can unexpectedly impact them more than others.

At the IWF, we have a gold-standard welfare system in place.

All new analysts go through a specially developed induction training programme to help them mentally process and cope with exposure to disturbing images. This was recently described in an independent audit as "outstanding".

Our analysts' working hours are strictly monitored; they take regular timetabled breaks and are encouraged to take more breaks as and when they need. All our staff work shorter days to ensure their personal lives don't suffer, and we don't allow overtime.

Each month they have individual mandatory counselling sessions and all employees who see criminal imagery have a full psychological assessment every year. In fact, everyone who works for us is offered counselling support.

The recruitment of our wonderful, resilient analysts is a strict process. And we put considerable thought into how we look after them. An independent inspection of our Hotline described our welfare programme as 'exemplary'. Find out more on page 27.



Heidi Kempster
Deputy CEO and COO

UK Safer Internet Centre

The UK Safer Internet Centre is a partnership of three charities which exists to make the internet a better place for children and young people.

Partly funded by the European Commission, we are one of 31 centres in the INSAFE network. We encourage the responsible use of technology and support making the internet a safer place. We do this through providing three elements:

1. **Hotline**
To anonymously and safely report and remove online child sexual abuse imagery and videos, wherever they are found in the world.
iwf.org.uk
2. **Helpline**
Offering independent advice to professionals working with children and young people on online safety issues such as privacy concerns, inappropriate behaviour and grooming. In 2019, the service was expanded with the launch of Report Harmful Content.
swgfl.org.uk
reportharmfulcontent.com
3. **Awareness Centre**
Providing advice and support to children and young people, parents and carers and schools on a host of subjects including online safety, cyber bullying and social networking.
childnet.com

Safer Internet Day

Safer Internet Day is a global event, celebrated in more than a hundred countries. It calls on children, young people, parents, carers, teachers, social workers, law enforcement, companies, policy makers, and other stakeholders, to join together in helping to create a better internet.

In 2019 it was themed:
“Together for a better internet”.

Nearly half of all UK children aged 8 to 17 heard about Safer Internet Day and as a result:

- 4 in 5 felt more confident about what to do if they were worried about something online;
- 4 in 5 were more aware of the importance of asking for permission before sharing content about others;
- 1 in 5 spoke to someone about something that had been worrying them online.



Our Members

£79,590+



£39,000+

£27,060+



£15,180+



£5,305+



£2,650+



Members who provide in kind support



£50,000+



£21,235+



£10,615+



£1,060+



THE

THE THE
RESU RESU

RESU RESU




THE

THE
RESULTS

RESULTS

RESULTS

RESULTS



THE EXPLOITATION OF
CHILDREN SUFFERING SEXUAL
ABUSE HAS REDUCED.

WE HAVE REMOVED
MILLIONS OF
IMAGES AND
VIDEOS ON OVER
132,000 WEBPAGES
IN 2019.




In 1996, nearly 20% of the world's child sexual abuse material was hosted in the UK. Because of our work and partnerships, it currently stands at 0.1%.

We have helped to remove over 15,000 websites that monetise the sexual abuse of children in 2019.

In 2019 alone 129,000 unique web addresses were added to our list that helps to block this material.

We have created nearly half a million digital fingerprints of duplicate images to help find and remove them from the web.



IN 2019 OUR WEBCRAWLER

SCANNED

NEARLY

72 MILLION

WEBPAGES

AND TWO THIRDS OF A
BILLION IMAGES IN SEARCH
OF THESE DUPLICATES.



Each of our reports contains up to 99 pieces of data and we benchmark our year-on-year records of child sexual abuse imagery across the world. A notice shown to visitors of these sites has led to more than 21,000 people seeking help for their behaviour since 2015.

Highlights and awards

January

Summit in Addis Ababa: Susie Hargreaves attended the African Union to plan a summit to tackle online child sexual exploitation as part of a Home Office delegation representing the WeProtect Global Alliance.

February

Safer Internet Day: With the theme “Together for a better internet,” the campaign in the UK focused on empowering young people to take control of their digital lives and consider how consent works in an online context.



Liberia: IWF launched a web-based reporting system through which the citizens of Liberia can fight online child sexual abuse imagery – with help from expert analysts in the UK.



March

UKSIC public report: The report highlights the progress and achievements the centre has made in making the internet a better and safer place for all.



April

Baroness Floella Benjamin blogs for IWF: “I’m proud to feel part of this unique team, doing what they do for all of us, for our children and for society itself.”



May

Mental Health Awareness Week: Heidi Kempster our COO highlights how IWF provides wellbeing support for our staff.



Woman’s Hour: Our CEO Susie Hargreaves joined BBC’s Woman’s Hour and talked about how we’re seeing more and more self-generated child sexual abuse imagery of girls aged 11-13.

Fred at Buckingham Palace: Our Deputy CEO & CTO Fred Langford attended a Garden Party at Buckingham Palace honouring individuals who have made a positive impact on their community.



June

Independent Inquiry into Child Sexual Abuse (IICSA): Our CEO Susie Hargreaves gave evidence at IICSA as a core participant.

Prestigious award: Civil Society Media honoured IWF staff in its annual awards programme created to recognise and reward “exceptional work” in all areas of charitable activity.



Exposing child victims:

The catastrophic impact of DNS-over-HTTPS: we launched a campaign to highlight the importance of ensuring the safety of children isn't sacrificed for privacy and security.

July**#SoSockingSimple wins ISPA best PR campaign:**

#SoSockingSimple, a campaign to educate young men to navigate safely online, wins an ISPA award.

Hackathon event: IWF and Banco Santander came together again to host the second IWF Online Child Safety Hackathon in London.

10th Asia Pacific Regional Internet Governance Forum:

Our International Development Manager Valentina Picco discussed IWF Reporting Portals in Russia.

August

MP visits IWF: Vicky Ford MP visited IWF to learn about our work and seek advice on how best to combat cyber flashing.



Sunday Times publishes open letter: Nineteen IWF Parliamentary Champions and supporters signed an open letter to the Secretary of State at DCMS explaining their concerns about the new encryption standard known as DNS over HTTPS.

September**The Cambridge International Symposium on Economic Crime:**

Our Technical Projects Officer Sarah Smith joined a panel discussion to raise awareness of trends in the distribution of child sexual abuse material on the dark web.

October

Experienced Leaders: Susie Hargreaves attended a Windsor Leadership Programme meeting leaders from all walks of life.



Honorary Doctorate: Fred Langford, IWF Deputy CEO & CTO was honoured for his child protection and cybersecurity work by the University of Suffolk.



UK Internet Governance Forum: Our Chair Andrew Puddephatt joined a panel discussion on policy and technology.

November**#NoSuchThing campaign:**

The #NoSuchThing as child pornography campaign launched to raise awareness of the importance of terminology.

ICANN: Our Policy and Public Affairs Manager Michael Tunks joined the ICANN conference in Montreal to highlight how we can help the domain sector to fight child sexual abuse imagery.

INTERPOL: Our Technical Projects Officer Sarah Smith attended the 37th meeting of the INTERPOL specialist group on crimes against children.

A meeting with the Pope:

Susie Hargreaves attended the interfaith conference on "Promoting Digital Child Dignity" and met Pope Francis at the Vatican.



© Servizio Fotografico Vaticano

December**Landmark data sharing agreement:**

With the USA's National Center for Missing and Exploited Children (NCMEC) we announced a landmark agreement to better protect children whose sexual abuse images are shared and traded on the internet.

WePROTECT Global Alliance:

Susie Hargreaves attended a summit in Ethiopia to tackle online child sexual exploitation.



Statistics and trends

Our annual report gives you the latest data on what's happening globally to tackle child sexual abuse images and videos online. Please use our statistics to help inform your work.

In 2019, we assessed a webpage every two minutes. Every four minutes, that webpage showed a child being sexually abused.

People report to us at iwf.org.uk, or through one of the 29 portals around the world, in multiple languages. All reports are assessed at our headquarters in the UK. We also actively search the internet for child sexual abuse imagery.

Total number of reports

260,426 reports were assessed by IWF in 2019: 260,309 were reports of webpages and 117 were reports of newsgroups.

132,730 reports were confirmed as containing child sexual abuse imagery or UK-hosted non-photographic child sexual abuse imagery. This is a 25% increase from 2018.

Child sexual abuse imagery reports

132,676 URLs (webpages) were confirmed as containing child sexual abuse imagery, having links to the imagery, or advertising it.

Additionally, 54 newsgroups were confirmed as containing child sexual abuse imagery.

Where all our reports came from	No of Reports assessed*	% of total	No of reports actioned**	% of total	Total actioned**	% actioned**
IWF analysts' proactive search	147,450	57%	114,119	86%	114,119	86%
Public	108,773	42%	14,910	11%		
Police	3,672	1.4%	3,466	3%		
IWF Members (see p38)	266	<1%	128	<1%		
INHOPE Hotlines	260	<1%	105	<1%		
Other Agencies	5	<1%	2	<1%		
Total	260,426		132,730***		132,730	

The table on the left shows the sources of reports into IWF, and how many of those were assessed as containing child sexual abuse material. Please be aware that not all reports we assess are found to contain criminal imagery within our remit.

*These figures include reports of non-photographic child sexual abuse imagery.

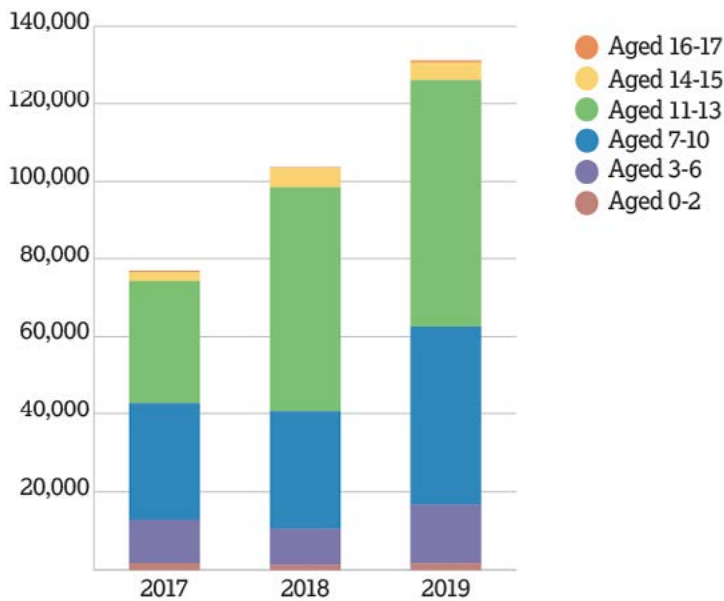
**These figures include reports "actioned" for containing child sexual abuse imagery – found on URLs and newsgroups.

***This figure is 132,676 URLs of child sexual abuse material plus 54 newsgroups showing child sexual abuse material. No UK-hosted non-photographic child sexual abuse material was found.

104,919 reports were assessed by our Hotline which came from external sources and were reported as suspected child sexual abuse imagery. These include all sources not originating from IWF's proactive work. 32% (28% in 2018) of these reports correctly identified child sexual abuse content. This figure includes newsgroups and duplicate reports, which is where several reports have correctly identified the same child sexual abuse content.

The following charts and data tables provide more information on the age and sex of children depicted in the imagery, and the severity of the abuse we saw.

