Once upon a year

The Internet Watch Foundation
Annual Report 2018

The Internet Watch Foundation is a not-for-profit organisation supported by the European Commission and internet companies around the world. We work closely with police and governments, globally. For 23 years, we have given people a safe place to report imagery anonymously, now covering 25 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 new technology and provide bespoke tools to our industry Members.

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 it is reporting to us, funding us, or collaborating on technology and research.

We have changed the names of children and some staff members featured in this report, but their stories are real.

Prologue: Why we are here

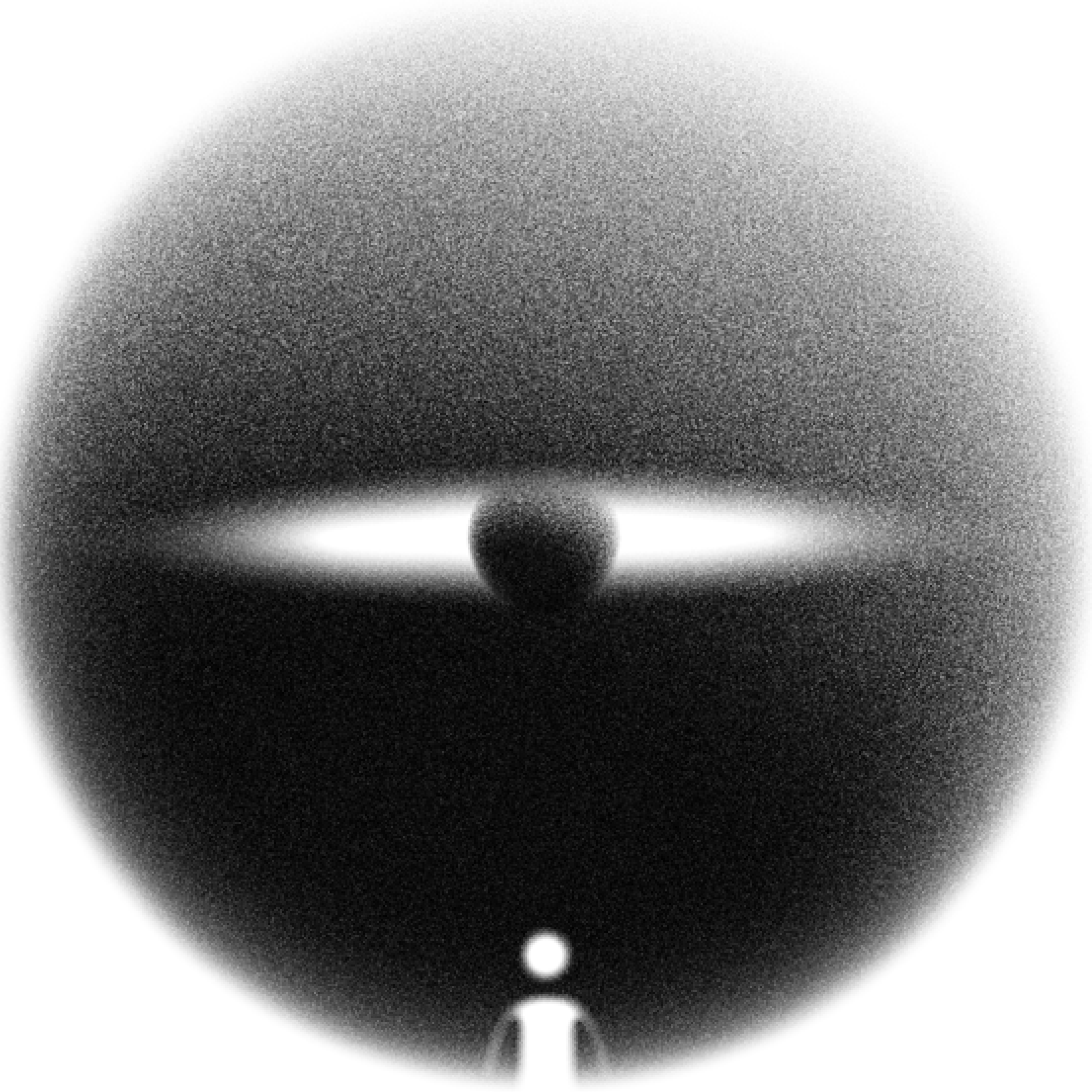
Chapter 1: Welcome

Chapter 2: What we are achieving

Chapter 3: How we help

Chapter 4: Who we are

Chapter 5: Where next



Once there was an invisible child

The child was a real human child,
but sometimes she didn’t feel like it.
Monsters who looked like
men and women took pictures of her.
The pictures were everywhere,
but it was as though nobody could see her.
If people could see her,
surely they would help her.
The child decided she must be invisible.
Sometimes, when she was finally alone
at night, she wondered how
many other invisible children
were out there.

The problem we are solving

Imagine a world where there are no images and videos of child sexual abuse on the internet. Where children and adults can experience the wonders of the internet without worrying about their safety. Not a lot to ask for, is it?

But, as we know, the internet has a dark side where children are groomed, coerced, deceived and sexually abused. Beyond the crime of the abuse, and the humiliation, is the crime of recording it. Beyond the abuse, humiliation and recording of it, is the crime of sharing it, then the viewing of it repeatedly by others who create the demand for more 'material'—more sexual abuse, more sharing. That's why the IWF exists.

Child sexual abuse has a devastating impact on people's lives. Online child sexual abuse is increasing globally, with criminals using technology to evade detection. Children are revictimised every time their images are viewed online.

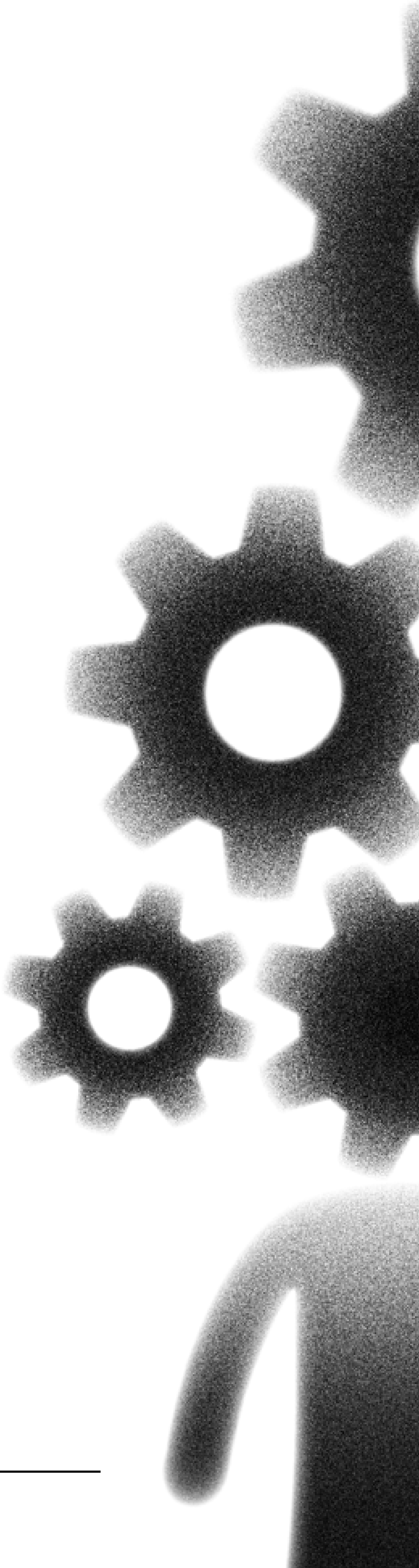
We want to make the internet a safer place for children and adults.

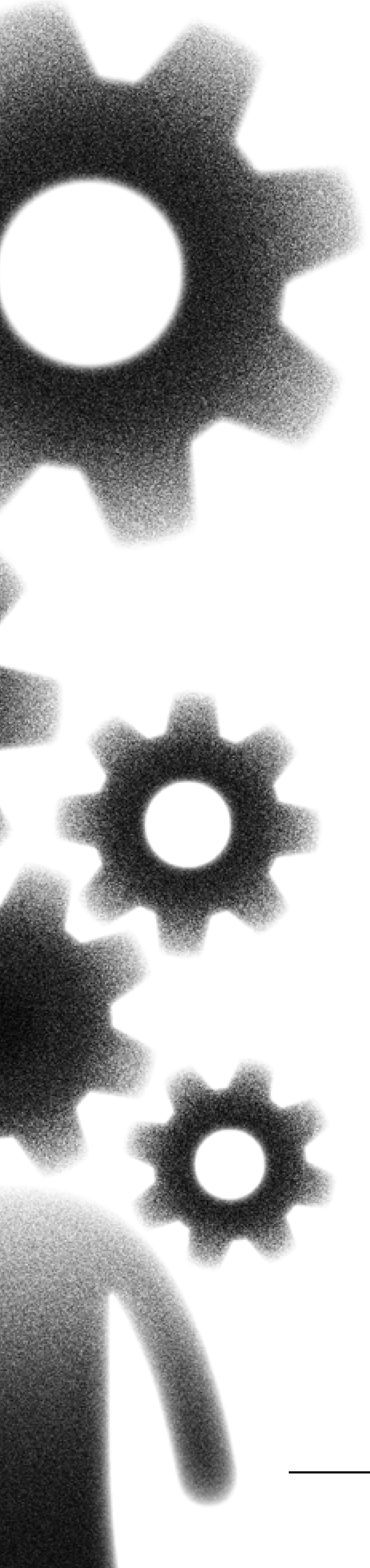
We want to reduce—and eliminate—child sexual abuse material all over the world.

We want to make the UK the most hostile country in the world to host child sexual abuse material and the safest place in the world to be online.

We will be innovative and bold in how we work to create the most impact.

When there are no child sexual abuse images and videos on the internet, that would be an acceptable reality.





Catherine’s story

“I’ve worked for the IWF for 10 years now and during that time I’ve had two children of my own. Having a family has affected the way I feel about my work, but in a positive way. I want every second to count and doing a meaningful job is incredibly satisfying.

Like most of the analysts, finding images of babies being abused is one of the hardest things. As a human being, you are always going to be sensitive to this. Some of the hideous things offenders are capable of inflicting on innocent children is unbelievable. But we’re highly trained to deal with this and it makes me even more motivated to search for any associated imagery and get it removed from the web.

For us, the Holy Grail of an analyst’s work is finding an image, or information that could lead to the rescue of a child. Recently, I identified a video that had been captured via a webcam. It appeared to be new and suddenly I felt like a clock was ticking—could I find any clues or evidence that could lead police to this child? I immediately called in our Manager and the information we identified was passed on and flagged to the National Crime Agency’s Child Exploitation and Online Protection (CEOP) Command, the specialist UK police.

We’ve seen a huge rise in child sexual abuse imagery captured by webcams this year. On commercial sites, where an offender could be making a profit from the material, the ages of the children appear to be getting younger. This certainly makes you more aware of online safety and that’s a message I’m happy to share.

Of course, I could go home at the end of the day and think that the world is a dreadful place. But for me, like all of our analysts, I just want to help the children in these terrible images. I have real empathy for them and that’s why I love my job.”

Paul’s story

“Most people would think we’d go home depressed every night. Yes, we do see some pretty horrific things during our working day. Child sexual abuse is an incredibly cruel crime. The images we see are of real children and babies. We never forget that.

But this work isn’t depressing, in fact it’s the opposite. Very early on in my IWF career, I was involved in identifying and analysing a series of child sexual abuse images that led directly to the rescue of a child. Wow, I suddenly understood the power an analyst can have. I felt like I’d been able to reach into the screen and help that child.

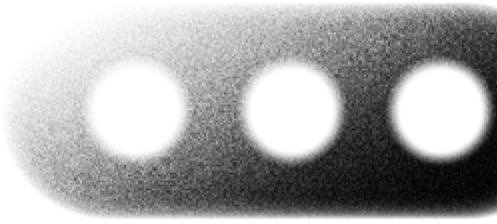
This year, I’ve had reports from the victims themselves. They can be desperate by the time they contact us. They may have been coaxed or groomed into doing something that they didn’t want to do and then it’s on the internet. Of course, we can only work within the legal framework, but I see personal reports as a real challenge and I’m always determined to do whatever I can to help these young people. The very fact that I can have an impact, that I can help, is amazing.

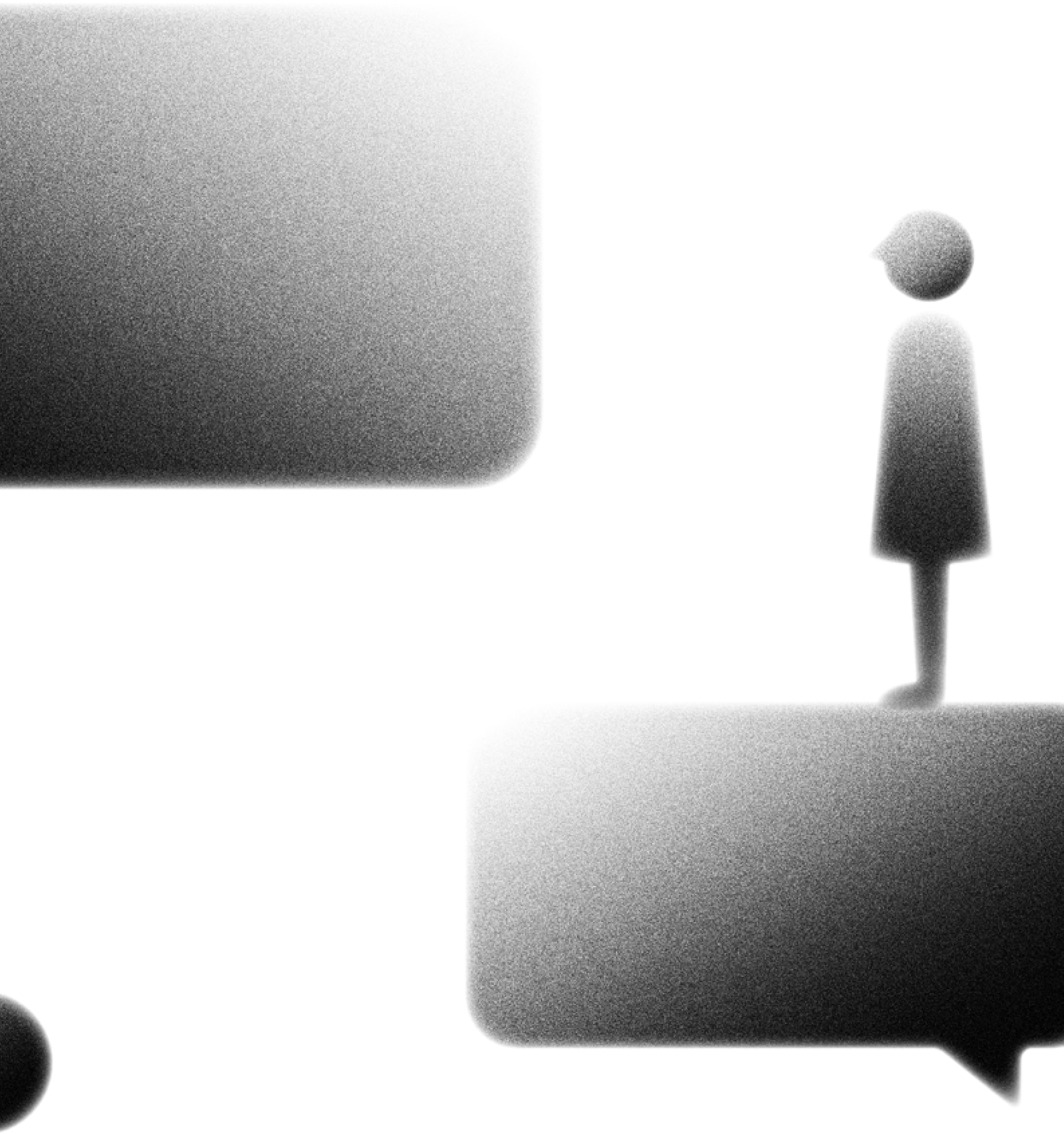
As a parent, I’ve realised that I’m more conscious now of what my children are doing online or, more importantly, who they are talking to.