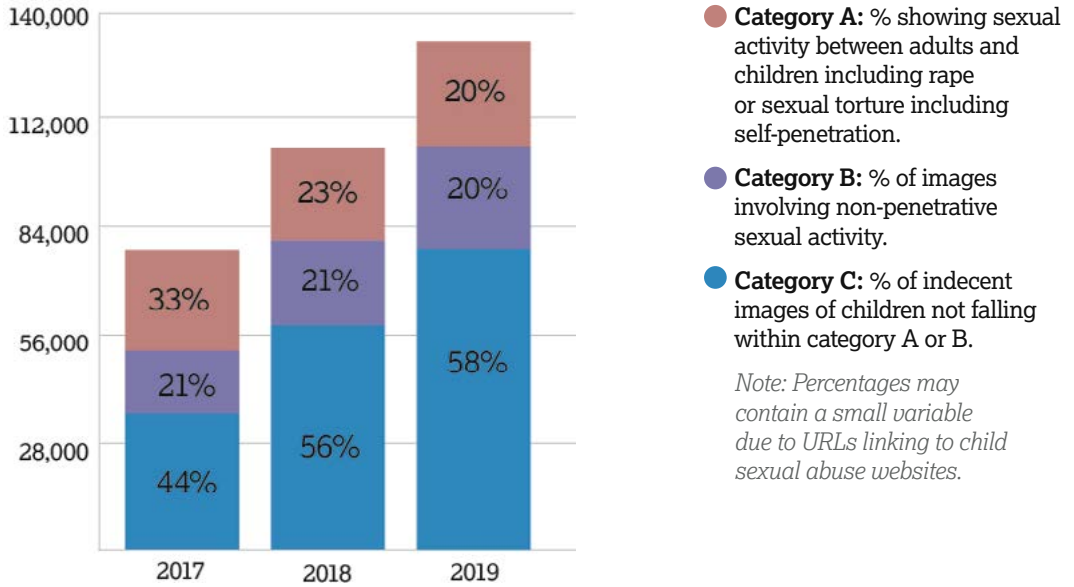
Number of children appearing to be aged 0-17 by year



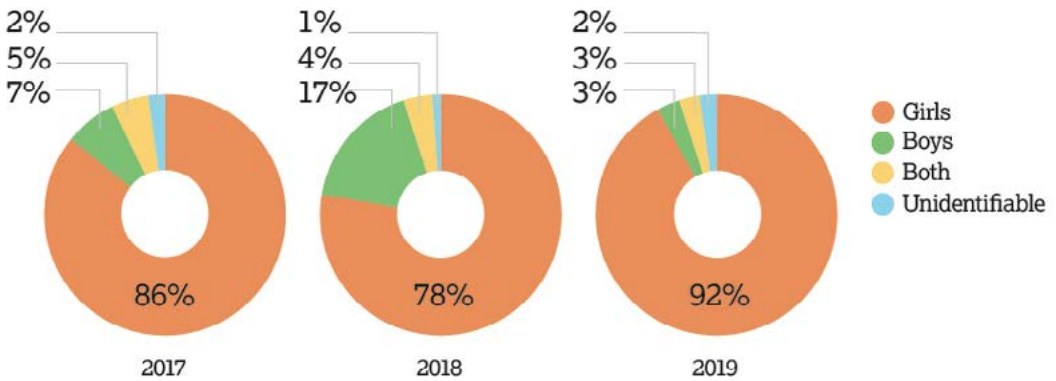
Age	2017	2018	2019
0-2	1,760 (2%)	1,347 (1%)	1,609 (1%)
3-6	10,912 (14%)	9,080 (9%)	15,119 (11%)
7-10	30,217 (38%)	30,156 (29%)	45,744 (34%)
11-13	31,517 (40%)	58,007 (56%)	63,533 (48%)
14-15	2,249 (3%)	4,732 (5%)	4,450 (3%)
16-17	284 (0.4%)	207 (0.2%)	460 (0.3%)

Note: A number for each year were adverts or links to child sexual abuse material.

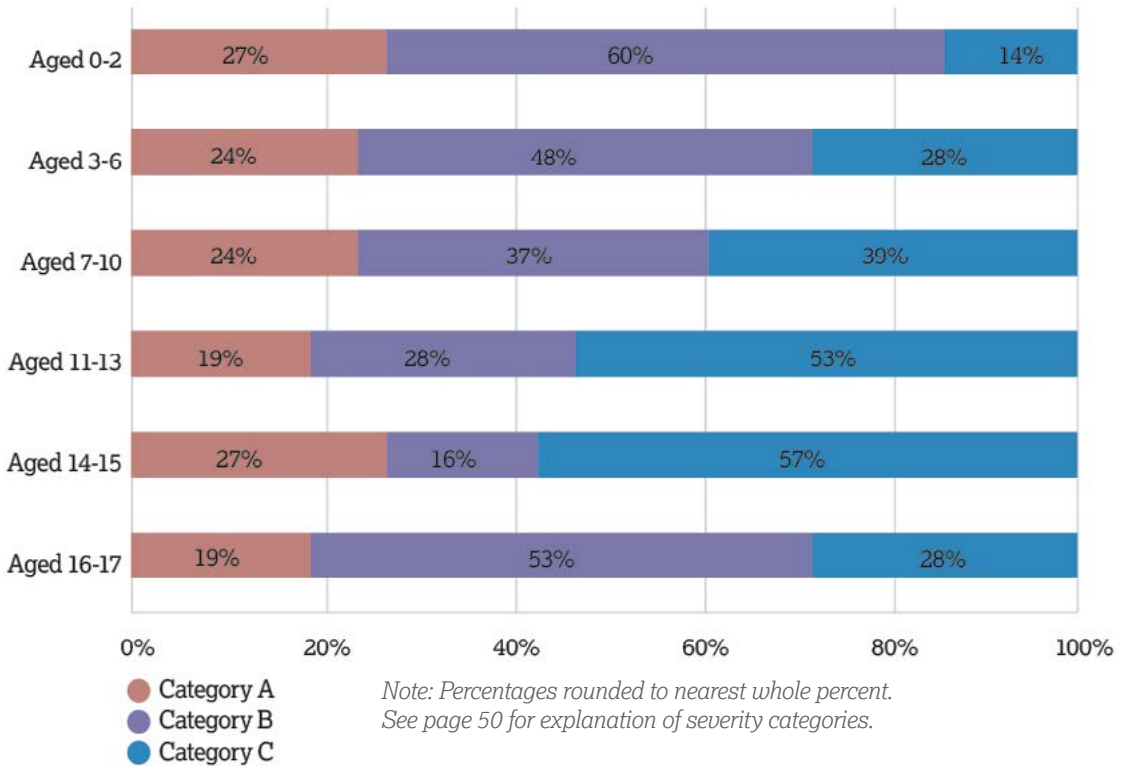
Severity of child sexual abuse



Sex of victims



Analysis of individual image hashes by age of the child and severity of abuse



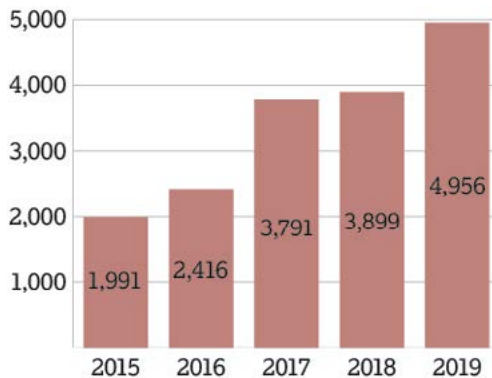
Analysis of the 471,239 hashes on the IWF Hash List at the end of 2019 shows that of the image hashes relating to children assessed as 10 years old or younger, 64% are at the highest levels of severity (Category A or B), compared to 47% of the image hashes relating to children aged 11-17.

Of the image hashes relating to babies and toddlers aged 2 and under, 87% show the most severe forms of abuse. To find out more about what a hash is, and how it helps us in our work, see page 73.

Domain analysis

Number of domains being abused to link to child sexual abuse images and videos

The 132,676 URLs which displayed child sexual abuse imagery in 2019 appeared across 4,956 domains, traced to 58 countries. This is a 27% increase from 3,899 domains in 2018.



The websites containing child sexual abuse content were registered across 168 generic top level domains (gTLDs).

Domain names

Several well-established domains including .com and .biz are known as ‘Generic Top Level Domains’ (gTLDs). Since 2014, many more gTLDs have been released to meet a requirement for enhanced competition and consumer choice in domain names, often in specific categories of content.

We first saw these new gTLDs being used by websites displaying child sexual abuse imagery in 2015. Many of these websites were dedicated to illegal imagery and the new gTLD had apparently been registered specifically for this purpose. New gTLDs being abused for the distribution of child sexual abuse imagery continued to be a trend in 2019.

- Of the 4,956 domains containing child sexual abuse imagery in 2019, 2,063 (42%) were using one of 68 different new gTLDs.
- Across these domains, we took action against 7,609 URLs.

Top 10 TLDs abused to show child sexual abuse material

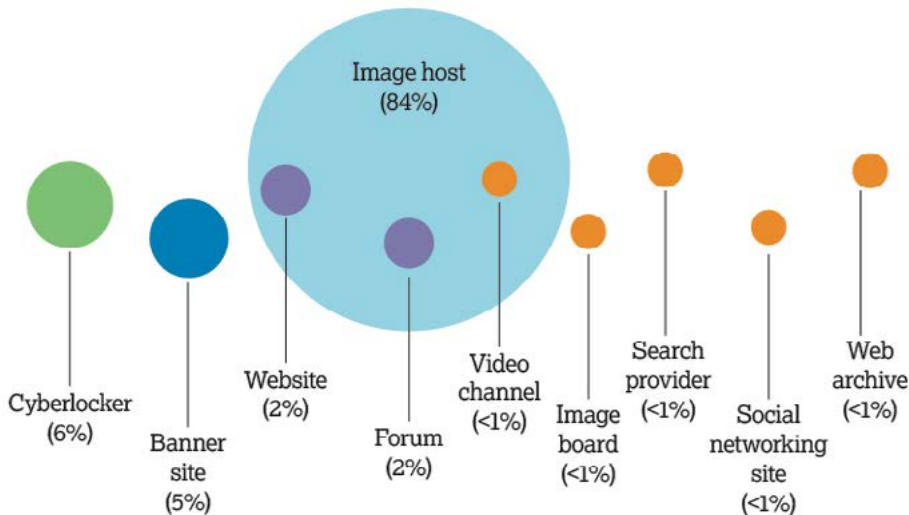
		Figure	%
1	.com	69,353	52%
2	.net	27,172	20%
3	.to	8,798	7%
4	.ru	4,281	3%
5	.co	3,546	3%
6	.me	1,703	1%
7	.fr	1,695	1%
8	.xyz	1,558	1%
9	.nz	1,325	1%
10	.cc	1,321	1%
	Total	120,752	91%

What can we do about this abuse?

Our Domain Alerts help our Members in the domain registration sector prevent abuse of their services by criminals attempting to create domains dedicated to the distribution of child sexual abuse imagery.

During 2020, we’re planning to launch an enhanced Domain Alerts service incorporating a suite of new tools, ensuring technology companies within the domain name sector can act even more efficiently to prevent their TLDs being abused to facilitate the distribution of child sexual abuse material.

Top 10 site types that were abused the most in 2019



See the glossary on p76-77 for explanations of site types

Image hosts are the most consistently abused site types for distributing child sexual abuse imagery.

Offenders distributing this material commonly use image hosts to host the images which appear on their dedicated websites, which can often display many thousands of abusive images. Where our analysts see this technique, they ensure the website is taken down and each of the embedded images is removed from the image hosting service. By taking this two-step action, the image is removed at its source and from all other websites into which it was embedded, even if those websites have not yet been found by our analysts.

Paid for vs free hosting services

In 2019, 125,570 URLs (95%) were hosted on a free-to-use service where no payment was required to create an account or upload the content. In the remaining 5% of cases, the content was hosted on a paid-for service, or it was not possible to tell whether the hosting was free or paid for.

What can we do about this?