Today most children are tech savvy, but they may not be tech safe.

On the web, offenders can disguise themselves as friends and build trust. The challenge is staying one step ahead of these people. And that’s the reason I tell friends and family about the job I do, so that I can help spread the online safety message.

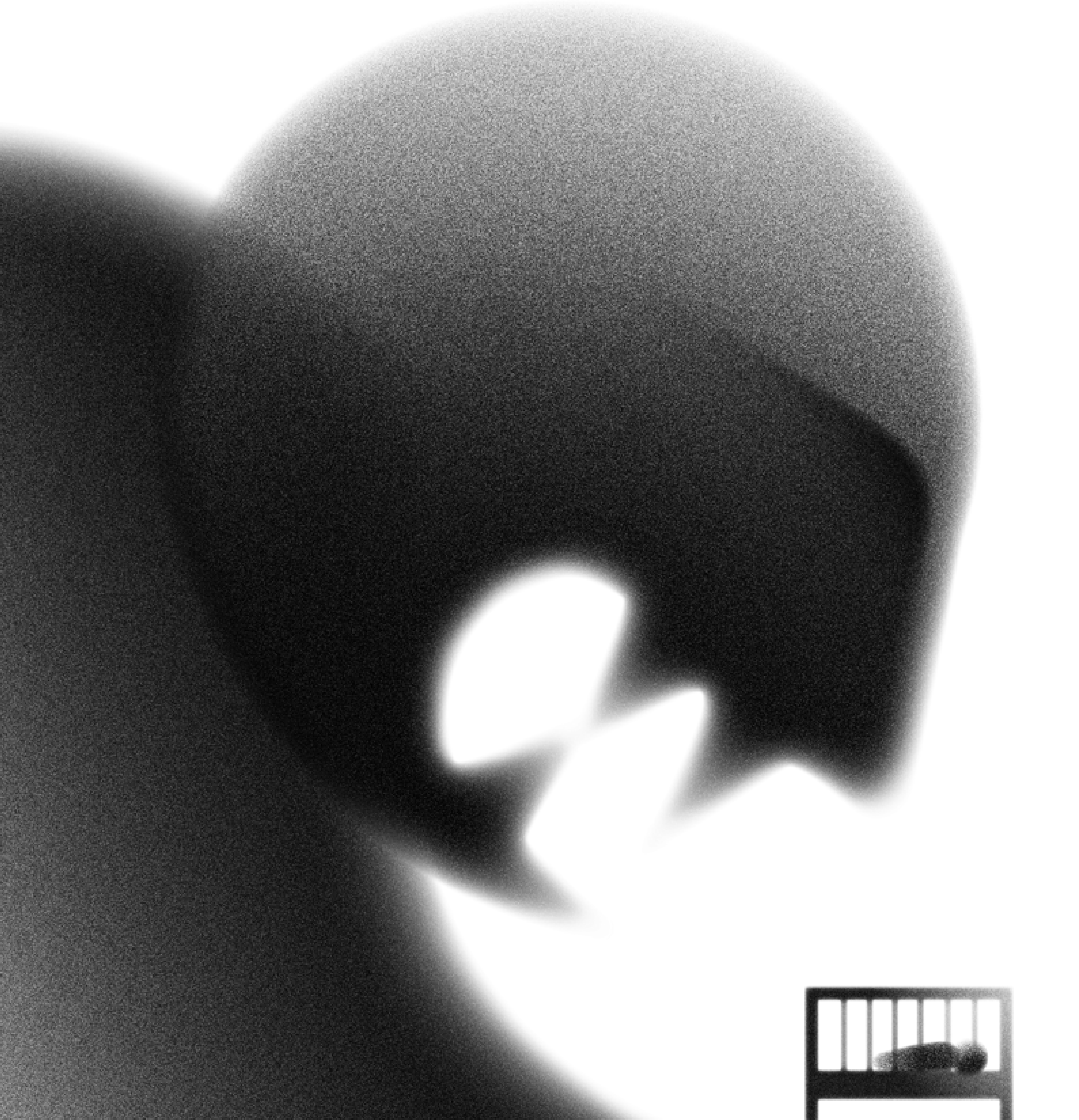
Each year the number of images we assess goes up. We are getting better at what we do and we’ve got the best new tech to hand, like our crawlers. They act like a ‘trusty sidekick’. But I think there will always be a need for ‘human’ analysts, because this work is so complex. Child sexual abuse imagery isn’t always black and white. Our team will always need to be there to identify the shades of grey, that could and sometimes do, lead to the rescue of a child.”





Olivia's story

A survivor's story,
told by an IWF analyst



"I first saw Olivia when she was about three. She was a little girl with big green eyes and golden-brown hair. She was photographed and filmed in a domestic setting. Sadly, it may well have been her home and she was with someone she trusted. Olivia was in the hands of someone who should have looked after her, nurtured her. He betrayed her trust and in the most hideous way possible. Olivia should have been playing with toys enjoying an innocent childhood. Instead, she was subjected to appalling sexual abuse over a number of years.

I've seen Olivia grow up through cruel images and videos, suffering hideous abuse. She was repeatedly raped and sexually tortured.

The abuser made sure his face wasn't seen and he distorted any image that would expose the crime scene.

It's highly likely that it was this man, her abuser, who first shared the images of Olivia's suffering. Other offenders may have followed his lead and done the same. It's also likely that some have profited financially from sharing this abuse. The suffering of children like Olivia is frequently a commercial crime. And for us, anyone who subsequently shared or paid to view this heinous material contributed to Olivia's torment.

The police rescued Olivia in 2013—she was eight years old at that time—five years after the abuse first began. Her physical abuse ended and the man who stole her childhood was imprisoned. But those images are still in circulation and heartless offenders continue to share and probably profit from Olivia's misery.

We see Olivia every day—five years after she was rescued. To show exactly what 'repeat victimisation' means, we counted the number of times we saw Olivia's image online during a three-month period. We saw her at least 347 times. On average, that's five times each and every working day.

In three out of five times she was being raped, or sexually tortured. Some of her images were found on commercial sites. This means that in these cases, the site operator was profiting from this child's abuse.

We simply don't know if Olivia was aware that images of her abuse were being shared online. If she was, it's difficult to imagine how traumatic that knowledge must be, particularly for someone so young.

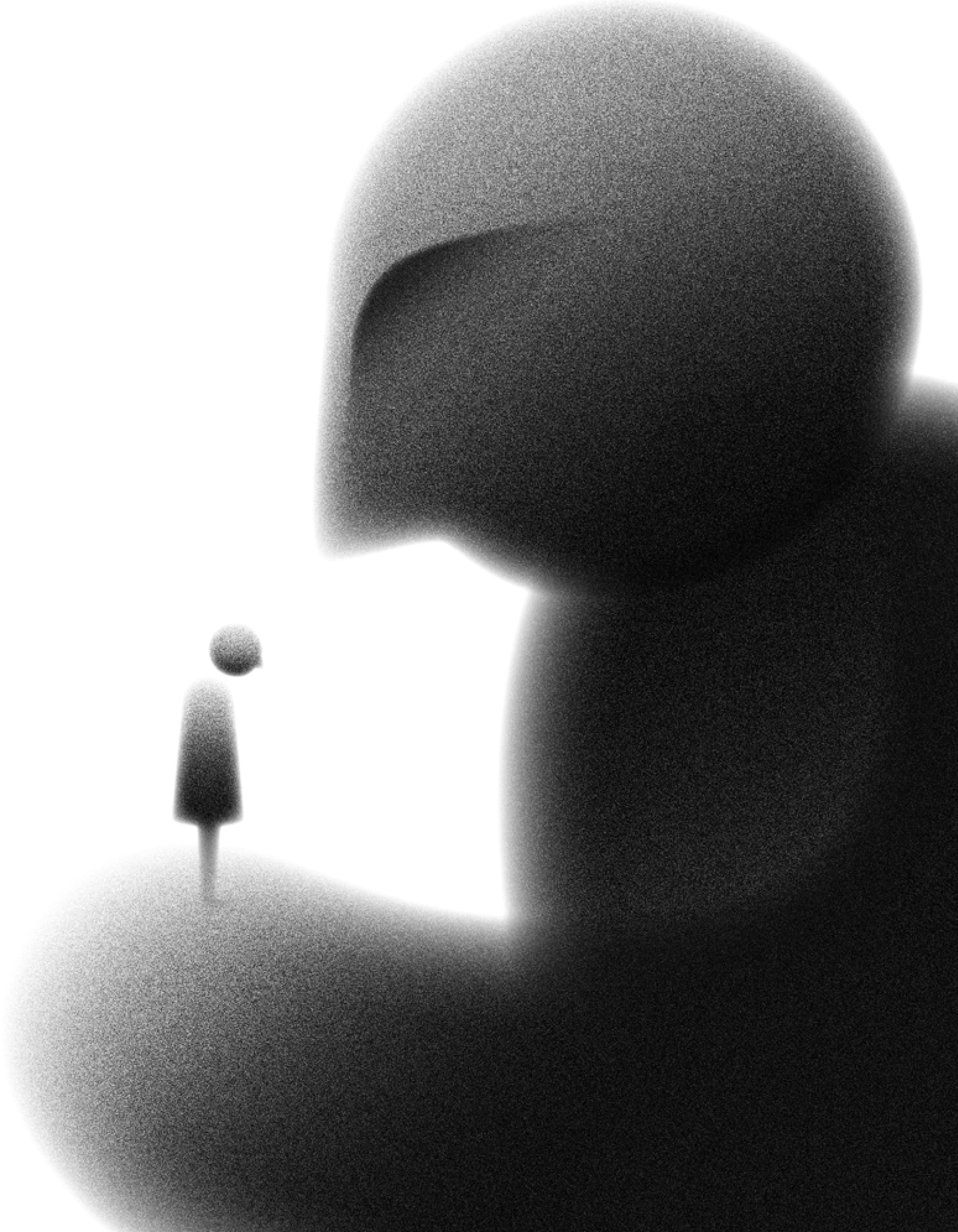
However, we do know, from talking to adults who have suffered re-victimisation, that it's a mental torture that can blight lives and have an impact on their ability to leave the abuse in the past. Knowing an image of your suffering is being shared or sold online is hard enough. But for survivors, fearing that they could be identified, or even recognised as an adult is terrifying."

Olivia is now a young teenager. But we still see her as a child. Every day.

We pieced together Olivia'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.

Somewhere far away

Many miles from the invisible child,
there was a grown-up
who was not a monster. He worked with
other people who weren’t monsters.
And they knew about the invisible children.
They were on a quest to help.
But they knew it would
not be easy.



Welcome

Welcome from our Chair

Throughout my first year as Chair, I've come to appreciate and value the IWF's work and its role in challenging the sexual abuse of children online.

I was left deeply shocked when I saw some of the images that the analysts assess for removal as part of my induction into the organisation; that the most vulnerable people in our society should be abused in this way is profoundly upsetting and cause for reflection on how such abuse can happen.

I deeply respect the analysts' work, and that of the whole staff team led by Susie Hargreaves. They deserve our support. I also acknowledge the work of many of our Member companies who partner with us and act promptly to remove the abusive images we find. But I know they could do more and we are exploring with them how to improve their transparency and accountability concerning what they do to prevent and remove such criminal imagery. In an era when it's fashionable to blame platforms for the behaviour of the people on them, IWF will always do its best in tackling problems by working in partnership.

It was sobering for me to hear from the specialist police unit that deals with child sexual exploitation that, in their estimate, something in the region of 100,000 men in the UK try to access images of children being sexually abused. We all need to recognise the scale of this problem and the unpleasant fact that where there is demand there will always be supply. We work to disrupt that supply and shut it down, and our role will remain necessary until there are no longer people wishing to access such material. But this requires a serious and long-term investment in prevention as well as co-operation and resources from government, the charitable sector and the industry itself. As a society we always tend to favour intervention once a crime has been committed (or the illness incurred) rather than in the less glamorous and longer process of prevention. But until we take this approach, we will always be fighting fires.

Last year our analysts found over 100,000 URLs of children being sexually abused. We should remember that each URL can contain hundreds, if not thousands, of images. These figures, while a testimony to the work of the IWF and its success, are a reminder of the scale of the problem and the size of the mountain that our society has still to climb.

Abusers are constantly innovating technically, and we are innovating to find them. We have a pool of highly talented engineers, both internally and as external advisors, who help us keep on top of technological change. We have a staff team dedicated to removing abusive images and a Board determined to support them in any way we can. However formidable the challenge, we are ready to face it.

Andrew Puddephatt
IWF Chair

Welcome from our CEO

Olivia is a little girl who we see every day. She was robbed of her childhood by a man who sexually abused her over many years. Although she's been rescued from her abuser, and her abuser is now imprisoned, that isn't enough to stop the images and videos of her rape from being watched again and again by offenders the world over.

Olivia is now in her teens, but we see her every day as a very young girl. This annual report is about Olivia, and all the other children whose abuse is watched through laptops, mobile phones, desktop computers and tablets.

We work for those children to give them a brighter future, free from the torment of knowing their abuse is being watched—and cruelly enjoyed—by others.

That is what motivates us. And last year we broke all previous records for the numbers of reports we assessed, and the amount of child sexual abuse imagery we found and had removed from the internet.

We're here to build the best, most sophisticated technology to speed up the work of finding the images and videos of Olivia, and those like her.

We also see the captures of children who have been deceived, coerced and groomed over the internet to produce sexual images and videos. For some, they've been duped into thinking they're in relationships; others want to gain likes. Each child will have their own story but what is clear is that these children are being accessed by offenders, often in their bedrooms and homes, and then taken advantage of in the most grotesque way. Everyone needs to take responsibility to protect children.

Our work to date has focussed on fighting the supply of images and videos being uploaded and shared. In 2019 we want to play a bigger role in fighting the demand and preventing people from accessing the content in the first place. We'll be working with other people and organisations through the year to explore how we can do this.

We can't fight this alone. We need to work closely with the internet industry, and others, to bring about any solution to this internet evil. Webcams, smartphones and other recording devices witness the most severe abuse being inflicted upon the youngest children. Software programmes are used to edit this abuse. File transfer software will be used to share it. Internet platforms and online image stores are used to distribute it. A network of people create the demand, and a network of people are all too ready to meet the supply.

We all have a duty to stop this content, to protect Olivia, and other children like her.

Susie Hargreaves OBE
IWF CEO and Director of
the UK Safer Internet Centre

A message from the Home Secretary

"The horrifying amount of online child sexual abuse material removed by the IWF shows the true scale of the vile threat we are facing. This is why I have made tackling it one of my personal missions.

I welcome this impressive work and have been encouraged by the progress being made by the tech companies in the fight against online predators. But l want the web giants to do more to make their platforms safe."