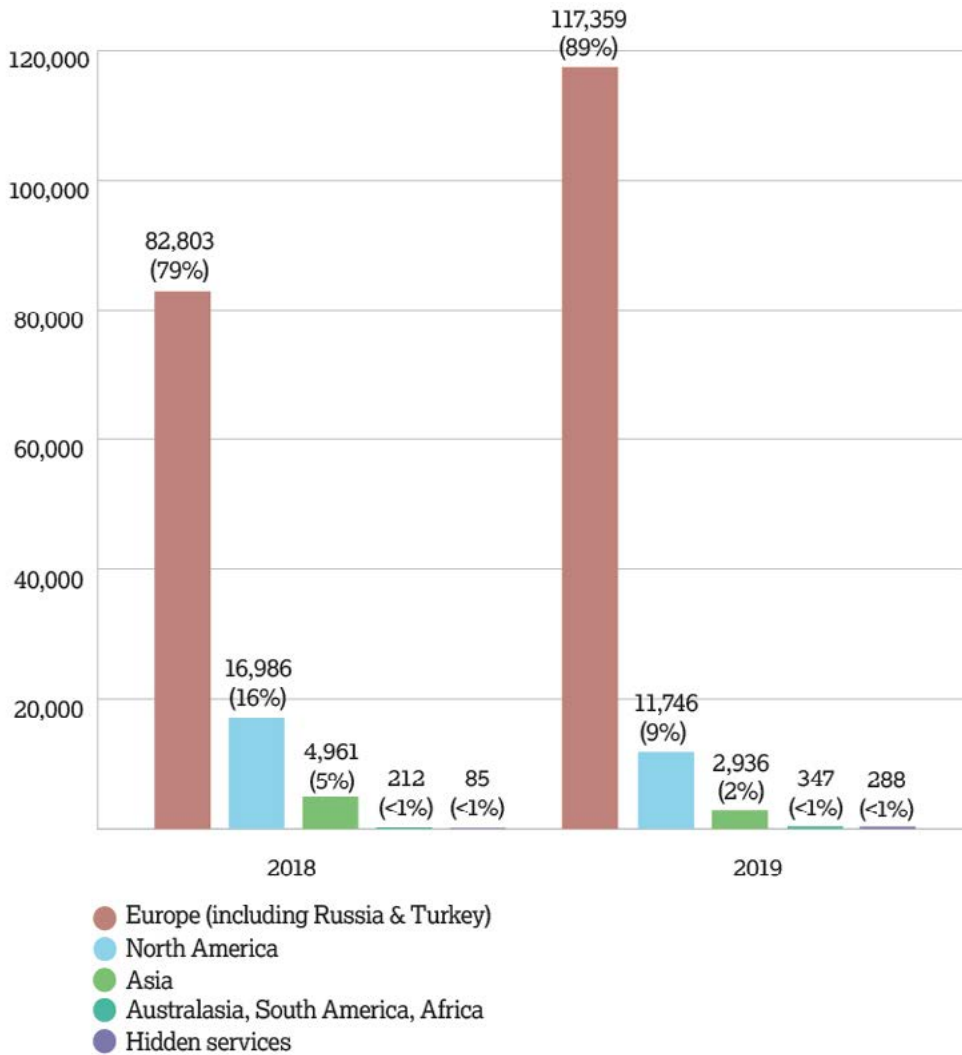
Our award-winning IWF Hash List, launched in 2016, can help image hosts to tackle this abuse by preventing the upload, sharing and storage of known child sexual abuse images and videos. See page 73 for more about our Hash List.

For domain analysis purposes, the webpages of iwf.org.uk, iwf.org.uk/report, and iwf.org.uk/what-we-do are counted as one domain: iwf.org.uk

Geographical hosting of child sexual abuse images

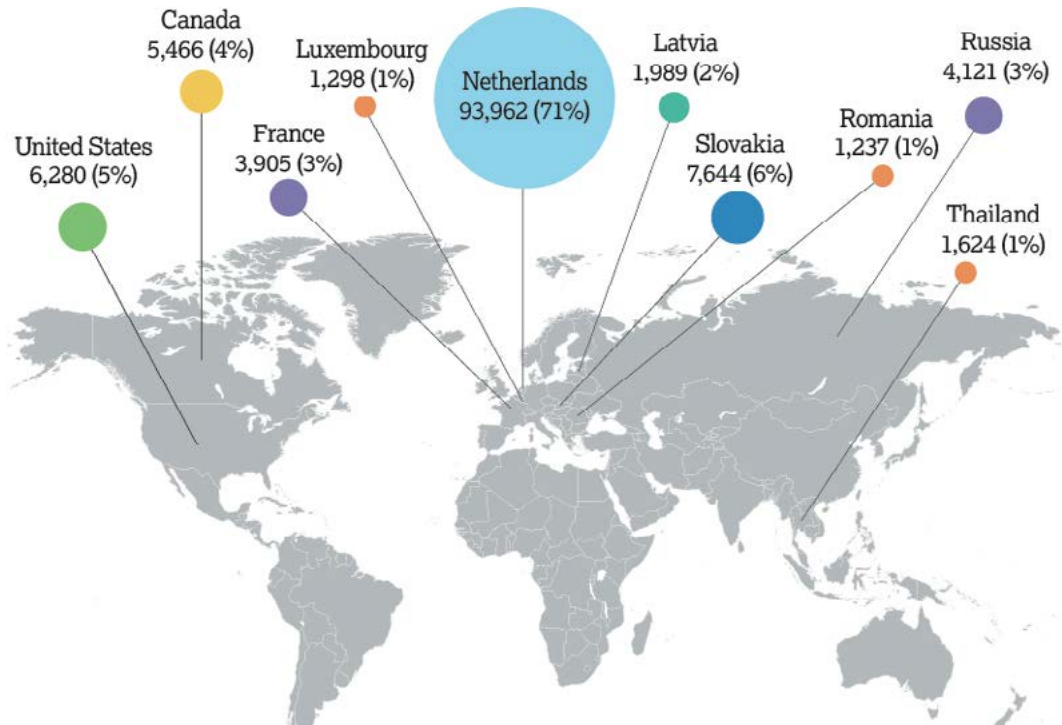
In 2016, we saw that for the first time most child sexual abuse webpages assessed by our analysts were hosted in Europe, which was a shift from North America. Since then, this trend has continued.

Continent hosting of all child sexual abuse URLs



A law in the USA requires technology companies to report any suspected child sexual abuse imagery. This is called mandatory reporting. We see the positive effect of this; over the past few years we've found fewer instances of child sexual abuse hosted in the USA, despite there being a high concentration of internet companies based there.

The top 10 countries for hosting child sexual abuse content



What can we do about this?

As an INHOPE Hotline (International Association of Internet Hotlines) we work closely with all other INHOPE Hotlines around the world to ensure that we alert our partners when we find child sexual abuse content hosted in their country. Our Deputy CEO & CTO Fred Langford is also INHOPE President, and IWF Portals (see page 29) are now included within the INHOPE umbrella.

We also have strong partnerships with countries with no INHOPE Hotline, individual police forces and with INTERPOL. Additionally, we “chase up” our partners if this criminal imagery is not removed quickly. Through doing this we help to speed up the removal of child sexual abuse imagery on a global level.

Trends and patterns

Hidden services

Hidden services are websites hosted within proxy networks – sometimes also called the dark web. These websites are challenging as the location of the hosting server cannot be traced in the normal way.

In 2019 we identified 288 new hidden services, up from 85 in 2018. This is an increase of 238%.

Trend: Commerciality of hidden services

Since 2016, we have seen a rising trend in “commercial” hidden services – dedicated websites offering child sexual abuse imagery for sale.

Of the 288 newly-identified hidden services distributing child sexual abuse imagery in 2019, 197 were assessed as being commercial. Due to the anonymous nature of hidden services, these commercial websites only accept payment in virtual currencies.

Trend: Next-gen or V3

In 2018, we first saw “next-gen” or “v3” hidden services being used for the distribution of child sexual abuse imagery. Launched in late 2017, “next-gen” hidden services use more sophisticated methods of encryption than traditional hidden services, making them harder to locate. This was a rising trend in 2019.

Of the 288 newly-identified hidden services found in 2019, 108 (37%) were “next-gen”, compared to 4 instances (5%) in 2018.

Hidden services commonly contain hundreds or even thousands of links to child sexual abuse imagery that is hosted on image hosts and cyberlockers on the open web.

What can we do about this?

We work with the National Crime Agency (NCA) Child Exploitation and Online Protection (CEOP) Command to provide intelligence on any new hidden services which are displaying child sexual abuse imagery. With this intelligence, NCA-CEOP can work with national and international law enforcement agencies to investigate the criminals using these websites.

What can we do about this?

Our Virtual Currency Alerts enable our Members in the virtual payments sector to identify payments which are associated with child sexual abuse imagery.

What can we do about this?

We take action to remove the child sexual abuse imagery appearing on the open web. Our analysts also add child sexual abuse images and videos hosted in hidden services to the IWF Hash List, helping to prevent wider distribution on the open web. Monitoring trends in the way offenders use hidden services to distribute child sexual abuse imagery also helps us when we are searching for this imagery online.

Trend: Commercial child sexual abuse material

We define commercial child sexual abuse imagery as images or videos that were seemingly produced or being used for the purposes of financial gain by the distributor.

Of the 132,676 webpages we confirmed as containing child sexual abuse imagery in 2019, 15,326 (12%) were commercial in nature. This is an increase on 2018, when we took action against 6,941 (7%) commercial webpages.

Why has there been an increase?

We believe the rise in the number of commercial hidden services (see page 56) in part accounts for the increase of commercial content we've seen in 2019. Hidden services often display thousands of criminal images and videos which are stored on image hosting sites and cyberlockers on the open web.

In 2018, we identified a group of dedicated child sexual abuse websites apparently associated with the same commercial distributor, which are hosted on the open web but which can only be accessed using the Tor browser, which enables people to browse the internet anonymously. If accessed using a normal browser, the website appears to be offline. This technique enables the website to stay live for longer and may also frustrate attempts by law enforcement to investigate the offenders visiting the website, as their identity is masked.

In 2019, we identified 187 commercial websites using this technique to distribute criminal imagery, compared to 86 instances in 2018.

Commercial trend: Web brands

We started the Website Brands Project in 2009. Since then, we have been tracking the different "brands" of dedicated child sexual abuse websites. Dedicated commercial websites are constantly moving their location to evade detection and our analysts see the same websites appearing on many different URLs over time.

Since the project began, we have identified 5,860 unique website brands.

What can we do about it?

In addition to reporting newly identified hidden services to law enforcement for further investigation, we also take action to remove each image and video individually at source.

We continue to monitor these trends and we share information with our sister Hotlines and law enforcement agencies who assist in removing these websites and ensure the distributors can be investigated. We also capture payment information displayed on these commercial websites which helps companies in the financial industry to prevent misuse of their services and disrupt further distribution of the criminal imagery.

What can we do about this?

We analyse hosting patterns and payment information, and through this, we conclude that the majority of these dedicated websites are operated by a small number of criminal groups. We provide this information to law enforcement and relevant technology companies.

- In 2019, the top 10 most prolific brands, which accounted for 25% of all commercial content in 2019, were apparently associated with just 4 distribution groups.

Since 2017, we've seen a trend towards the use of more dynamic commercial websites meaning that the names and titles change each time the page is reloaded. As a result, our analysts devised different methods to establish when these sites still represent the same "brand" despite dynamically changing.

- In 2019, we saw 1,408 active brands, compared to 1,245 in 2018.
- Of these active brands, 375 were previously unknown to us, compared to 446 in 2018.

We will continue to monitor trends and work closely with law enforcement partners and our financial industry Members to ensure the commercial distribution of child sexual abuse imagery is disrupted.