Home Secretary
Rt. Hon. Sajid Javid MP

Each day the quest continued

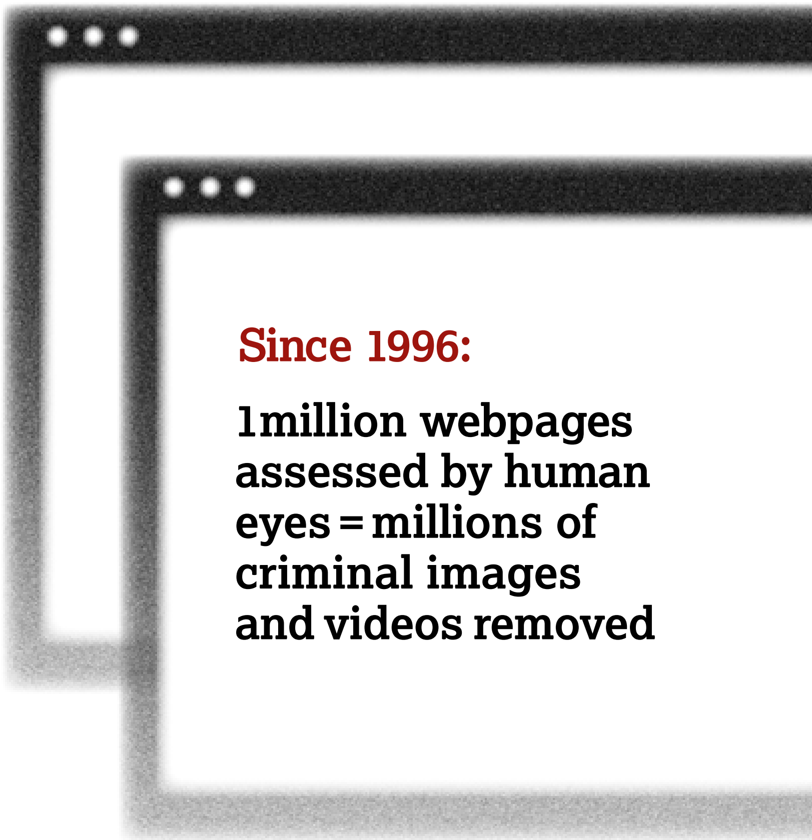
The story of the invisible children
spread across the land.
People realised there were many of them.
People kept watch and kept count.
They did what the children had always wanted
them to do—they fought back
against the monsters.

Our year at-a-glance

We assessed a webpage every 2 minutes. Every 5 minutes, that webpage showed a child being sexually abused.

4 in every 5 times the public chose to report anonymously.

2 in every 7 public reports were accurate (28%).



Since 1996:

1million webpages assessed by human eyes = millions of criminal images and videos removed

229,328

reports assessed

105,047

URLs confirmed as child sexual abuse images or videos

Who are the children?

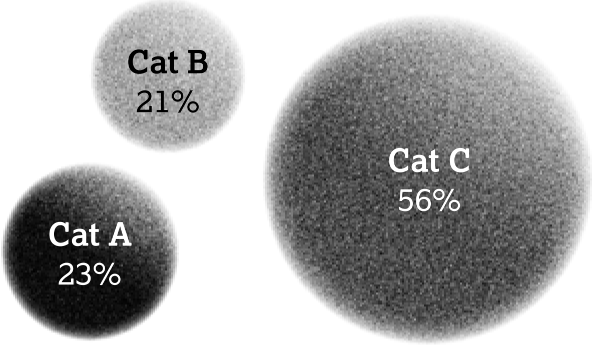
78% of images where victims were girls

17% of images where victims were boys

4% of images with both genders

In a small number of images, gender could not be identified

Severity of abuse



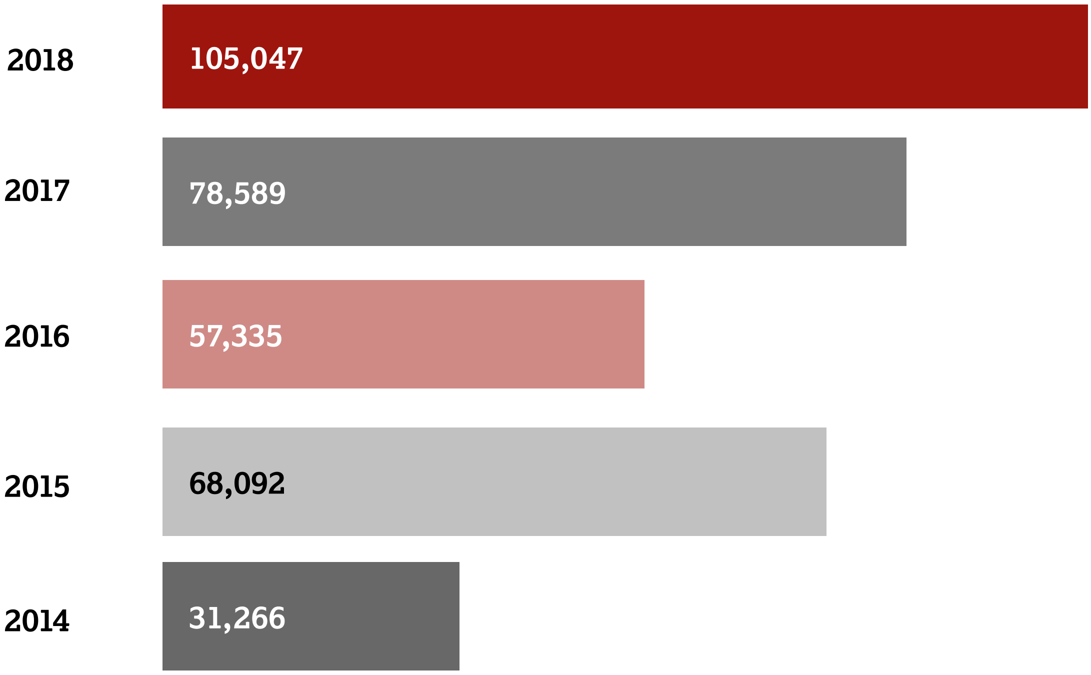
Category A: % showing sexual activity between adults and children including rape or sexual torture

Category B: % of images involving non-penetrative sexual activity

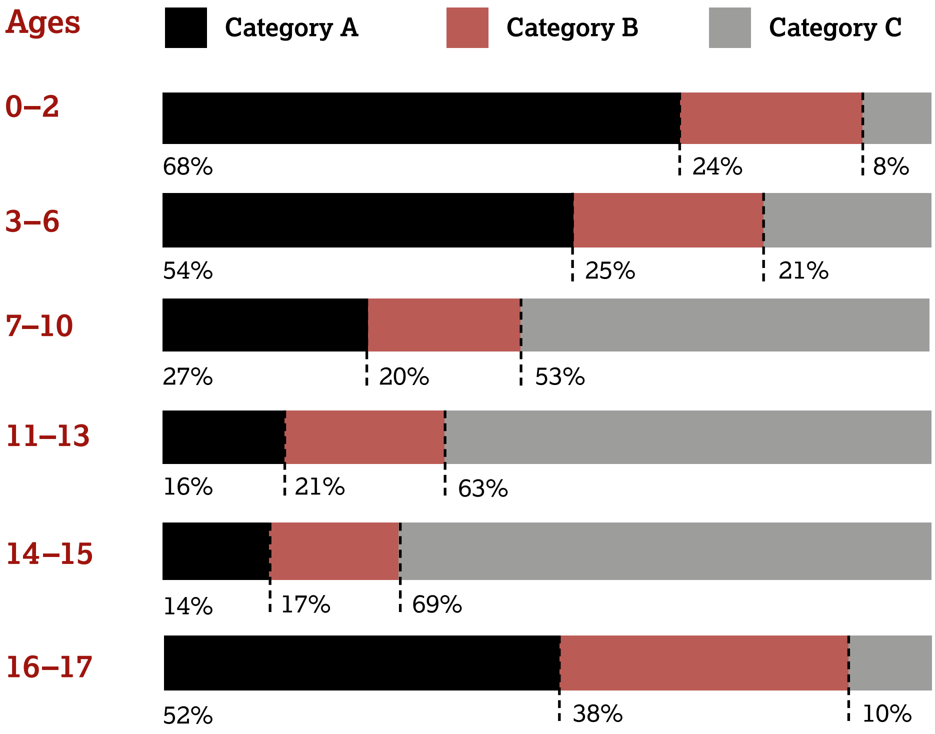
Category C: % of other indecent images not falling within categories A or B

477,595 webpages showing the sexual abuse of children removed since 1996 due to the work of IWF analysts

Child sexual abuse URLs

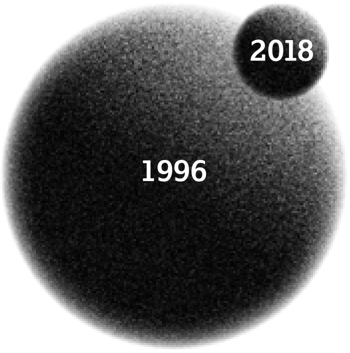


All URLs actioned by age group and severity

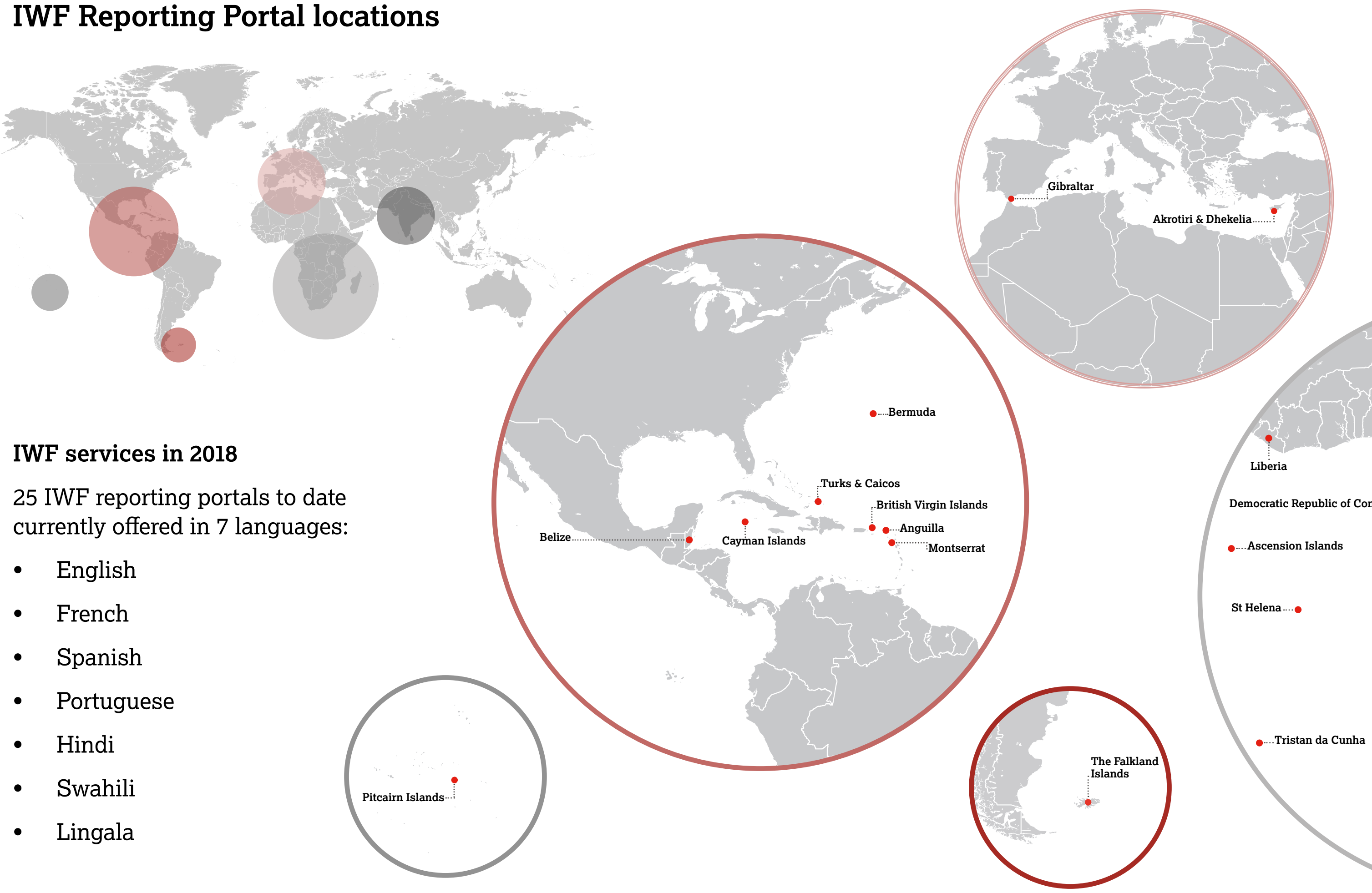


*rounded to nearest whole percent.

When we started in 1996, the UK hosted 18% of the known child sexual abuse URLs. In 2018 this figure was just 0.04%



IWF Reporting Portal locations



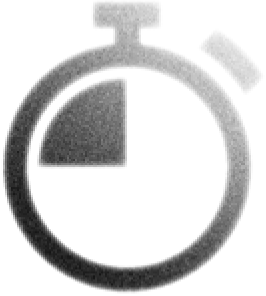
IWF services in 2018

25 IWF reporting portals to date currently offered in 7 languages:

- English
- French
- Spanish
- Portuguese
- Hindi
- Swahili
- Lingala

Which types of sites are abused the most?

Top 10 site types	No of reports 2018	%
Image host	86,197	82%
Cyberlocker	5,074	5%
Banner site	4,558	4%
Blog	3,270	3%
Website	1,265	1%
Forum	1,190	1%
Search provider	818	<1%
Image board	783	<1%
Video channel	772	<1%
Social networking site	530	<1%



8 minutes:

Our fastest content removal time last year.

4 minutes:

The IWF record.

10 occasions we provided police with a package of information we believed could help rescue a child.

India
Uganda
go
Burundi
Tanzania
Angola
Mozambique
Namibia
Mauritius
Malawi
Zambia

Where is child sexual abuse imagery hosted?

Continent hosting of all child sexual abuse URLs	No of reports 2018	%
Europe (inc Russia & Turkey)	82,803	79%
North America	16,986	16%
Asia	4,961	5%
Africa	1	<1%
South America	28	<1%
Australasia	183	<1%
Hidden services*	85	<1%
Total	105,047	

**Hidden services, see page 34*

Top 5 countries	2018 data	% of total for 2018
Netherlands	48,900	47%
United States	12,818	12%
Russian Federation	11,877	11%
Slovak Republic	11,004	11%
France	6,607	6%

IWF services in 2018

URL List: 100,682 unique URLs and an average of 6,046 URLs per day.

Hash List: 345,961 individual images.

Highlights and awards

January

A Demos report says the model of industry self-regulation pioneered by the IWF means less than 0.1 percent of online child sexual abuse content is now hosted in the UK, down from 18 percent in 1996.

IWF
Technology Briefing Series:
Online Child Sexual Abuse Imagery
DEMOS

February

Africa: On Safer Internet Day, the Government of Mozambique announces the opening of an IWF Portal for the confidential reporting of online child sexual abuse content.

UK Safer Internet Day: The country—and world—celebrates Safer Internet Day which results in nearly half of all UK children aged 8 to 17 hearing about how to stay safe online.

Create, connect and share respect:
A better internet starts with you.
IWF
UK Safer Internet Centre

March

The IWF scoops the Excellence in Internet Safety 'Oscar' from CorporateLiveWire, whose Innovation Awards celebrate those that transform industries and set standards and trends.

IWF becomes the first non-law enforcement agency to get access to the Child Abuse Image Database—CAID—so we can hash child sexual abuse images in-house, and share thousands of hashes through our partners in the internet industry worldwide.

April

In partnership with entertainment company LADbible, our film about the work of our analysts shows how one report can change a victim's life. Created for the Indecent Images of Children (IIOC) campaign, launched in partnership with HM Government, the NSPCC and the Marie Collins Foundation, it received over 2.5m views.

Our CEO Susie Hargreaves OBE is voted a finalist in the prestigious European CEO Awards.

Belize joins our network tackling online child sexual abuse imagery.

Disturbing data: IWF global figures show the amount of child sexual abuse imagery found online is up by one third from 2016.

May

IWF
Of the 2,082 images and videos of live-streamed child sexual abuse, 28% were of children aged 10 or under.

IWF research on child sexual abuse livestreaming reveals 98% of victims are 13 or younger and we call for greater public vigilance as the youngest victim identified is just three years old.

Malawi becomes the latest African country to launch an IWF Portal for confidential reporting.

June

Our Internet Content Analysts win the illustrious Comms Business Award, 'Hidden Heroes'.

IWF's Deputy CEO & CTO Fred Langford becomes President of INHOPE, the International Association of Internet Hotlines, for the second time.

The Democratic Republic of Congo joins the IWF network, opening its own public Reporting Portal.

The IWF becomes the first Hotline and the first UK organisation to gain Observer status at the Lanzarote Committee, giving us influence at a pan-European level.

July

IWF scoops 20th Anniversary Award from the UK Internet Service Providers Association (ISPA) for its ground-breaking work. The IWF was nominated alongside the UK Safer Internet Centre for another ISPA award for best partnership.

The IWF and Banco Santander host the first ever IWF Online Child Safety Hackathon, bringing together volunteer engineers in finding ways to stop the distribution of online child sexual abuse material.

August

India's IWF Portal passes the significant milestone of 1,000 reports from the public.

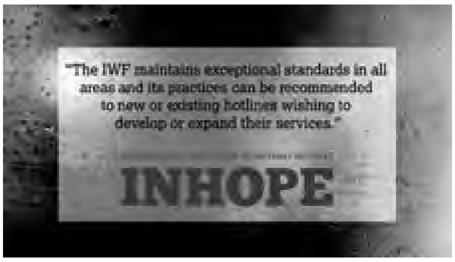
September

The Home Secretary the Rt. Hon. Sajid Javid MP praises our work in bringing down UK-hosted child sexual abuse content and announces that fighting child sexual exploitation will be his top priority.

Angola and Burundi each set up an IWF Portal where citizens can confidentially report suspected child sexual abuse imagery.

The High Commissioner marks the launch of Zambia's new IWF Portal by hosting Ambassadors, international child-protection organisations, and internet companies in a celebration of partnership working against the borderless crime of child sexual abuse online.

October



"The IWF maintains exceptional standards in all areas and its practices can be recommended to new or existing hotlines wishing to develop or expand their services."

INHOPE

The IWF wins praise for exceptional standards, audited by INHOPE. Assessors reviewed our relationship with government, law enforcement and child welfare agencies, together with our care for staff, internet security and data management.

As part of the Children's Charities Coalition on Internet Safety, we flagged the dangers of proposed EC legislation on e-privacy which would neuter the ability of tech companies to scan their networks for child sexual abuse imagery.

November

Our expertise is recognised as the IWF is granted Core Participant status on the Independent Inquiry into Child Sexual Abuse's Internet Investigation.

Our analysts break their own record for reports actioned in a single day, assessing and confirming 2,057 reports of online child sexual abuse imagery and marking them for takedown.

The Home Secretary tasks the IWF with reviewing the extent to which legitimate online ads from mainstream brands end up making money for offenders when appearing alongside child sexual abuse material.

Our Deputy CEO & CTO Fred Langford travels to Seattle with the Home Secretary and chairs a panel at Microsoft's HQ on livestreaming issues.

At Abu Dhabi's Interfaith Alliance, His Highness Sheikh Saif bin Zayed Al Nahyan presented a public service award to our CEO, Susie Hargreaves for her work leading the IWF and as a Board member of WePROTECT.

The Secretary of State for Digital, Culture, Media and Sport, the Rt. Hon. Jeremy Wright QC MP visits the IWF and meets our analysts.

December

Liberia announces it will join the IWF reporting network and open a portal in the New Year.

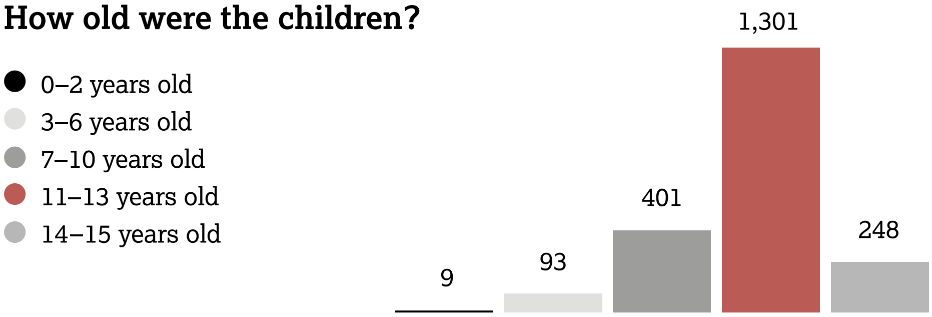
Home Office campaign: In partnership with VICE, we publish a feature about our analysts' vital work, to publicise our educational campaign developed in collaboration with HM Government, the NSPCC and the Marie Collins Foundation.

The Home Office announces a round table on advertising as a result of research by the IWF.

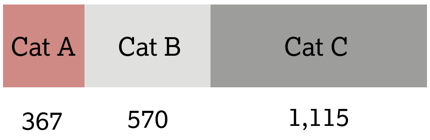
Our record day

On 27 November we assessed and verified 2,057 reports of child sexual abuse—the most reports we've ever completed in a day. We then worked with partners across the globe to get that content removed.

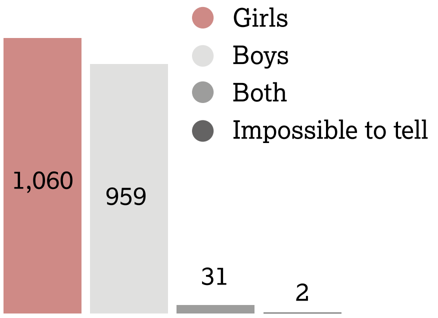
How old were the children?



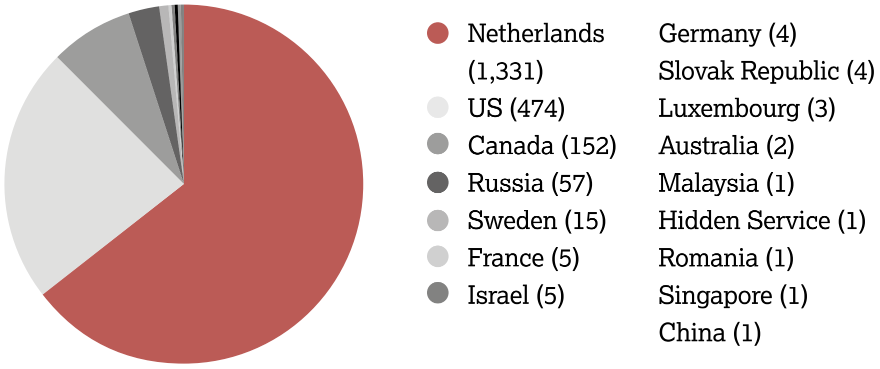
Severity of abuse seen in the images



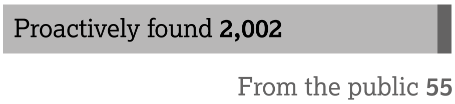
Who were the victims?



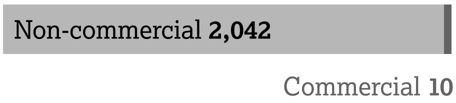
Where was the image or video hosted?



Where did the reports come from?



Type of sites



The totals reflect that 5 sites were gateway sites which didn't show child sexual abuse but led to such content

Statistics and trends

Our annual report gives the latest data on what’s happening globally to tackle child sexual abuse images and videos online. We encourage anyone working in this area to use our statistics to help inform their valuable work.

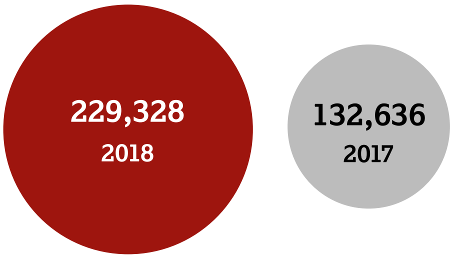
Reports

In 2018, we assessed a webpage every 2 minutes. Every 5 minutes, that webpage showed a child being sexually abused.

People report to us at iwf.org.uk, or through one of the 25 portals around the world, in multiple languages. All reports come to our headquarters in the UK. We also actively search the internet for child sexual abuse imagery. For every such image or video we identify, we assess the severity of the abuse, the age of the child/children and the hosting location.

Total number of reports

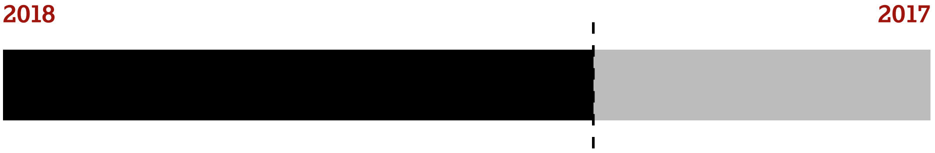
229,328 reports were processed by IWF analysts in 2018, a 73% increase on the 2017 figure of 132,636. Please be aware that not all reports we process are found to contain criminal imagery within our remit.



▲ 73% increase from 2017

Reports by source

Publicly-sourced reports

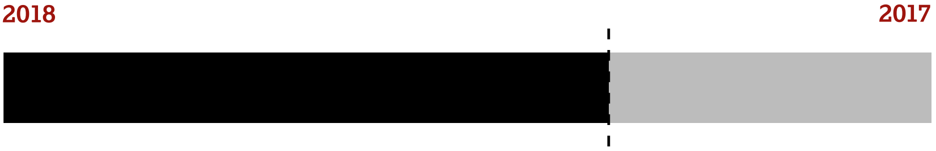


114,735 reports

66,650 reports

▲ 72% increase from 2017

Actively searched for



114,593 reports

65,986 reports

▲ 74% increase from 2017

Of all processed reports

228,333
were reports of webpages

995
were reports of newsgroups

Criminal content

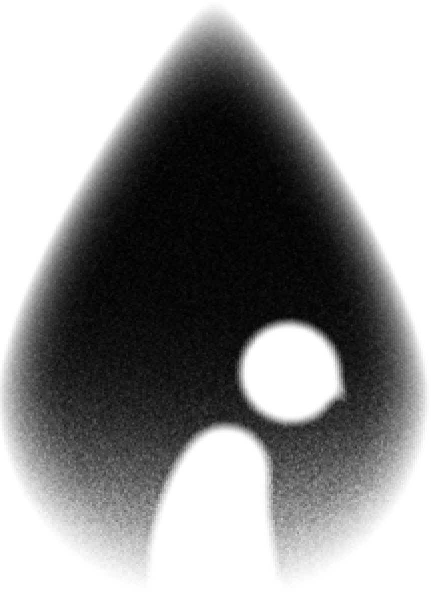
105,969 reports
were confirmed as containing criminal content covering all areas of our remit

▲ 32% increase from 2017

Child sexual abuse imagery on URLs

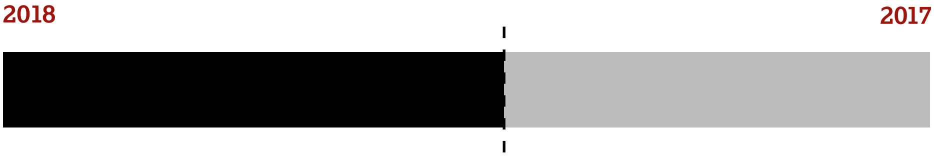
106,830 public reports were processed by our Hotline where the person thought they were reporting child sexual abuse imagery. This includes public reports from all external sources, which includes law enforcement, Members, professionals and the public. 28% of these reports correctly identified child sexual abuse images. This figure includes newsgroups and duplicate reports, where several reports have correctly identified the same child sexual abuse website.

- 16,272 URLs were from public sources (17% increase from 13,857 in 2017).
- 88,775 URLs were from active searches (37% increase from 64,732 in 2017).



105,047 URLs were confirmed as containing child sexual abuse imagery, having links to the imagery, or advertising it.

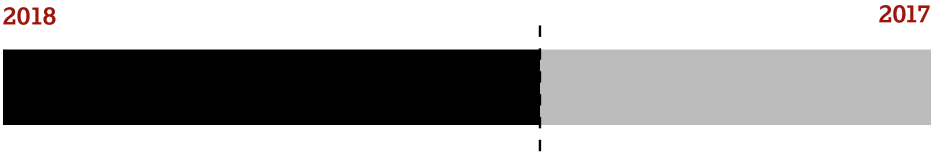
Public sources



16,272 URLs 13,857

▲ 17% increase from 2017

Active searches



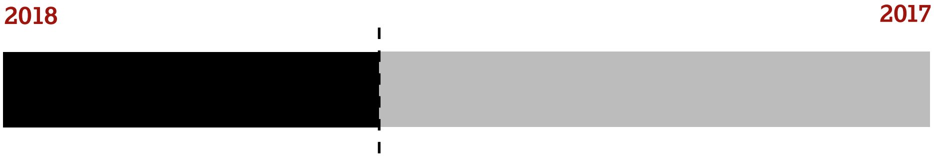
88,775 URLs 64,732 URLs

▲ 37% increase from 2017

Child sexual abuse imagery on newsgroups

443 newsgroups were confirmed as containing child sexual abuse imagery.

Removed posts



29,865 posts containing child sexual abuse imagery were removed from public access.

43,767 posts containing child sexual abuse imagery were removed from public access.

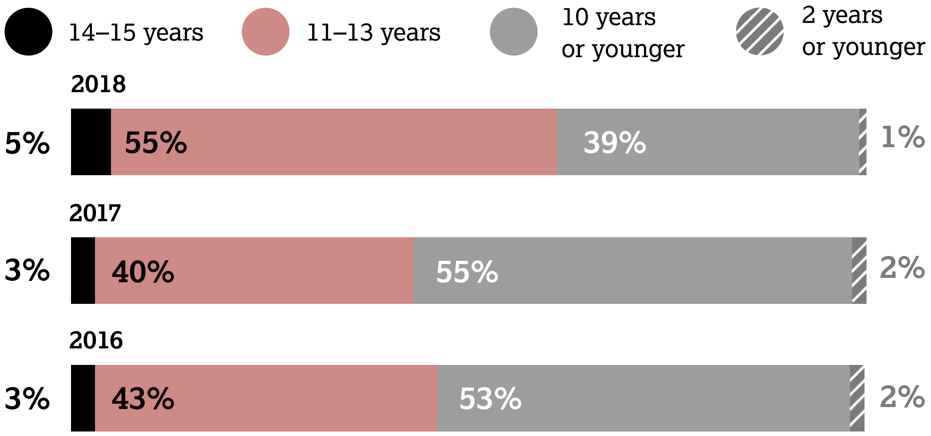
▼ 32% decrease from 2017

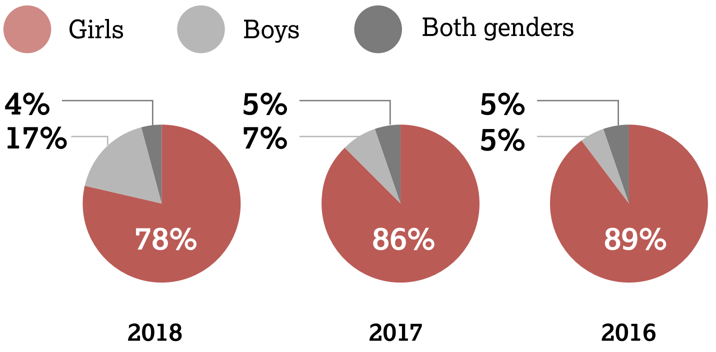
All child sexual abuse URLs analysed by the IWF

Since 2014 we have seen a gradual drop in the percentage of children we assess as being aged 10 or younger. However, where we do see child sexual abuse imagery of younger children, it is more likely to show the most severe forms of abuse, including rape and sexual torture.