Commercial trend: Disguised websites

Since 2011, we have been monitoring commercial child sexual abuse websites which display child sexual abuse imagery only when accessed by a 'digital pathway' of links from other websites. When the pathway is not followed, or the website is accessed directly through a browser, legal content is displayed. This means it is more difficult to locate and investigate the criminal imagery. This trend for distributors to hide the distribution of criminal imagery has increased in 2019, with criminals continually changing the methods used.

Commercial disguised trend: Abuse of digital advertising networks and legitimate brands

In 2018, we identified a group of disguised websites which are apparently exploiting digital advertising networks and legitimate brand owners to fraudulently generate additional revenue. We've continued to see this trend during 2019.

- Of the 1,408 commercial website brands active in 2019, 807 were using the "digital pathway" technique.
- Of these 807 active brands, 170 had not been seen by us before.

What can we do about this?

It takes more time and expertise to tackle these sorts of websites, and we've adapted our techniques to reveal and remove them in response.

In 2019, we uncovered 3,882 websites using a "digital pathway" to hide child sexual abuse imagery. That's 16 times every working day. It represents an increase of 50% on the 2,581 disguised websites identified in 2018.

What can we do about this?

We've been working with brand owners, the advertising industry, government, and law enforcement to understand more about the problem and what action can be taken to tackle the issue.

By sharing our expertise in uncovering these websites with our sister Hotlines and law enforcement worldwide, we help disrupt the operation of commercial child sexual abuse websites.

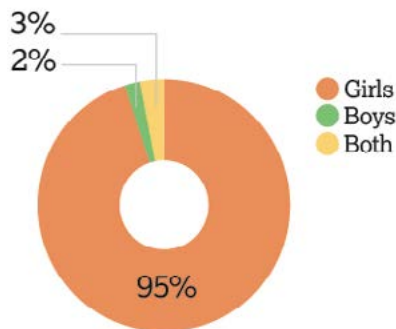
Trend: “Self-generated” content

In recent years, we’ve seen an increase in what is termed “self-generated”^{*} child sexual abuse content, created using webcams and then shared online. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves. Care must be taken not to suggest the child is to blame in any way. Research we’ve previously carried out in this area found that this imagery is frequently being produced through live streaming services and is then captured and distributed widely across other sites. The images and videos predominantly involve girls aged 11 to 13 years old, in their bedrooms or another room in a home setting.

We take this growing trend very seriously.

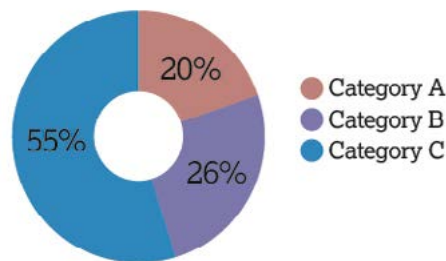
Of the 132,676 webpages actioned during 2019, almost a third (38,424 or 29%) was assessed as containing self-generated imagery. See pages 63 to 69 for a detailed breakdown.

Sex of victims



**Percentages rounded to nearest whole number*

Severity of child sexual abuse



See page 50 for explanation of severity categories

3 in every 4 (76%, or 29,312) images or videos of self-generated child sexual abuse shows a girl aged 11 to 13 years old. For our analysts who assess and remove this imagery, this is 118 times every working day.

13% (5,026) of images or videos showed a girl aged 7 to 10 years old. That’s 20 times each working day.

What can we do about it?

We adapted our bespoke systems to ensure we can continue to capture changes in this trend over time. We identify this imagery and work with technology companies to get it removed.

During 2019, we also commissioned research carried out in partnership with BritainThinks and Zinc Network to understand more about the vulnerabilities which can lead to children falling victim to grooming and coercion. We hosted a roundtable with our partners in the UK Safer Internet Centre which brought together stakeholders from the online industry, child protection, law enforcement, government, academia and technology companies. In 2020, we will launch a campaign to help prevent the creation of self-generated child sexual abuse imagery.

**Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, P43.*

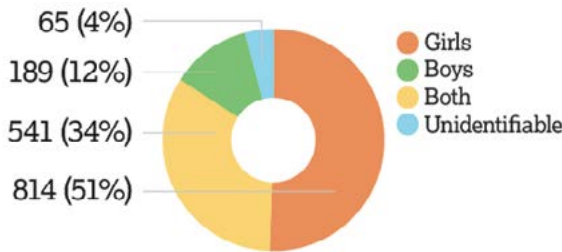
Analysis: Child sexual abuse material by age

Babies and toddlers (0-2 years old)

All the imagery we deal with on a daily basis is difficult to watch, but images and videos featuring babies and toddlers are among the most shocking. It's not unusual for us to see very young boys and girls – sometimes even newborns – being raped and subjected to horrendous sexual sadism at the hands of adults.

As in previous years, we have seen a higher proportion of category A images – the most severe – relating to babies and toddlers.

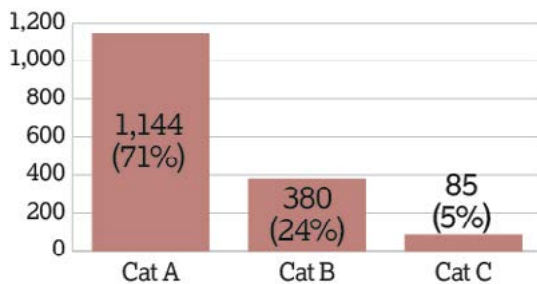
Sex of victims



Type of sites

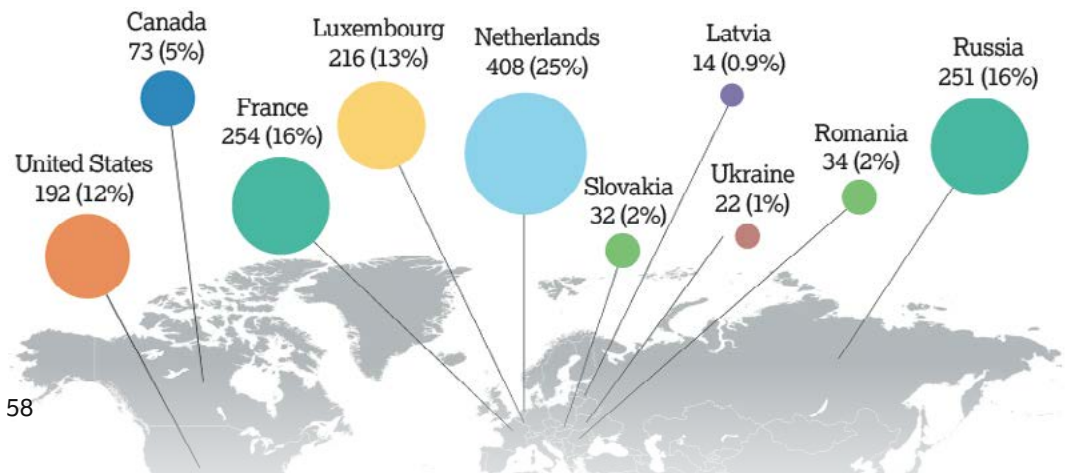
Site Type	Reports	%*
Image Host	585	36%
Cyberlocker	485	30%
Banner	421	26%
Website	38	2%
Forum	19	1%
Web Archive	16	1%
Video Channel	13	0.8%
Social Network	12	0.7%
Blog	6	0.4%
Image Board	5	0.3%
Chat	3	0.2%
Search	3	0.2%
Image Store	2	0.1%
Live Stream	1	0.1%
Total	1609	

Severity of child sexual abuse



*Percentages rounded to nearest whole number

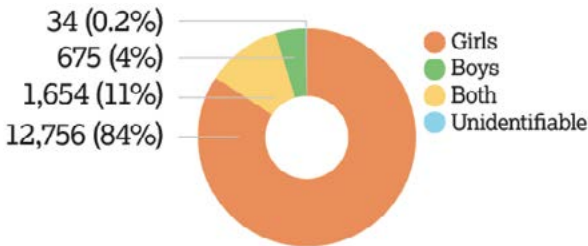
The top 10 hosting locations



Young children (3-6 years old)

As difficult as it is to witness the physical sexual abuse of a child, watching the abuse of their trust is often as heart-breaking. We frequently see images and videos of adults committing the most severe acts of sexual abuse against young children in their care. Often, the children appear to believe that the abuse they're suffering is a normal part of life.

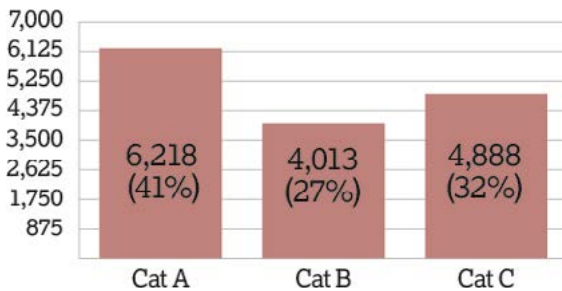
Sex of victims



Type of sites

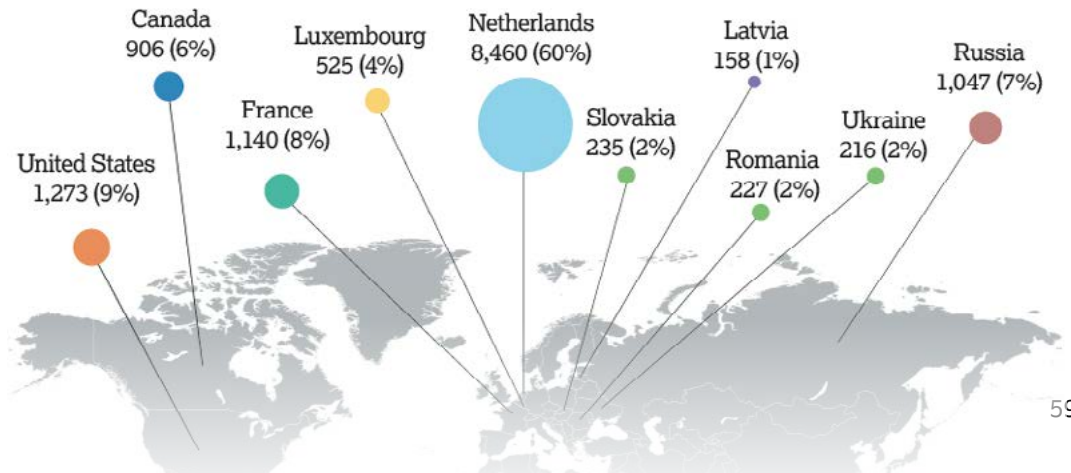
Site Type	Reports	%*
Image Host	10,006	66%
Banner	2,381	16%
Cyberlocker	1,865	12%
Website	284	2%
Forum	185	1%
Web Archive	122	0.8%
Video Channel	78	0.5%
Social Network	59	0.4%
Image board	58	0.4%
Search	36	0.2%
Blog	16	0.1%
Chat	16	0.1%
Image Store	9	0.1%
Redirector	3	0.0%
Live Stream	1	0.0%
Total	15,119	

Severity of child sexual abuse



*Percentages rounded to nearest whole number

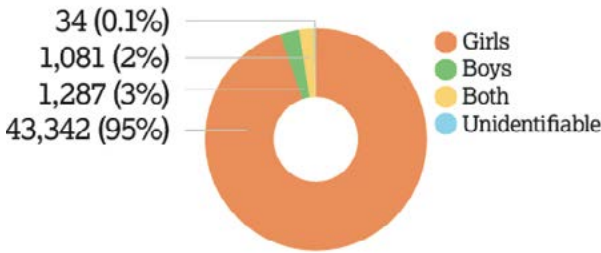
The top 10 hosting locations



Pre-pubescent children (7-10 years old)

Most of the images and videos we see of prepubescent children being sexually abused involve an adult or older child. However, in recent years we've started to see children in this age group being coerced and deceived into sexual activity on live streaming sites, often in exchange for "likes" or other rewards. Typically, children will be encouraged to expose themselves to the webcam and are then asked to perform increasingly severe sexual acts in front of the camera.