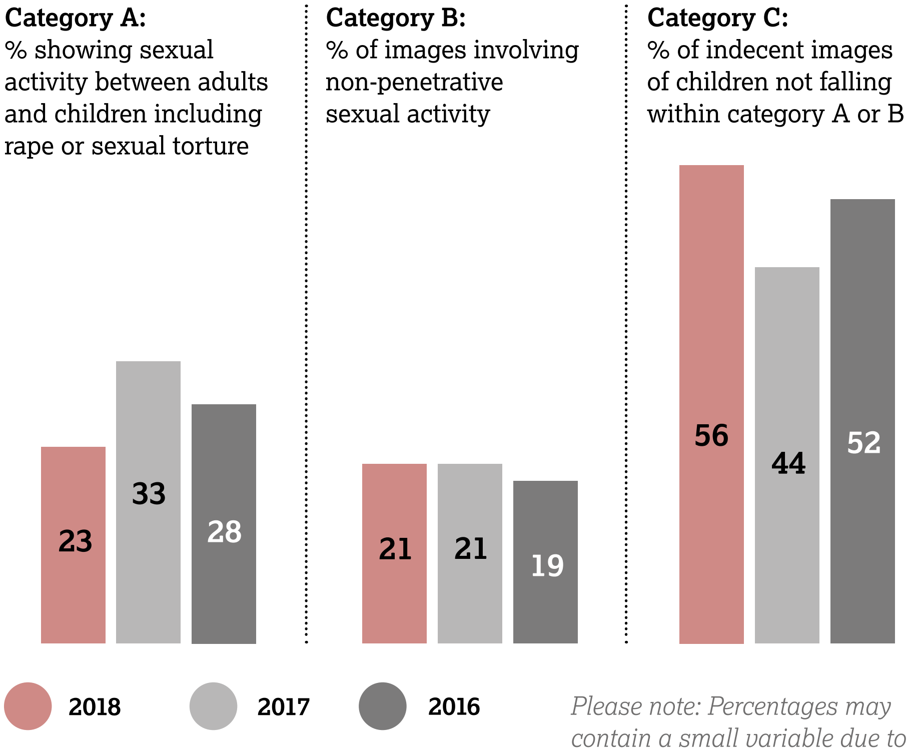
In 2018, 35% of the imagery showing children appearing to be aged 10 or younger was assessed as being Category A, compared to 16% of the imagery showing children aged 11–17.

We increasingly see more imagery of 11–15 year olds in what is termed 'self-produced' content created using webcams and then shared online. This can have serious repercussions for young people and we take this trend very seriously. We have looked into this before and the latest trends are explored in more detail further on.



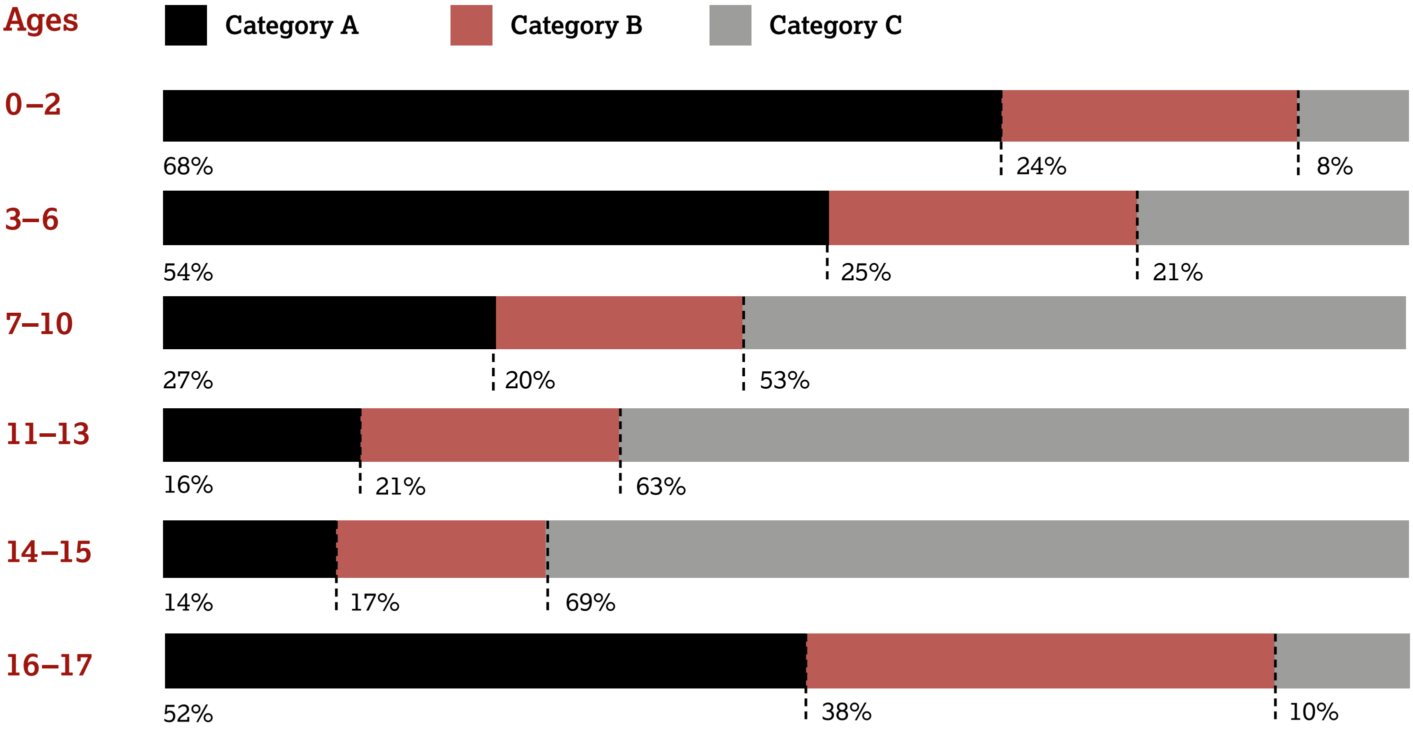


Please note: Figures are rounded to nearest whole %. A small number of the victims could not be identified as either male or female.



Please note: Percentages may contain a small variable due to URLs linking to child sexual abuse websites.

All actioned reports by age group and severity

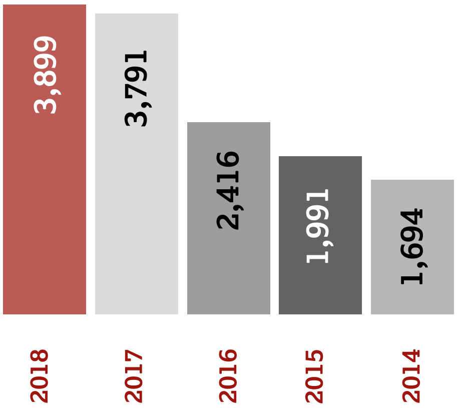


Domain analysis

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

The 105,047 URLs which displayed child sexual abuse imagery in 2018 appeared across 3,899 domains. This is a 3% increase from 3,791 domains in 2017.

This increase is consistent with the trend we first identified in 2014.



The websites containing child sexual abuse content were registered across 151 top level domains, with five (.com, .net, .co, .ru, .to) accounting for 80% of all webpages identified as containing child sexual abuse images and videos.

The 3,899 domains hosting child sexual abuse content were traced to 54 countries.

Domain names

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.

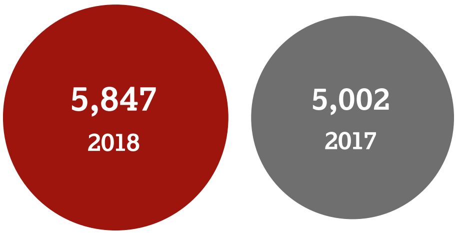
Several well-established domains including .com and .biz are known as ‘Generic Top Level Domains’ (gTLDs). Since 2014, many more gTLDs have been released to meet a requirement for enhanced competition and consumer choice in domain names, often in specific categories of content.

In 2015, we first saw these new gTLDs being used by websites displaying child sexual abuse imagery. 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 continues to be a rising trend in 2018.

In 2018, we took action against 5,847 URLs on websites using new gTLDs. These URLs were located across 1,638 different domains and 62 different new gTLDs.

In 2017, we took action to remove 5,002 URLs from websites using new gTLDs.

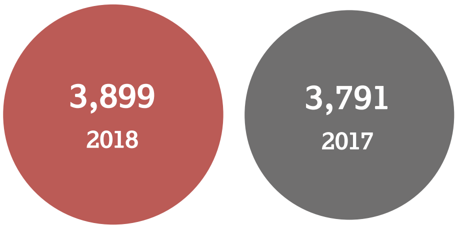


▲ 17% increase from 2017

Since 2016, we have also seen an increase in the number of domains in all TLDs being abused to distribute child sexual abuse imagery.

In 2018, we took action against child sexual abuse imagery being distributed across 3,899 domains worldwide. In 2017 this was 3,791.

And in 2016, this figure was 2,416 domains worldwide.



▲ 3% increase from 2017

This is due in part to a rising trend amongst commercial distributors, particularly distributors of ‘disguised websites’, to register individual domain names for use on their dedicated websites rather than using the services of free-hosting websites.

Which types of sites are abused the most?

In 2018, 99,900 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.

The top 10 most abused site types

Site Type	No of reports 2018	%	No of reports 2017	%
Image host	86,197	**82%**	54,539	**69%**
Cyberlocker	5,074	**5%**	11,223	**14%**
Banner site	4,558	**4%**	5,712	**7%**
Blog	3,270	**3%**	827	**1%**
Website	1,265	**1%**	1,091	**1%**
Forum	1,190	**1%**	1,984	**3%**
Search provider	818	**<1%**	297	**<1%**
Image board	783	**<1%**	752	**1%**
Video channel	772	**<1%**	587	**1%**
Social networking site	530	**<1%**	695	**1%**

2018

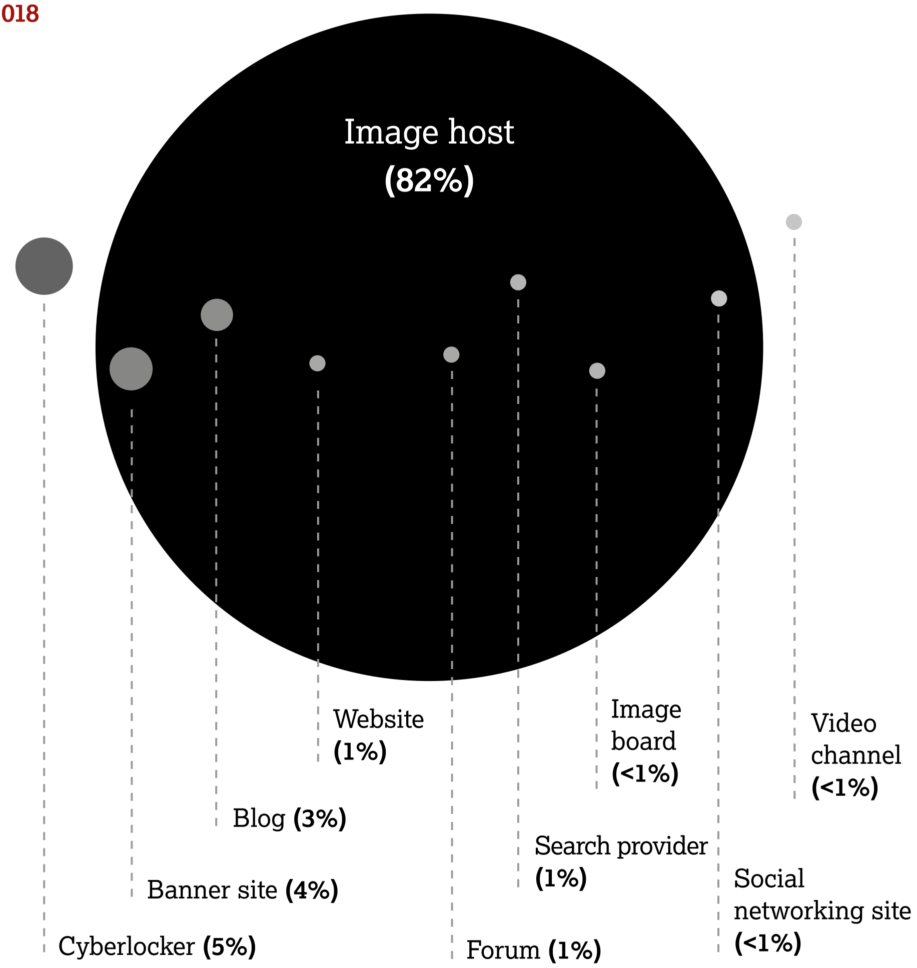


Image Hosts

Image hosts are the most consistently abused 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.

The award-winning IWF Image Hash List, launched in 2016, can help image hosts to tackle this abuse.

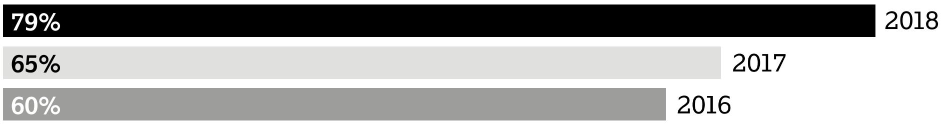
Global hosting of child sexual abuse images

In 2016, we saw that for the first time the majority of 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. In 2018, 79% of child sexual abuse content was hosted in Europe; 16% was hosted in North America.

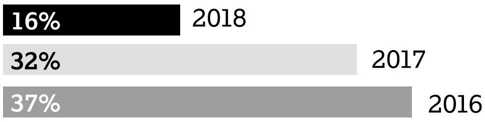
In 2018, 1 webpage containing child sexual abuse imagery was hosted in Africa. 5% of content was hosted in Asia. Images and videos hosted in Australasia, South America and in hidden services totalled less than 1% of all confirmed child sexual abuse content in 2018.

Continent hosting

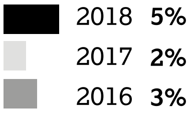
Europe (inc Russia and Turkey)
82,803 reports (2018)



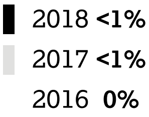
North America
16,986 reports (2018)



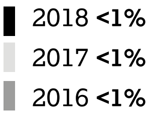
Asia
4,961 reports (2018)



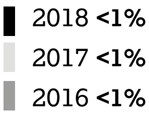
Africa
1 report (2018)



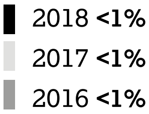
South America
25 reports (2018)

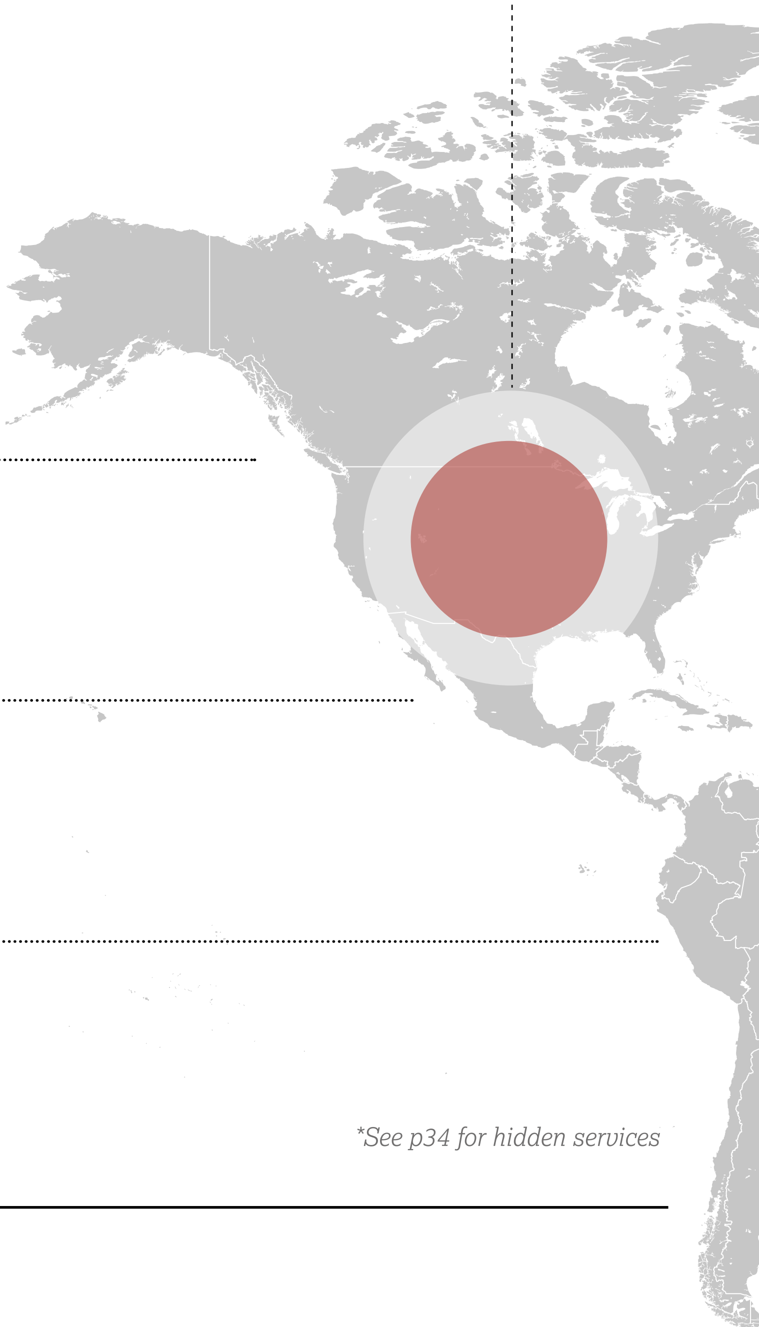


Hidden services*
85 reports (2018)