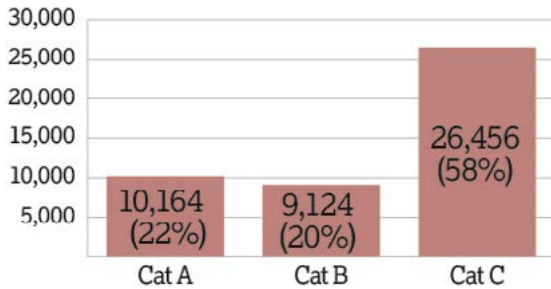
Sex of victims



Type of sites

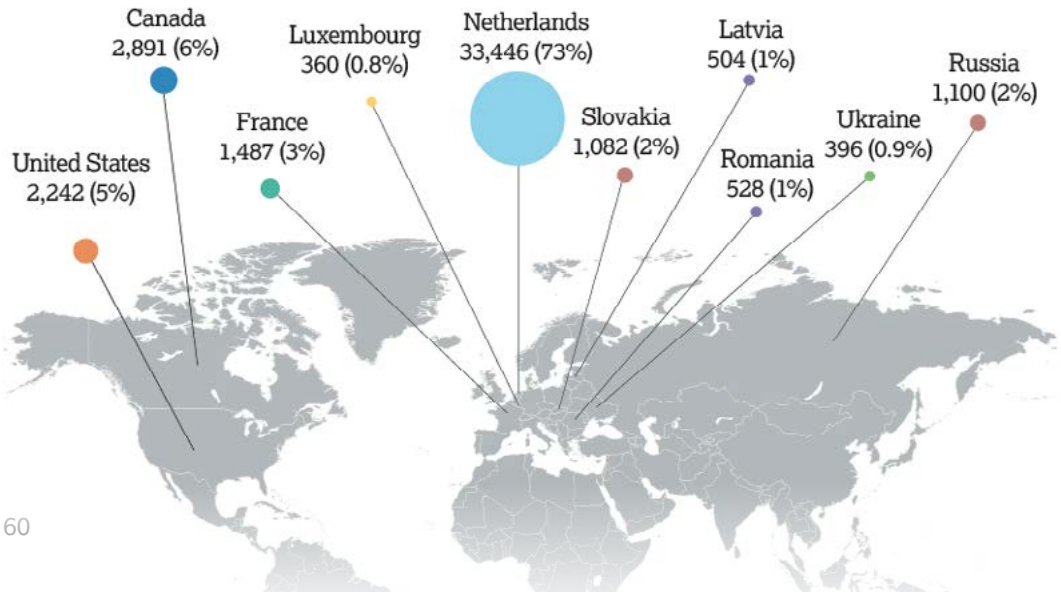
Site Type	Reports	%*
Image Host	38,629	84%
Cyberlocker	2,607	6%
Banner	1,880	4%
Website	873	2%
Forum	735	2%
Video Channel	219	0.5%
Image board	219	0.5%
Web Archive	167	0.4%
Social Network	147	0.3%
Search	132	0.3%
Blog	68	0.1%
Image Store	55	0.1%
Chat	9	0.0%
Redirector	2	0.0%
Live Stream	2	0.0%
Total	45,744	

Severity of child sexual abuse



*Percentages rounded to nearest whole number

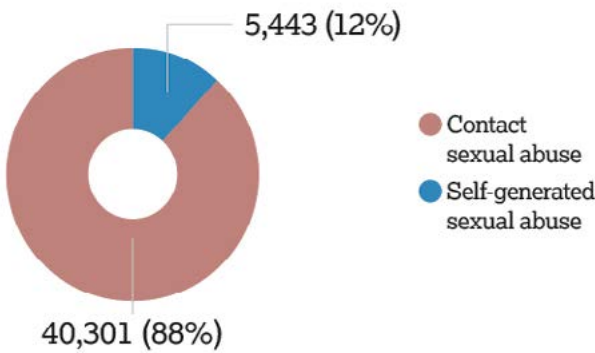
The top 10 hosting locations



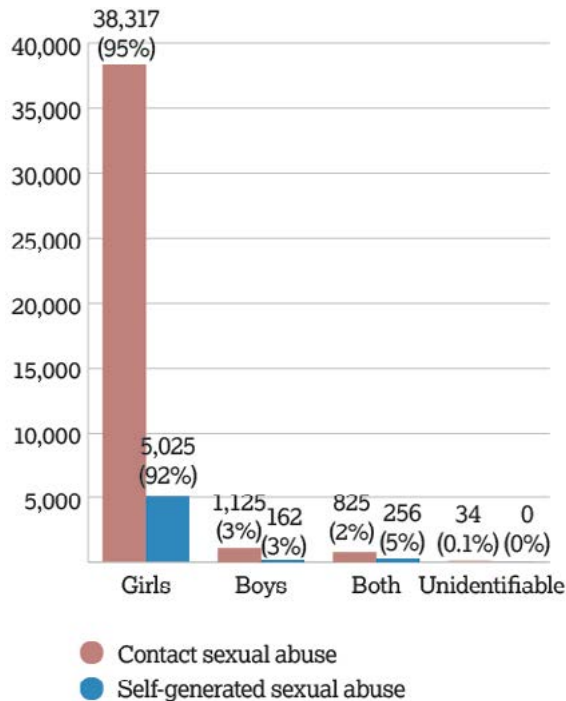
7-10: Self-generated child sexual abuse & contact child sexual abuse

In order to help experts and professionals working in this space, we've provided a breakdown by sex and severity for self-generated child sexual abuse imagery, and contact child sexual abuse imagery.

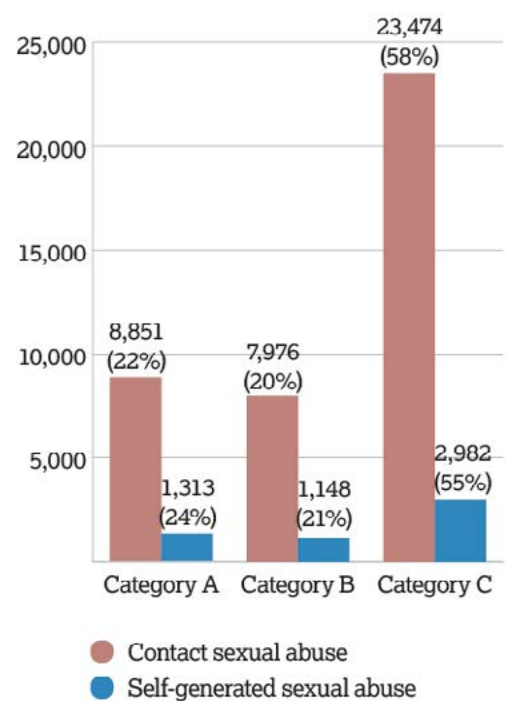
Type of abuse



Type of abuse by sex



Type of abuse by severity

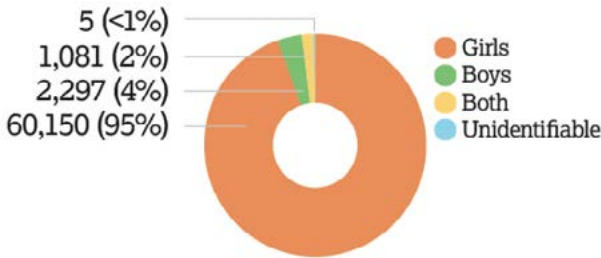


See page 50 for explanation of severity categories

Older children (11-13 years old)

Where we see 11-13 year olds, nearly half of the time it's in “self-generated” child sexual abuse imagery, often created using webcams. Mostly, these are girls who are alone in their bedroom or other home setting. Frequently, these girls are being groomed, extorted or deceived into creating and sharing sexual images and videos online. We've seen situations where the child clearly believed she was in an ongoing relationship with her abuser, and even cases where girls were being blackmailed into more and more extreme activities.

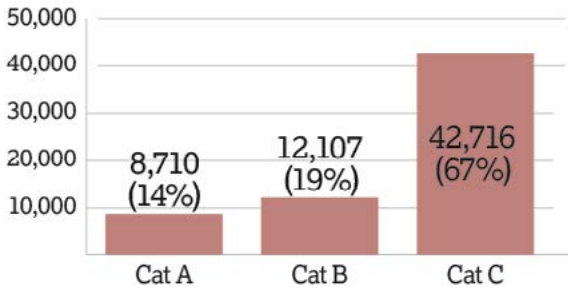
Sex of victims



Type of sites

Site Type	Reports	%*
Image Host	57,735	91%
Cyberlocker	2,422	4%
Forum	1,134	2%
Website	792	1%
Banner	445	0.7%
Image Board	234	0.4%
Search	200	0.3%
Video Channel	196	0.3%
Social Network	182	0.3%
Web Archive	82	0.1%
Blog	77	0.1%
Image Store	27	0.0%
Chat	4	0.0%
Live stream	2	0.0%
Redirector	1	0.0%
Total	63,533	

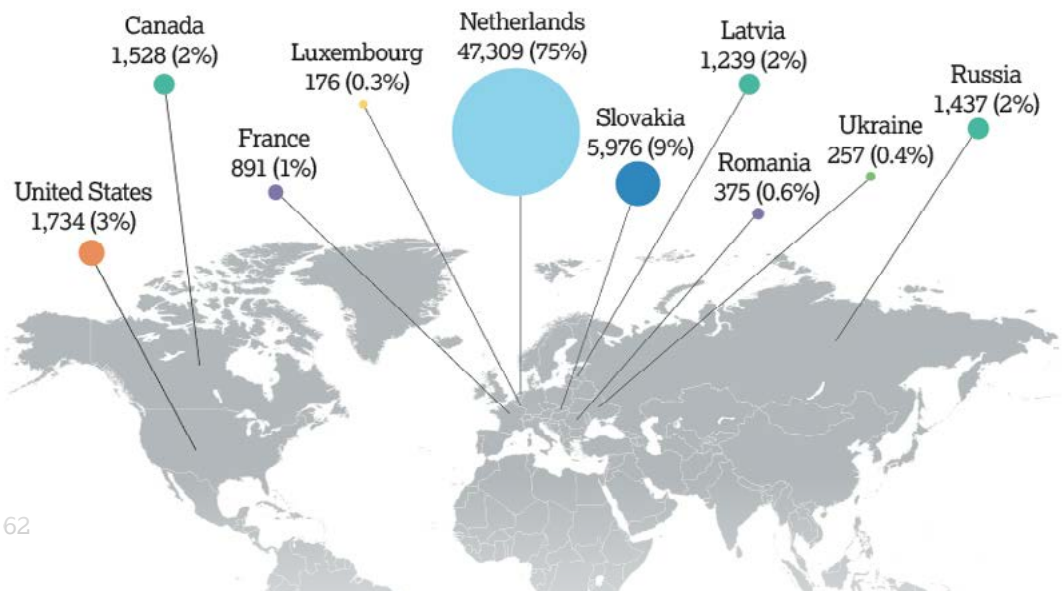
Severity of child sexual abuse



*Percentages rounded to nearest whole number

See page 50 for explanation of severity categories

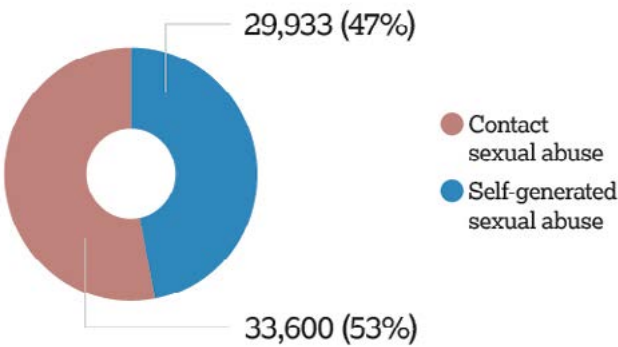
The top 10 hosting locations



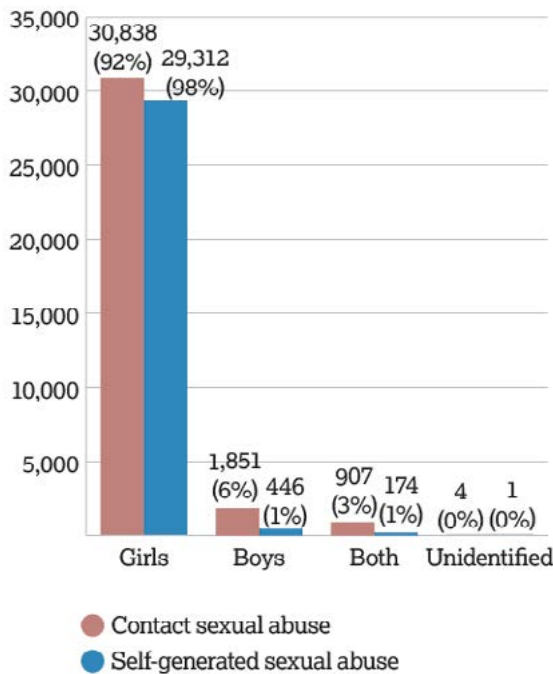
11-13: Self-generated child sexual abuse & contact child sexual abuse

In order to help experts and professionals working in this space, we've provided a breakdown by sex and severity for self-generated child sexual abuse imagery, and contact child sexual abuse imagery.