Australasia
183 reports (2018)





*See p34 for hidden services

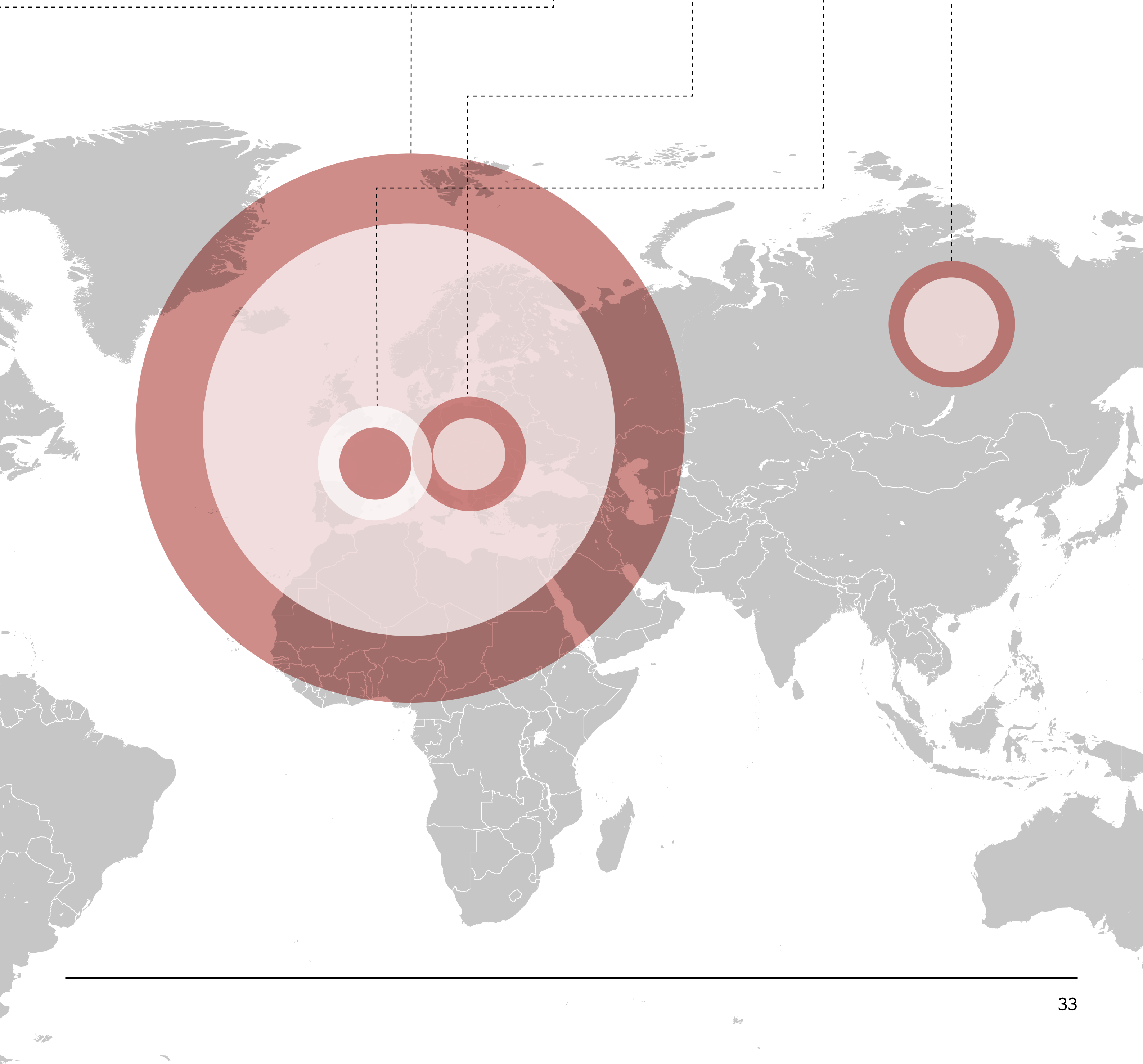
Top five countries

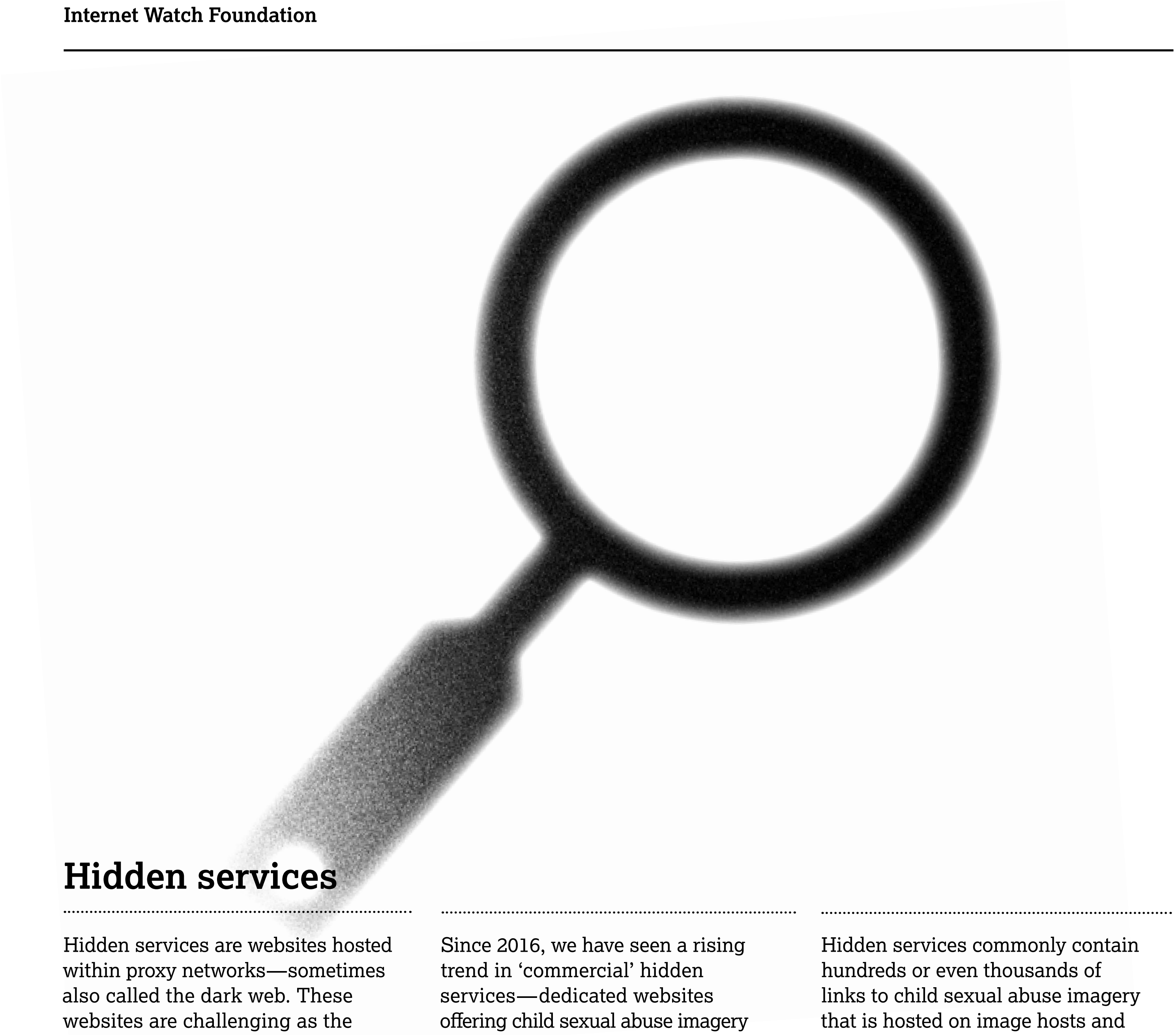
87% of all child sexual abuse URLs we identified globally in 2018 were hosted in these five countries:

■ 2018

□ 2017

	Netherlands	United States	Slovak Republic	France	Russian Federation
2018	48,900 (47%)	12,818 (12%)	11,004 (11%)	6,607 (6%)	11,877 (11%)
2017	27,970 (36%)	13,766 (18%)	4,414 (6%)	7,811 (10%)	6,335 (8%)





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. 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.

In 2018, we identified 85 new hidden services, an increase from 44 in 2017.

Since 2016, we have seen a rising trend in 'commercial' hidden services—dedicated websites offering child sexual abuse imagery for sale. Of the 44 newly-identified hidden services distributing child sexual abuse imagery in 2017, 13 (30%) were assessed as being commercial. Of the 85 newly-identified hidden services actioned in 2018, 40 (47%) were assessed as being commercial.

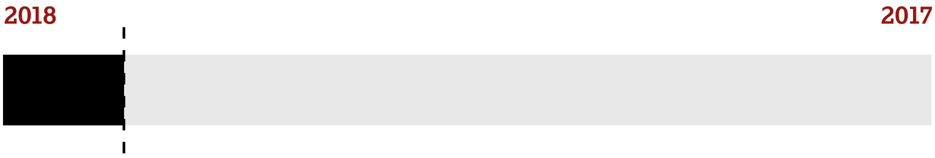
In 2018, we've also seen the first instances of 'next-gen' or 'v3' hidden services being used for the distribution of child sexual abuse imagery. Launched in late 2017, 'next-gen' hidden services use more sophisticated methods of encryption than traditional hidden services, making them harder to locate. Of the 85 newly-identified hidden services found in 2018, 4 (5%) were 'next-gen'.

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. We take action to remove the child sexual abuse imagery 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.

UK hosting of child sexual abuse imagery

The UK hosts a small volume of online child sexual abuse content. When we started in 1996, the UK hosted 18% of the global total—in 2018 this figure was just 0.04%.

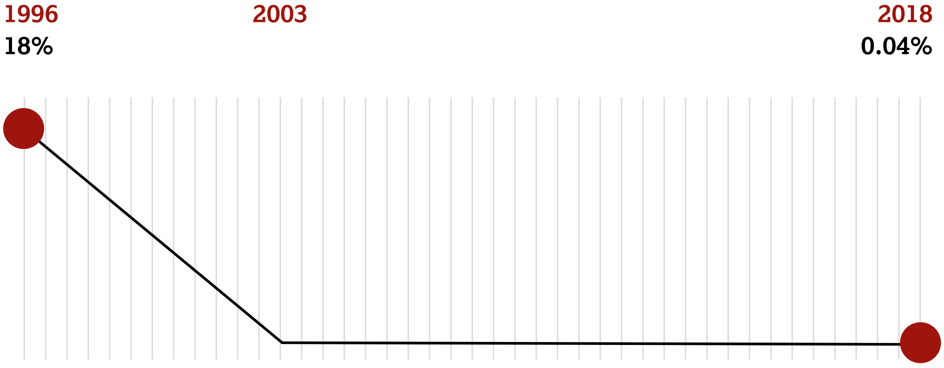
- In 2018, 41 URLs displaying child sexual abuse imagery were hosted in the UK, a decrease of 85% from 274 URLs in 2017.
- 31 takedown notices were sent to hosters of these 41 URLs. We might send one notice for several webpages and content may have already been removed by the time we get authorisation from the police.



41 URLs

274 URLs

▼ 85% decrease from 2017



UK child sexual abuse content removal in minutes

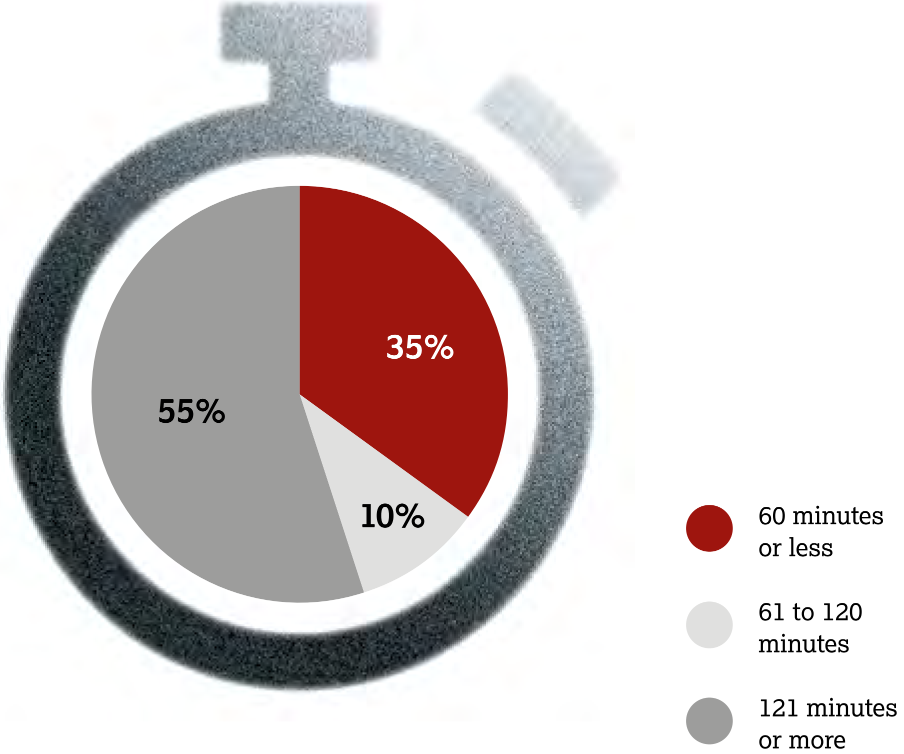
In partnership with the online industry, we work quickly to push for the removal of child sexual abuse content hosted in the UK. The 'take down' time-clock ticks from the moment we issue a takedown notice to the hosting company, to the time the content is removed.

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.

14 companies' services in the UK were abused to host child sexual abuse images or videos during 2018. We issued takedown notices to companies, whether they are our Members or not.

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

2018



They discovered the monsters were beatable

Word spread about how the monsters could be defeated.
People invented new tools and forms of defence. They studied the language of the monsters and how to use it against them. They found ways to see through their disguises.

Our services

IWF URL List

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

During 2018:

The list was sent across all seven continents.

100,682 unique URLs included on the list

77,082 unique URLs

▲ 31% increase from 2017

376 new URLs on average, added each day

298 new URLs

▲ 26% increase from 2017

6,046 URLs contained on the list on average each day

3,473 URLs

▲ 74% increase from 2017

IWF Hash List

Each image can be given a unique code, known as a hash. A hash is like a digital fingerprint of an image. IWF creates hashes of the child sexual abuse content we see and we add these to our Hash List. The list of these hashes can be used to find duplicate images. This makes us more efficient at what we do. It also means the Hash List could stop the sharing, storage and even the upload of child sexual abuse content.

- At the end of 2018, the list contained hashes relating to 345,961 individual images.
- Of these hashes, 83,456 relate to the worst forms of abuse—images of rape or sexual torture of children.

This means that in 2018, our analysts assessed 4,361 images each, alongside assessing public reports, and actively searching for child sexual abuse images and videos.