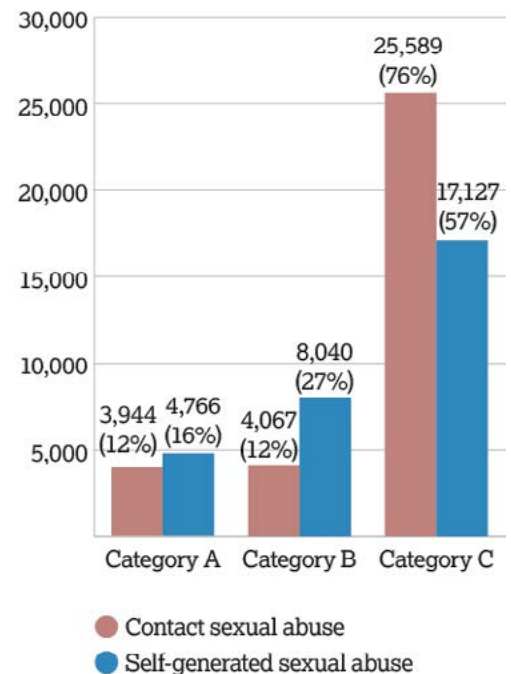
Type of abuse



Type of abuse by sex



Type of abuse by severity

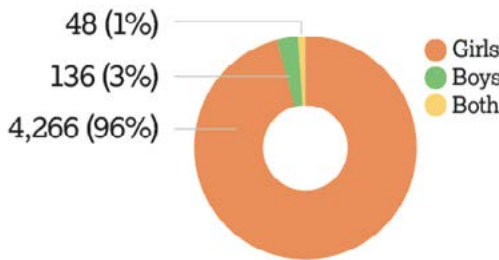


See page 50 for explanation of severity categories

Teenagers (14-15 years old)

One of the major challenges we face in assessing child sexual abuse imagery featuring teenagers (particularly girls) is reliably determining age. This is even harder in the increasing instances we're seeing of self-generated imagery, as the children will often be trying to appear older than they are – by wearing make-up for instance. Sadly, we see this confidence is often exploited by offenders who encourage girls into sexual activity which is being secretly recorded. Too often, it seems the children are not fully aware of the potential long-term consequences; we see the same videos of these children being shared over and over again.

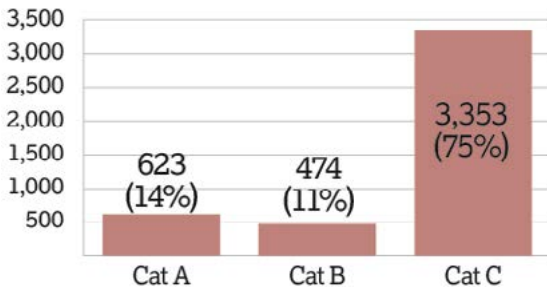
Sex of victims



Type of sites

Site Type*	Reports	%
Image Host	3,982	89%
Website	143	3%
Cyberlocker	94	2%
Video Channel	72	2%
Forum	50	1%
Social Network	31	1%
Search	31	1%
Blog	21	<1%
Image Board	12	<1%
Image Store	5	<1%
Web Archive	5	<1%
Banner	3	<1%
Chat	1	<1%
Total	4,450	

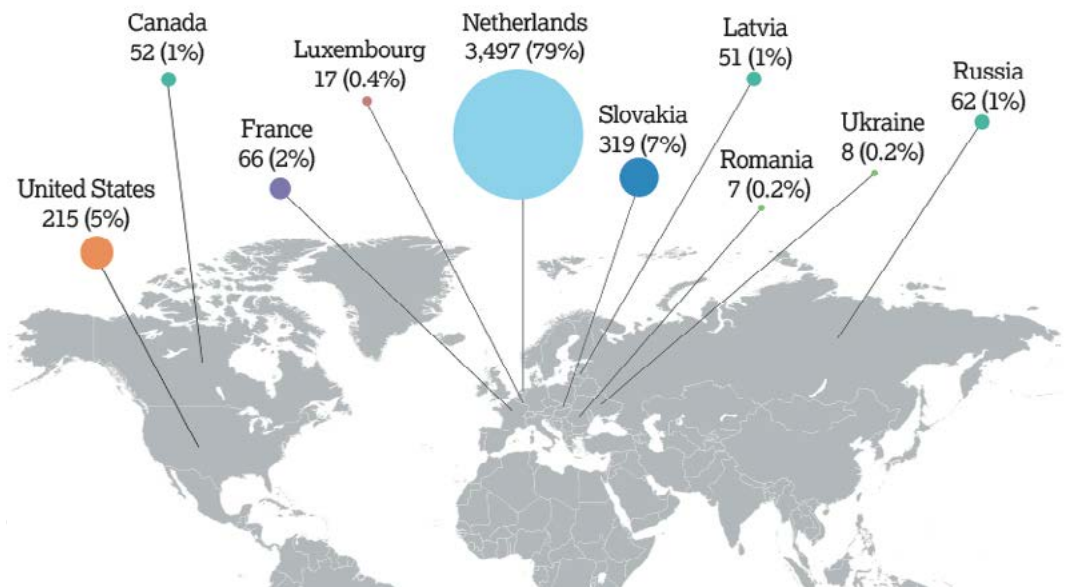
Severity of child sexual abuse



*Percentages rounded to nearest whole number

See page 50 for explanation of severity categories

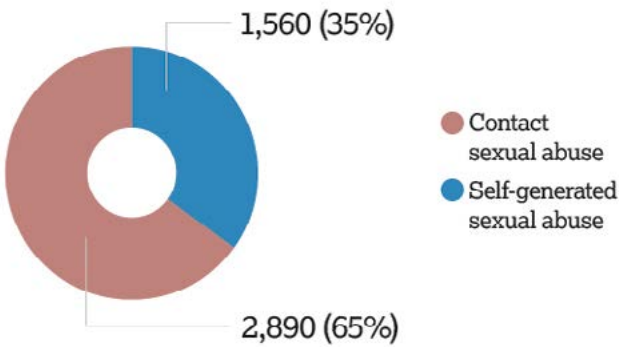
The top 10 hosting locations



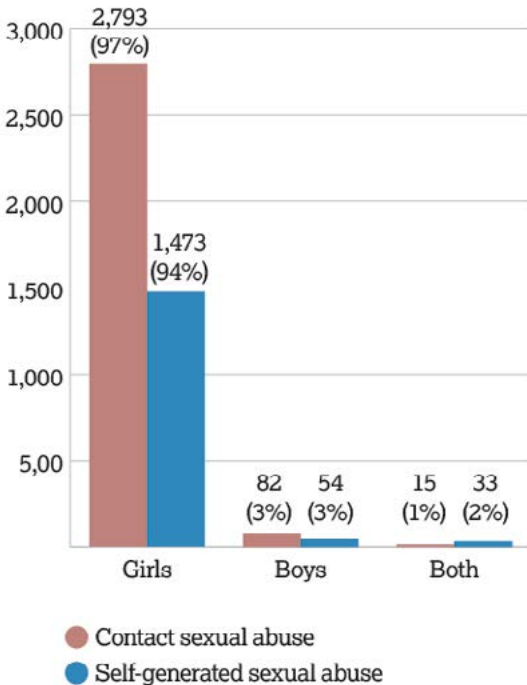
14-15: Self-generated child sexual abuse & contact child sexual abuse

In order to help experts and professionals working in this space, we've provided a breakdown by sex and severity for self-generated child sexual abuse imagery, and contact child sexual abuse imagery.

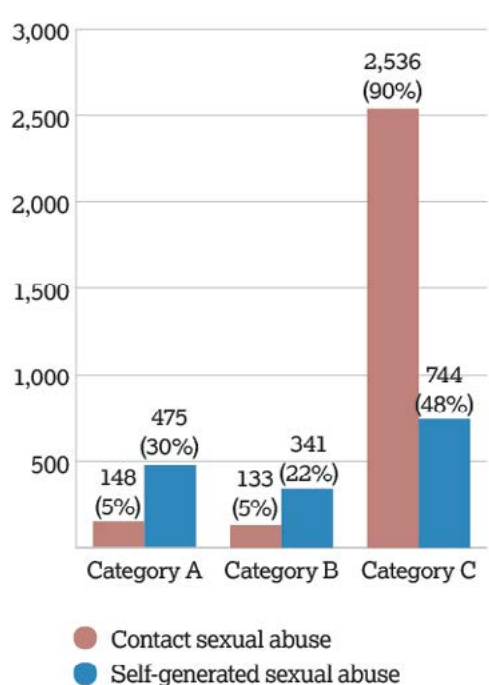
Type of abuse



Type of abuse by sex



Type of abuse by severity

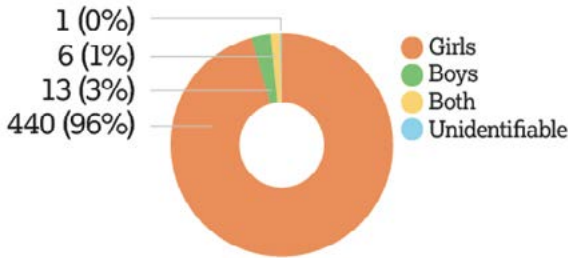


See page 50 for explanation of severity categories

Older teenagers (16-17 years old)

Because of the difficulty in assessing the age of older teenagers, we can only remove sexual imagery of them where we can verify their age. As a result, we generally know the circumstances which led to the content being online. Mostly, the imagery is self-generated and is likely to have been initially shared consensually with a boyfriend or girlfriend. The imagery has then been further shared without their consent which is a huge source of worry and distress. We're so glad that we can help these young people take back control and make sure the images are taken down.