Keywords List

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

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.

- In December 2018 the Keywords List held 453 words associated with child sexual abuse images and videos.

Looking ahead:

Using IWF's intelligent crawler we can identify more efficiently additional keywords associated with imagery appearing on child sexual abuse websites. In 2019 our analysts will perform a manual review of these terms for inclusion in IWF's Keywords List.

During 2019, we will be working on a project in partnership with Nominet which may assist in identifying additional terms used by criminals when they are looking for child sexual abuse imagery via search engines.

Newsgroups

Our Hotline team monitors the content of newsgroups and issues 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 they can be removed.

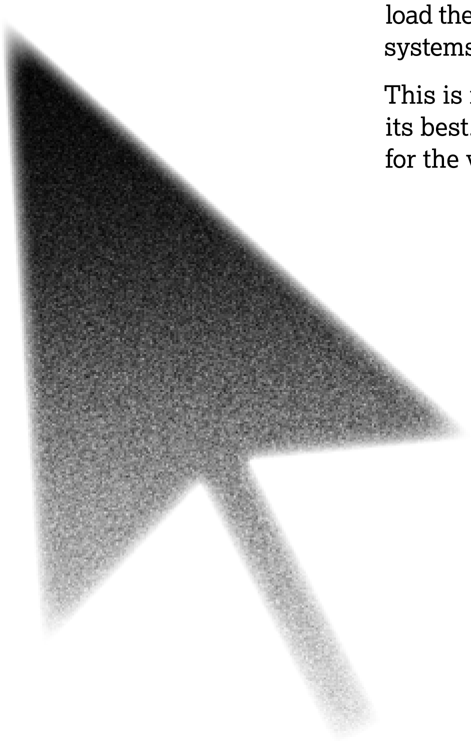
We are one of only a handful of hotlines in the world that processes reports on newsgroups.

Throughout 2018, we monitored and reviewed newsgroups and issued takedown notices.

- We processed 995 reports alleging child sexual abuse images hosted within newsgroups.
- 922 takedown notices were issued for newsgroups containing child sexual abuse images (1,729 in 2017). One takedown notice can contain details of several newsgroup postings.
- 29,865 postings were removed from public access (43,767 in 2017).
- After monitoring newsgroups, we recommended our Members do not carry 348 newsgroups containing or advertising child sexual abuse images and videos.

New technology

We harness cutting edge technologies and combine this with expert 'human' analysts to tackle online child sexual abuse imagery.

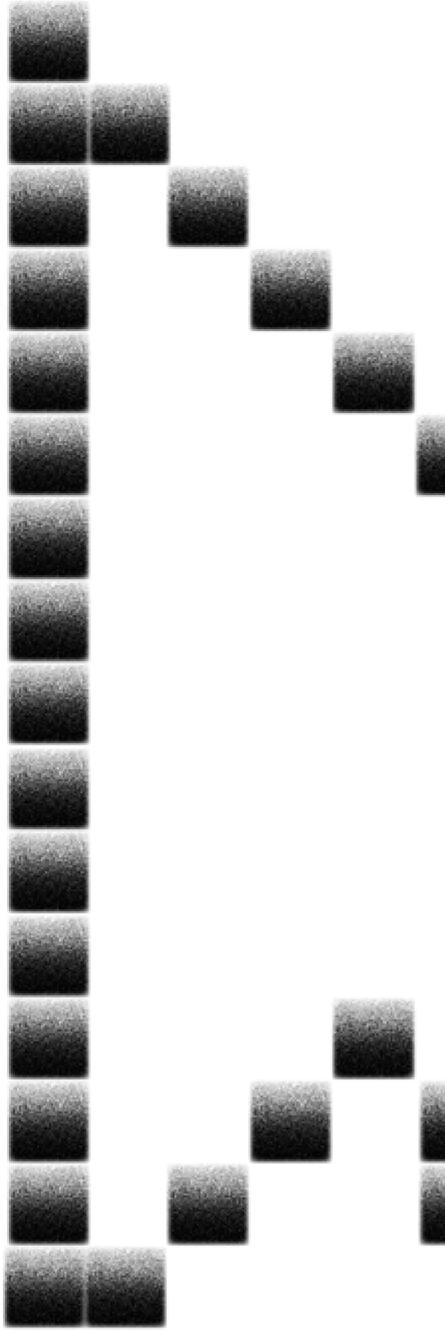


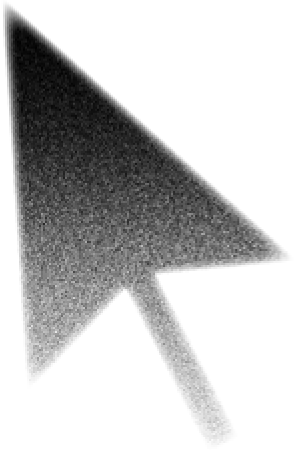
Video hashing

2018 saw the full roll-out of PhotoDNA for video hashing. IWF launched the Hash List, after a successful pilot in 2015. Back then, the technology was ground-breaking, creating a huge library of known criminal images that could be given a 'digital fingerprint' and identified online. However, there was a drawback; this only worked for pictures—videos couldn't be tagged.

That's now changed. With the help of Microsoft PhotoDNA for video, we took our hashing to the next level. We began identifying and tagging videos, so that they could be added to our extensive Hash List. This was a breakthrough. It meant that all the images and videos that our analysts confirmed as containing criminal material could be put on our list and given to tech companies. They could then make sure that offenders would never be able to load these disturbing films onto their systems again.

This is revictimisation-prevention at its best. And it's a huge step forward for the victims of this horrific abuse.





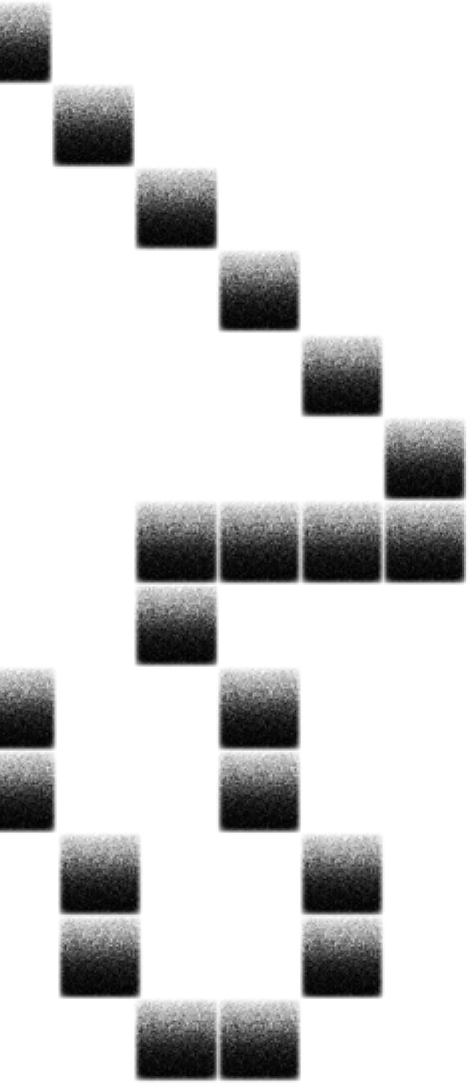
New reporting system

Due to the unique nature of our work, we've always needed a bespoke report management system (RMS). It allows us to receive, process and action the all-important reports that are made to our Hotline.

This year we've launched RMS4. It brings automation and integration to our Hotline analysts; it has streamlined the reporting system and allowed our intelligent crawler to be integrated, both of which were major factors in the record number of reports our analysts have been able to confirm this year.

All this, whilst maintaining the high level of accuracy and expertise we demand. This is more revolution than evolution.

In addition to this, RMS4, like its predecessor, allows direct reporting of suspected child sexual abuse imagery that's been identified by our tech Members' own abuse teams. Working together has never been as efficient.

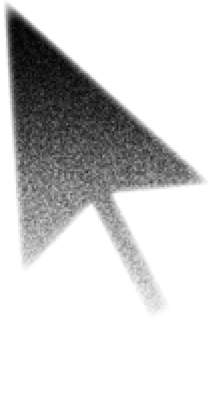


The future of tech and Artificial Intelligence (AI)

Looking to the future, we are already working and experimenting with AI systems. Auto-classification will become part of our everyday work. So, we're working on projects with tech partners, to give IWF services the edge.

However, we believe that while harnessing the power of new AI technology is incredibly important, it needs to be balanced with real people—our experts. We believe that what success looks like in our world demands a balance of human expertise and technical development.

Put simply, we're working to put the best new technology into the hands of some of the world's best experts. And judging by our 2018 figures, it's an equation that works.



Commerciality and trends

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 105,047 webpages we confirmed as containing child sexual abuse imagery in 2018, 6,941 (7%) were commercial in nature. This is a decrease on 2017, when we took action against 8,976 (11%) commercial webpages.

In 2015, we assessed 21% of the webpages containing child sexual abuse imagery as commercial. Since then, we have seen a decline. We believe this is due in part to changing methods used by criminals to evade detection, such as the increase in disguised websites.

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 anonymously browse the internet. 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. This is an emerging trend, however of the 86 instances identified to date, 46 (53%) related to commercial websites which we had not previously seen.

We will continue to monitor this trend and share information with our sister hotlines and law enforcement to ensure these websites can be removed and the distributors investigated.

In addition to taking action to have these websites removed, we also capture payment information displayed on commercial websites, enabling us to provide alerts to our Members in the financial industry to prevent the misuse of their services and further disrupt distribution of the imagery.

Web brands

Our Website Brands Project started in 2009. Since then, we have been tracking the different 'brands' of dedicated child sexual abuse websites. These 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 4,452 unique website brands.

Our ongoing analysis of hosting patterns, registration details and payment information indicates that the majority of these dedicated websites are operated by a small number of criminal groups. In 2018, the top 20 most prolific brands were apparently associated with just 6 distribution groups.

In 2017, we identified changes in the methods used by commercial distributors to create their websites. Increasingly, the names and titles of these websites were dynamic, meaning that they change each time the page is reloaded. This resulted in a large increase in the number of active 'brands' selling child sexual abuse imagery. During 2018, our analysts have devised different methods to establish when these sites still represent the same 'brand' despite changes to the name and title. In response, we have adopted new processes for categorising such sites to ensure the total number of 'brands' we encounter continues to be accurately reflected.

- In 2018, we saw 1,245 active brands, compared to 1,624 in 2017.
- Of these active brands, 446 were previously unknown to us, compared to 1,263 in 2017.

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.

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. When we first identified this technique, we developed a way of revealing the criminal imagery, meaning we could remove the content and the websites could be investigated. But the criminals continually change how they hide the criminal imagery, so we adapt in response.

- In 2018, we uncovered 2,581 websites which were using the 'digital pathway' method to hide child sexual abuse imagery, a decrease of 11% on the 2,909 disguised websites identified in 2017.
- During 2018, we also identified a group of disguised websites which are apparently exploiting digital advertising networks and legitimate brand owners to fraudulently generate additional revenue. In 2019, we'll be working on a project in partnership 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.

Disguised websites continue to be a significant problem. 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.

'Self-generated' content

We increasingly see what is termed 'self-generated' 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.

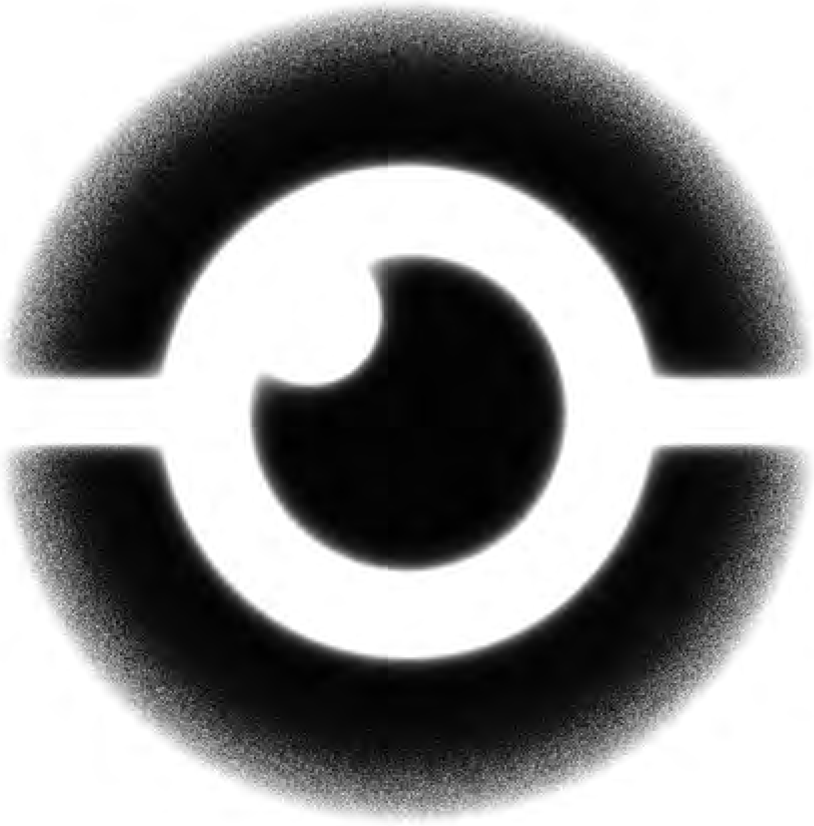
In response, we decided to undertake an in-depth study which was published in May 2018. The study was funded by Microsoft and the full report is available on our website.

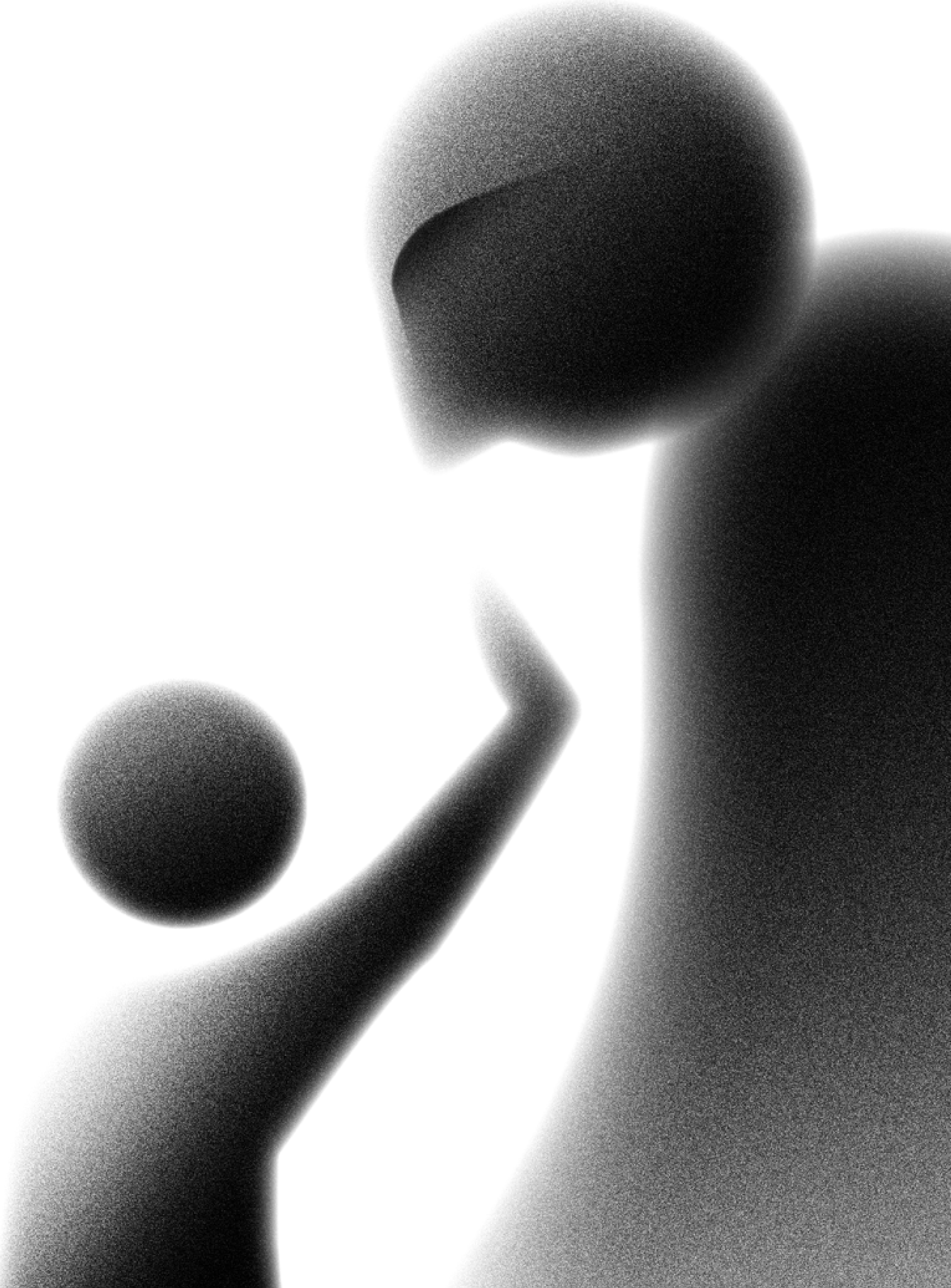
We take this growing trend very seriously. As a result, we adapted our bespoke systems to ensure we can continue to capture changes in this trend over time.