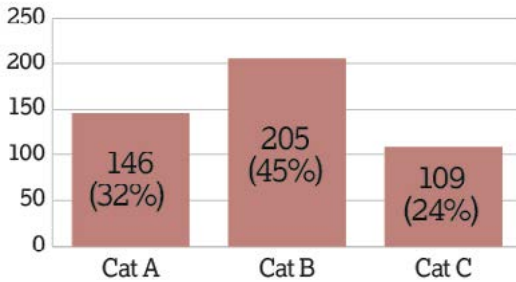
Sex of victims



Type of sites

Site Type	Reports	%*
Image Host	151	33%
Video Channel	101	22%
Search	91	20%
Website	78	17%
Forum	19	4%
Cyberlocker	9	2%
Blog	8	2%
Social Network	2	<1%
Banner	1	<1%
Total	460	

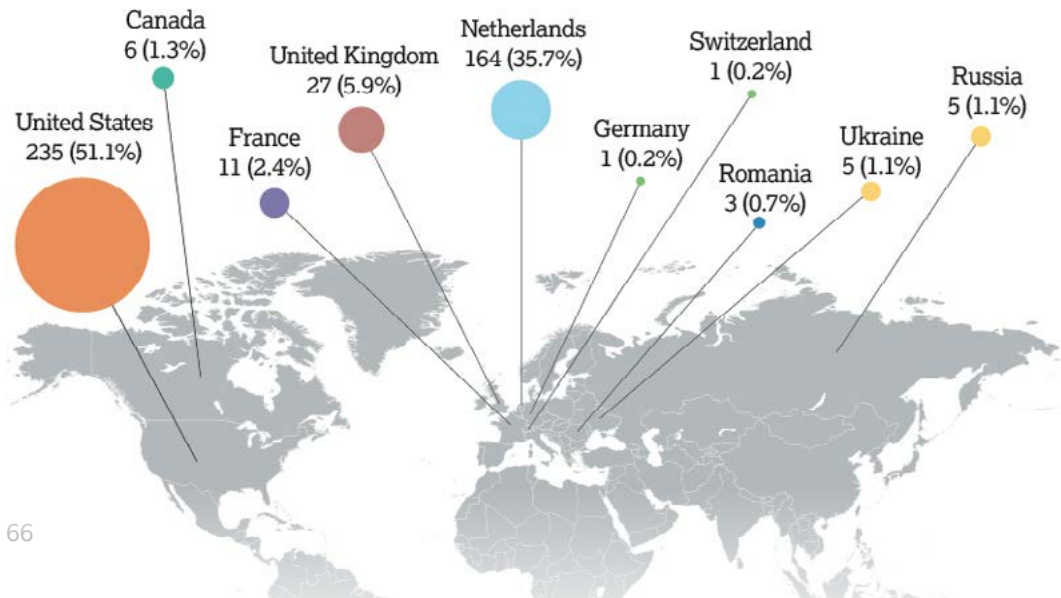
Severity of child sexual abuse



*Percentages rounded to nearest whole number

See page 50 for explanation of severity categories

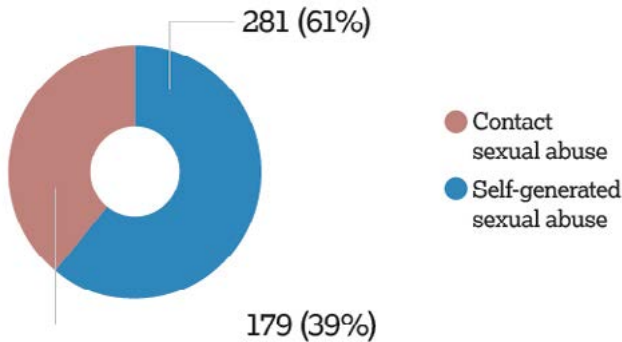
The top 10 hosting locations



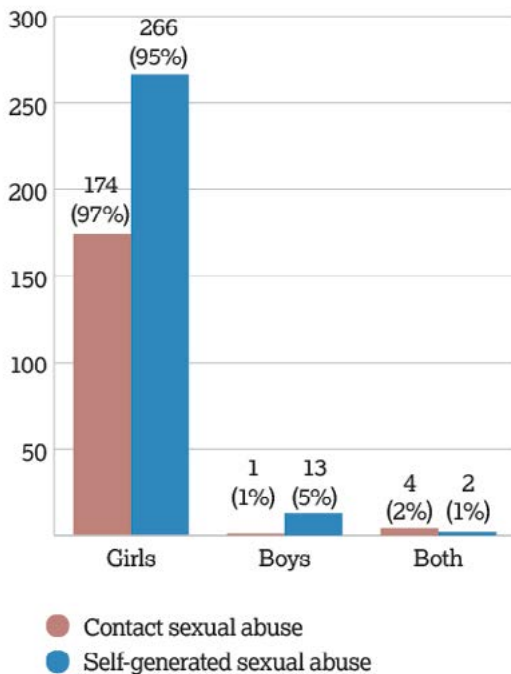
16-17: Self-generated child sexual abuse & contact child sexual abuse

In order to help experts and professionals working in this space, we've provided a breakdown by sex and severity for self-generated child sexual abuse imagery, and contact child sexual abuse imagery.

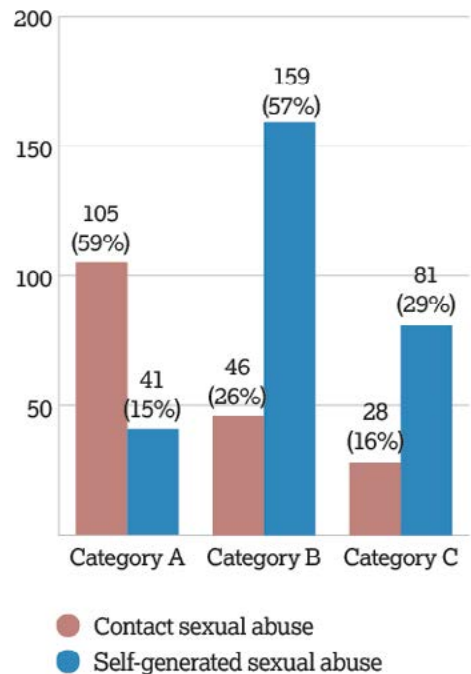
Type of abuse



Type of abuse by sex



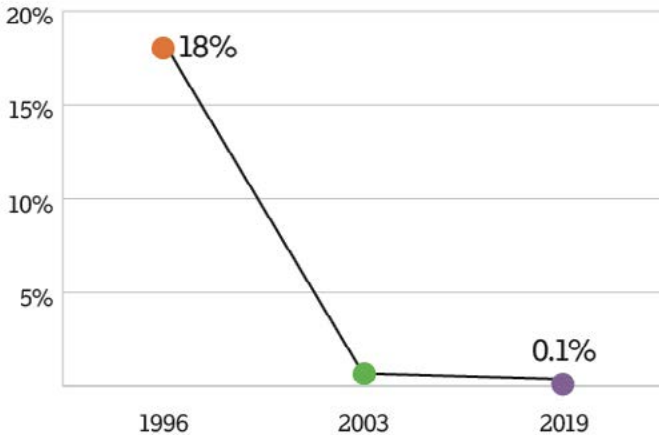
Type of abuse by severity



See page 50 for explanation of severity categories

UK hosting of child sexual abuse imagery

The UK hosts a small volume of online child sexual abuse content. When we were founded in 1996, the UK hosted 18% of the global total; in 2019 this figure was just 0.1%.



In 2019, 158 URLs displaying child sexual abuse imagery were hosted in the UK, an increase of 266% from 41 URLs in 2018.

This increase is a result of more sophisticated crawler technology being used by the IWF and our international partners, enabling us to find and remove more criminal imagery from the open web.

What can we do about this?

We use three pieces of technology to trace the hosting location, then issue a takedown notice to the company which is hosting the material. Law enforcement are consulted during this process and evidence is retained for investigation.

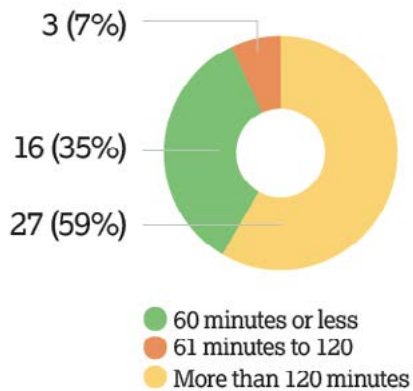
- 46 takedown notices, relating to the 158 URLs, were sent to the UK hosting companies.

We might send one notice for several webpages, and in some cases content may already have been removed by the time we receive authorisation from the police.

UK child sexual abuse content removal in minutes

Time really matters. The longer an image stays live, the more opportunity there is for offenders to view and share it, and more damage is caused to victims.

In partnership with the online industry, we work quickly to push for the fast removal of child sexual abuse content hosted in the UK. The “takedown” time-clock ticks from the moment we issue a takedown notice to the hosting company, to the time the content is removed.



Fastest removal time: 4 mins

Although the URL numbers are relatively small compared to the global problem, it's important the UK remains a hostile place for criminals to host this content.

21 companies' services in the UK were abused to host child sexual abuse images or videos during 2019. We issue takedown notices to UK companies, whether they're in IWF membership or not.

- 19 companies who were abused were not IWF Members.
- 2 companies were IWF Members.

Non-photographic child sexual abuse imagery

IWF's remit includes the identification and removal of UK-hosted non-photographic child sexual abuse images and videos.

- Despite receiving 8,057 reports of suspected non-photographic child sexual abuse imagery from external sources, no reports were confirmed as UK-hosted non-photographic child sexual abuse imagery in 2019.

Complaints

Anyone can lodge a complaint to IWF to appeal the inclusion of a URL on our URL List service, the receipt of a Notice and Takedown or make a more general complaint.

- In 2019 we received 41 complaints regarding the inclusion of a URL on our URL List, and three for the receipt of a Notice and Takedown.
- Of these, none were upheld. This means we could confidently assure the complainant that the issue raised did not stem directly from any IWF action, or that the assessment made by our analysts was legitimate and lawful.
- We have an independent appeals process. Information is found at iwf.org.uk.

What can we do about this?

The UK is one of the few countries in the world where non-photographic child sexual abuse imagery is criminal. When we find this content hosted in the UK, we issue a notice to the hosting provider who removes the content. This hasn't happened in the UK since 2016.

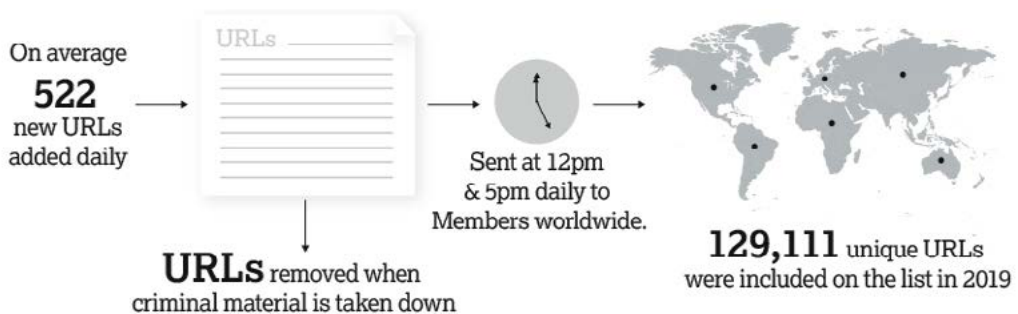
However, this content does exist online and if UK-hosted, would fail UK laws. Technology companies want the flexibility of being able to block and filter this content to prevent their customers from stumbling across it. Therefore, we created the NPI List, which contains cartoons, drawings, computer-generated imagery (CGI) and other non-photographic representations of child sexual abuse which is hosted outside of the UK.

The URLs provided in the NPI List are those deemed at the time of assessment to breach UK legislation, specifically Sections 62 to 69 of the Coroners and Justice Act 2009. Several international technology companies use this list to protect their services for their customers.

Our key services to technology companies

Finding and removing child sexual abuse imagery is only half of the job. We create and administer first-class tools and services which are used by technology companies to help keep the internet safer. We have close partnerships with governments, law enforcement and civil society across the world, but it's our unique independence from our partners which enables our tools and services to be used with confidence by hundreds of technology companies.

IWF URL list



We provide a list of webpages with child sexual abuse images and videos hosted outside of the UK to companies who want to block or filter them for their users' protection, and to prevent the repeat victimisation of the children in the images. We update the list twice a day, removing and adding URLs.

Since 2015, the IWF splash page has resulted in 21,750 new users coming through to the Stop It Now! Get Help website.

“We don’t know how many times the Splash page has been served to those attempting to access a URL known to have contained indecent images of children. But we do know that, since 2015, over 21,000 people have clicked through from a Splash page to the Stop It Now! Get Help website - a self-help website expressly for those concerned about their illegal online behaviour. From recent evaluation of the Stop It Now! indecent images of children deterrence campaign, we know that many who contact us need to hear about us on a number of occasions or via different routes before they really ‘hear’ the prevention message and get in touch. Evaluation also tells us many of them do take steps to change their behaviour. Splash pages are one vital mechanism for delivering this message and getting people to get in touch and stop their illegal behaviour.” Donald Findlater, Director of the Stop It Now! helpline.

Why is the URL List important?

When the URL List is deployed by a technology company, it prevents people from stumbling across known – and live – images or videos of children being sexually abused. In tandem, we recommend that companies show a “splash page” or information page in the event that someone tries to access a webpage which is on our list. This tells people why they can’t access the webpage and where they can go for help should they be worried about their online behaviour.

IWF Hash List

We have a growing list of hashes of child sexual abuse imagery. A hash is a unique code – like a digital fingerprint of an image. Using PhotoDNA and MD5 technology, we create hashes of the child sexual abuse content we see and we add these to our Hash List. See page 51 for a breakdown of our data.

Why is this hash list important?

Up to three trained IWF experts have looked at each image and assessed it before a hashed image is included on the list. We use these hashes to help us find duplicate images of child sexual abuse. This makes us more efficient at what we do. Up to 99 pieces of data are recorded against each image. This helps us to build a growing picture of the nature of child sexual abuse imagery on the open internet. See page 74 to find out more about how we use hashes in our Intelligent Crawler.

Keywords List

Offenders often create their own language – codes – for finding and hiding child sexual abuse images online.

- In December 2019 the Keywords List held 453 words associated with child sexual abuse images and videos.

What can we do about this?

To help counter this, each month we give our Members a list of keywords that are used by people looking for child sexual abuse images online. This is to improve the quality of search returns, reduce the abuse of their networks and provide a safer online experience for internet users.

How does this help technology companies?

When technology companies use our Hash List, it helps them to stop the sharing, storage and even the upload of child sexual abuse content. To make it easy for technology companies to use, each hashed image is graded according to international standards so companies have confidence in the data we provide them.

- At the end of 2019, the list contained hashes relating to 471,239 individual images.
- Of these hashes, 105,178 related to the worst forms of abuse – images of rape or sexual torture of children.

During 2019, we've increased the size of the Hash List by 125,278 hashes. This means that in 2019, our analysts assessed 9,637 images each, alongside assessing public reports, and actively searching for child sexual abuse images and videos.

What more are we doing about this?

During 2019 we've undertaken a review of our Keywords List. This process began with a research project, funded by Nominet, to better understand how offenders use search engines to locate child sexual abuse imagery online. The findings have enabled us to use our intelligent crawler to identify thousands of new keywords and key phrases which our team can use to proactively locate criminal imagery and attend to its removal. In 2020, we'll be developing new technical solutions to make this expanded Keywords List available to our Members, ensuring that we have a more diverse and dynamic list of keywords available.

This is a significant step forward, helping build a safer online space for all. It disrupts access to this content, safeguards users from stumbling across it, and saves victims from further revictimisation.

Newsgroups

Our Hotline team monitors the content of newsgroups.

In 2019:

- We processed 117 reports alleging child sexual abuse images hosted within newsgroups.

What can we do about this?

We issue takedown notices for individual postings of child sexual abuse imagery. We also provide a Newsgroup Alert to Members, which is a notification of child sexual abuse content hosted on newsgroup services so it can be removed. We are one of only a handful of Hotlines in the world that assesses reports on newsgroups.

- 51 takedown notices were issued for newsgroups containing child sexual abuse images (922 in 2018). One takedown notice can contain details of several newsgroup postings.
- 2,843 postings were removed from public access (29,865 in 2018).

After monitoring newsgroups, we recommended our Members do not carry 260 newsgroups containing or advertising child sexual abuse images and videos.

How did our work help?

During 2019, we saw a reduction in the number of newsgroup postings distributing criminal imagery. This reduction is in part attributable to the disappearance of one extremely prolific commercial distribution group.

In 2018, one of our analysts identified financial information which could assist law enforcement to trace the location of the distributor. Working in partnership with our Members in the newsgroup sector together with international law enforcement, the intelligence was referred to the relevant agency to enable them to launch an investigation. Since that referral, no further instances of criminal imagery associated with this commercial distributor have been identified in 2019.

Intelligent Crawler

We've created an intelligent web crawler. This is technology which we deploy to methodically browse targeted areas of the internet. What makes ours unique is that it's loaded with over 470,000 hashes of known child sexual abuse images (see page 51 on hashes).

How does using the crawler help our mission?

We use our crawler as one operational tactic in a suite of tools designed to find, remove, and disrupt the availability of child sexual abuse material. Our crawler is deployed in a considered and targeted manner in order to be most effective. In addition, it reduces unnecessary exposure to child sexual abuse imagery for our analysts, as well as providing domain "health checks" for technology companies.

- In 2019 it crawled almost 72 million webpages, and two thirds of a billion images.

By comparing each image it finds to the hashes of known child sexual abuse material, it means we can find duplicate child sexual abuse images hidden across the internet.

Cryptocurrency alerts

We see child sexual abuse material for sale in exchange for virtual currencies.

What can we do about this?

Notifications are sent to relevant companies when we see virtual currency wallets associated with online child sexual abuse images and videos, anywhere in the world. We provide personalised information for businesses, including transaction amounts, to help them with payment tracking and cryptic keyword terms associated with child sexual abuse content.

We also accept reports of suspicious webpages from those companies for our specialist analysts to assess. Our alerts have allowed technology companies to identify people who are involved in the sale or purchase of child sexual abuse material online.

Child Abuse Image Database (CAID)

We work closely with the police and the Home Office on the Child Abuse Image Database (CAID).

Why is this important?

Our access to CAID enables us to share IWF images and hashes with law enforcement. It also allows our analysts to carry out victim identification checks. By doing these checks, our analysts can find out if a child has been safeguarded, which has a positive impact on our analysts' welfare. It also means our analysts can prioritise making a referral to police if the victim isn't found in the database. In these cases, we've had some success in helping to ensure that children are safeguarded.

See page 21 where Internet Content Analyst Henry describes his role in helping two children.

Glossary of terms

Banner site: A website or webpage made up of adverts for other websites with text links or images that take you to third-party websites when you click on them.

Blog: A blog is a discussion or information site made up of separate entries, or posts. Most are interactive, and visitors can leave comments and even message each other on the blog. The interactivity is what makes them different from other static websites.

CAID: The Child Abuse Image Database (CAID) is a project led by the Home Office which enables UK law enforcement to assess, categorise and generate unique hashes for tens of millions of child abuse images and videos found during their investigations.

Category A, B and C: We assess child sexual abuse images and videos based on UK law, according to the levels in the Sentencing Council's Sexual Offences Definitive Guidelines. Since April 2014, there have been three levels: A, B and C. For definitions see our website: iwf.org.uk/assessment-levels

Child sexual abuse images/videos/imagery/content/material: Images or videos that show the sexual abuse of children. We use the term 'child sexual abuse' images to reflect the gravity of the images we deal with.

Cyberlockers: File hosting services, cloud storage services or online file storage providers. They are internet hosting services specifically designed to host users' files.

Dark net: The dark net, also known as the dark web, is the hidden part of the internet accessed using Tor. Tor is anonymity software that makes it difficult to trace users' online activity.

Disguised websites: Websites which, when loaded directly into a browser, show legal content—but when accessed through a particular pathway (or referrer website) show illegal content, for example child sexual abuse images.

Domain alerts: Details of domain names that are known to be hosting child sexual abuse content.

Forum: Also known as a 'message board', a forum is an online chat site where people talk or upload files in the form of posts. A forum can hold sub-forums, and each of these could have several topics. Within a topic, each new discussion started is called a thread, and any forum user can reply to this thread.

Gateway sites: A webpage that provides direct access to child sexual abuse material but does not itself contain it.

Hash/hashes: A 'hash' is a unique code, or string of text and numbers generated from the binary data of a picture. Hashes can automatically identify known child sexual abuse images without needing to examine each image individually. This can help to prevent online distribution of this content.

Hidden services: Websites that are hosted within a proxy network, so their location can't be traced.

Image board: An image board is a type of internet forum that operates mostly through posting images. They're used for discussions on a variety of topics, and are similar to bulletin board systems, but with a focus on images.

Image host/Image hosting site: An image hosting service lets users upload images which are then available through a unique URL. This URL can be used to make online links, or be embedded in other websites, forums and social networking sites.

IWF Reporting Portal: A world-class reporting solution for child sexual abuse content, for countries which don't have an existing Hotline.

Keywords: A list of terms associated with child sexual abuse material searches.

Newsgroups: Internet discussion groups dedicated to a variety of subjects. Users make posts to a newsgroup and others can see them and comment. Sometimes called 'Usenet', newsgroups were the original online forums and a precursor to the World Wide Web.

Non-photographic child sexual abuse content: Images and videos of child sexual abuse which aren't photographs, for example computer-generated images.

Proactive/proactively searching/proactively seeking: We can now actively search for child sexual abuse content, in addition to taking public reports. We're one of only a few Hotlines in the world that can do this.

Proxy network: These are systems that enable online anonymity, accelerate service requests, encryption, security and lots of other features. Some proxy software, such as Tor, attempts to conceal the true location of services.

Re-victimisation: Re-victimisation, or repeat victimisation is what happens to a victim when their image is shared online. A single image of a victim can be shared hundreds or thousands of times.

Service Provider/Internet Service Provider: An internet service provider (ISP) is a company or organisation that provides access to the internet, internet connectivity and other related services, like hosting websites.

Social networking site: A social networking service is a platform to build social relations. It usually has a representation of each user (often a profile), their social links and a variety of other services. Popular examples include Facebook and Twitter.

Top-level domain (TLD): Domains at the top of the domain name hierarchy. For example .com, .org and .info are all examples of generic top-level domains (gTLDs). The term also covers country code top-level domains (ccTLDs) like .uk for UK or .us for US and sponsored top-level domains (sTLDs) like .mobi or .xxx

URL: An acronym for Uniform Resource Locator. A URL is the specific location where a file is saved online. For example, the URL of the IWF logo which appears on the webpage www.iwf.org.uk is www.iwf.org.uk/themes/iwf/images/theme-images/logo.png.

Webpage: A document which can be seen using a web browser. A single webpage can hold lots of images, text, videos or hyperlinks and many websites will have lots of webpages. www.iwf.org.uk/about-iwf and www.iwf.org.uk/Hotline are both examples of webpages.

Website: A website is a set of related webpages typically served from a single web domain. Most websites have several webpages.

Designed by Johnson Banks
Design and print sponsored by




Internet Watch Foundation

Discovery House, Chivers Way
Histon, Cambridge, CB24 9ZR

E media@iwf.org.uk

T +44 (0) 1223 20 30 30

 Internet Watch Foundation
@IWFHotline

iwf.org.uk

Charity number: 01112398

Company number: 03426366



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

"As a result of the IWF's work, the UK hosts a tiny proportion of child sexual abuse material. The work of the IWF in removing significant amounts of child sexual abuse material is a genuine success story."

The Independent Inquiry
into Child Sexual Abuse,
The Internet Investigation
Report March 2020.



IWF
Internet
Watch
Foundation