Of the 72,954 webpages actioned in the last six months of 2018, 1 in 4 (27%) was assessed as containing a self-generated image or video. We mostly see this imagery being produced through livestreaming services, which is then captured and distributed widely across other sites.

These images predominately involve girls aged 11 to 13 years old, in their bedrooms or another room in a home setting. Of the 27% of webpages containing 'self-generated' child sexual abuse imagery, 94% depicted children assessed as being 13 years or under; 78% depicted children assessed as 11–13 years of age; and 16% depicted children assessed as 10 years or under. We found 44% of these webpages contained imagery at the highest levels of severity including rape and sexual torture (Categories A and B).

We identify this imagery and work with industry partners to get it removed. We will also continue to work with our partners, including the UK Safer Internet Centre, to raise awareness of trends in the distribution of self-generated content and inform strategies for better protecting victims of this form of abuse.





Many people joined in

Across the world, concerned
people joined the quest.
In every city and every country there
were new battles to fight.
Sometimes people refused to believe
in the invisible children
and asked for evidence. Sometimes people
thought the battle would never be won
and needed encouragement.
Remembering the invisible children
helped them work
even harder.

Our Members

£78,030+

amazon.com

AT&T

sky

BT

CISCO

facebook

£52,020+

Oath:
YAHOO!

paloalto
NETWORKS

THE
UKCARDS
ASSOCIATION

McAfee

TATA
COMMUNICATIONS

Symantec

£20,810+

WatchGuard

ATLASSIAN

SANDVINE

SONICWALL

WEBROOT
Smarter Cybersecurity

The FA
For All

SOPHOS

Barracuda

ROBLOX

zscaler
Secure. Everywhere.

£5,200+

Manchester
Metropolitan
University

ELLIPTIC

SAFEDNS

iomartcloud

Afilias

donuts

ICM
REGISTRY

names.co.uk

ISPAUK

JT

neustar

SYSTEM1

SafeToNet

seethelight

Sheffield
Hallam
University

WEBSHIELD

£15,605+

Adobe

JAGEX

The Walt Disney Company
UK & Ireland

Allot
communications

BlackBerry

£2,600+

askfm

LONDON

idaq
NETWORKS

NUI Galway
OÉ Gaillimh

E2BN

futuredigital

UseNeXT

IT Systems

netopian

NOTTINGHAM
TRENT UNIVERSITY

Relish

DHIRAAGU

UNIVERSITY OF
SURREY

University of
Hertfordshire UH

Securus

Google

Microsoft

TalkTalk
For Everyone

vodafone

Virgin media

Telefonica

£26,010+

Dropbox

linx

FORCEPOINT

TREND MICRO

PA

Three.co.uk

BAE SYSTEMS
INSPIRED WORK

PayPal

FORTINET

GIGANEWS

£10,405+

adaptivemobile

badoo

BBC

BLOCKCHAIN
INTELLIGENCE GROUP

G2 Web Services

crisp

CHAINALYSIS

CYREN

exa networks

eSafe

impero

Jisc

NetSupport

netsweeper

Leeds
CITY COUNCIL

LGfL

Lightspeed Systems

Openwave Mobility

Omicron

TESCO mobile
www.tescomobile.ie

KCOM

kik

schools BROADBAND

securly://

POST OFFICE

Your Public Interest Registry

RM Education

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

NOMINET

iboss
NETWORK SECURITY

zen

zoom

zvelo
We categorize the Web

Royal Mail

sure.

NetClean

smoothwall

STACKPATH

£1,040+

4D

Association of Network Managers in Education
anme

avanti

BRIGHTSTAR

C/THREE

CYDA

Diladele B.V.

DNSFilter

evolveODM

KRYSTAL
Honest. Reliable. Personal.

National Online Safety

OAKFORD

OneTek
BUSINESS SOLUTIONS

Opendium
e-Safety

plan.com

QUICKLINE

senso.

TecSmart

The Social Element

usenet.nl

USENET
EXPRESS

XS NEWS
USENET ACCESS

yubo

Jigidi

rawstream

Working with industry

Reducing child sexual abuse material with our Members

We proudly team up with other countries and companies to tackle online child sexual abuse material.

Our Members

Our Members mean everything to us. Without them, our important work would not happen. We work with the world's biggest and most far-reaching companies, along with small-scale start-ups with great ambitions. We help them keep their networks safe by giving them cutting-edge solutions to prevent and remove child sexual abuse imagery on their platforms and in their services.

Our Members come from all corners of the globe and they deploy our technical solutions across all continents. Nearly two thirds of new companies joining us in 2018 were based outside of the UK. This isn't a surprise; online child sexual abuse imagery does not respect international boundaries. Universities are learning the benefits of membership too, with seven joining us this year.

We welcome Members from every sector: hosting companies, domain registries and registrars, filterers, games companies, payment companies, virtual currency companies, mobile operators, search engines, social media, cyberlockers, trade organisations and those joining for CSR reasons—all keen to play their part in making sure there is no place for this criminal material.

Only by working together can we make a difference.

"Roblox is dedicated to providing both our players as well as parents with the resources necessary to ensure the safest experience possible on our platform. We look forward to working with the IWF and other Member companies to play an active role in helping keep children safe on the internet."
Remy Malan, Roblox.

"The IWF are a fundamental part of our safety strategy, through the professional support and advice they offer as well as supplying us with invaluable keywords, which we integrate into our ever-evolving safety heuristics. We are delighted to partner with the IWF, and we would urge any company with an online presence to foster a relationship with them and support the fantastic work they do."
Steve Wilson, Jagex.

Our policy work

Shaping policy to make the internet a safer place

The right legislative and policy environment is needed to allow us to work with partners to remove child sexual abuse material from the internet. That's why we help shape policy in the UK, EU and relevant international countries.

Regulation: The UK Government has committed to making the nation the "safest place in the world to go online" and we've been actively contributing to help shape what this could look like. This topic is also high on the agenda of the Home Secretary, the Rt. Hon. Sajid Javid MP, who praised our work in a passionate speech.

Advertising: The Home Secretary asked us to look into legitimate adverts which appear alongside child sexual abuse material online and whether offenders were able to generate money by making this happen. We provided a report on this work in December and we're looking at how we can work with partners on this issue through 2019.

Online grooming and livestreaming: We went to Microsoft's HQ in Seattle, USA, with the Home Secretary, other NGOs and tech companies to discuss challenges around online grooming. Livestreaming was also discussed during a panel chaired by our Deputy CEO and CTO, Fred Langford.

E-privacy: We've shared our views with the European Union which helped amend proposals for a new e-privacy directive. This was important because it might have prevented tech companies from scanning their networks to remove online child sexual abuse material.

Brexit: Brexit could have big implications for our future funding as 10 percent comes from the European Union. We raised this concern at a roundtable meeting with both the European Commission (EC) and British MEPs. We were pleased to find out that our funds are secure until the end of 2020 after the EC approved our UK Safer Internet Centre funding application. The UK Government has also pledged to continue that funding during any Brexit transition period.

Ministerial visits: We welcomed the DCMS Secretary of State, Rt. Hon. Jeremy Wright QC MP, and the Parliamentary Under Secretary of State, Rt. Hon. Victoria Atkins QC MP, to the IWF. We discussed how to help make children and young people safer online, and how this fitted with a forthcoming White Paper on online harms.

Engagement: Our local MP, Daniel Zeichner MP launched our 2017 Annual Report with a roundtable discussion with tech companies, policing stakeholders and Government representatives. We've also been actively raising our strategic priorities with more than 30 Parliamentarians throughout the year.

Consultations and committees: We like to contribute to consultations and committee discussions and where possible, we publish our responses on our website. During 2018, our CEO Susie Hargreaves gave evidence to the House of Commons Science and Technology Committee on its inquiry into Social Media and Screen Time, the House of Lords Communications Select Committee, and she was reappointed to the revamped UK Council for Internet Safety Executive Board. We're also the only Hotline and only UK-based organisation to secure observer status to the Lanzarote Committee, which plays a crucial role in monitoring the convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

The IWF also secured Core Participant Status on the Independent Inquiry into Child Sexual Abuse when they examine the role of the internet. Our CEO Susie Hargreaves will attend as a representative.

IWF Champions: Our Champions have continued to raise our issues in Parliament on our behalf. A highlight was the hugely supportive and passionate speech in the House of Lords by Baroness Floella Benjamin OBE who promoted our portals programme and encouraged Commonwealth nations to do all that they can to tackle child sexual abuse.

Our Reporting Portals

Empowering people around the world

IWF Reporting Portals enable countries and territories without the financial means or resources, to tackle online child sexual abuse imagery. We're proudly launching 50 Reporting Portals by 2020.

As the portals are gateways into our Hotline in the UK, they enable us to take reports from people around the world. This fulfils an important requirement of the United Nations (UN) Convention on the Rights of the Child, the UN's Sustainable Development Goals, particularly to end the abuse, exploitation, trafficking and all forms of violence and torture against children, and the WePROTECT Model National Response (MNR).

"In Angola, there are 13 million users of the mobile network and more than five million access the internet through a mobile phone, tablet, computer and other means. Our children today grow up in the so-called digital era which supports their education and communication, but which can also present serious risks. Children deserve to grow and develop, free from prejudices or harm caused by our inadequate actions, inactions or attitudes of negligence. The launch of this portal is an added value for the Angolan State in the promotion and protection of the Rights of the Child and the fulfilment of the 11 Commitments of the Child. With this IWF Portal, Angola joins the campaign against sexual abuse of children on the internet."

The Angola Secretary of State for Human Rights and Citizenship, Dr Ana Celeste Cardoso Januário.

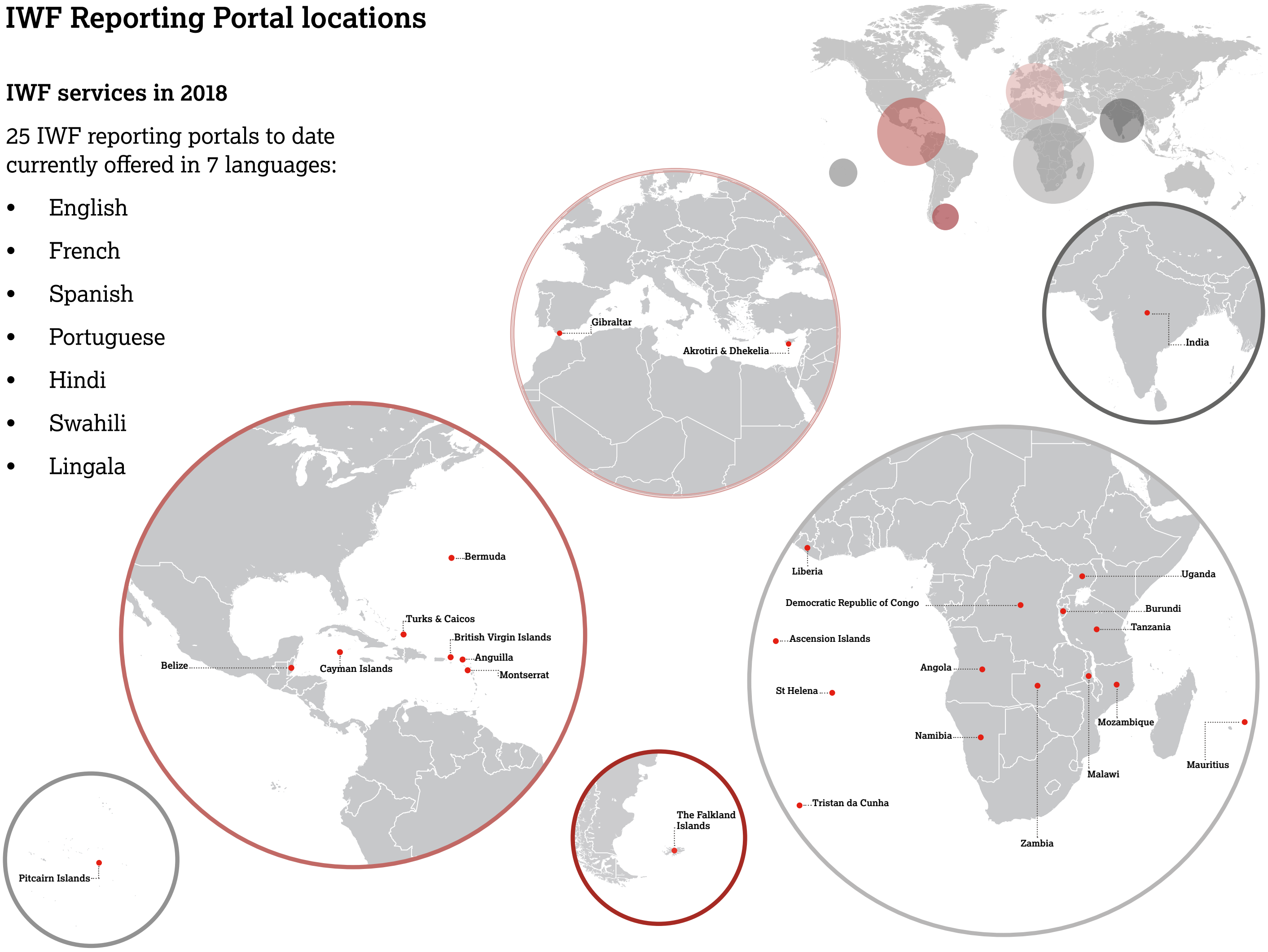
Angola roundtable participants. Luanda – July 2018

IWF Reporting Portal locations

IWF services in 2018

25 IWF reporting portals to date currently offered in 7 languages:

- English
- French
- Spanish
- Portuguese
- Hindi
- Swahili
- Lingala



Mozambique, Belize, Malawi, the Democratic Republic of Congo, Angola, Zambia and Burundi have joined the portals network in 2018. We're pleased that governments are committing to tackling this online crime, and that national bodies—including industry, NGOs and police—are giving professionals and citizens the tools to remove criminal imagery. This work has increased the global awareness of online dangers posed to children in the digital age.

"I strongly believe that the soul of any nation is reflected in how well it treats its most vulnerable. It takes a community in the largest sense of the word, to raise a child and all of us, irrespective of who we are and where we are, must play a part in that community to protect and defend children."

Theodore Menelik,
Director of Menelik Education,
Democratic Republic of Congo

Our international portal partnership in action

Our highly trained Internet Content Analysts helped the Royal Cayman Islands Police Service (RCIPS) to convict a sex offender.

The RCIPS were faced with an overwhelming number of images and URLs to analyse, so we helped them. Thanks to the portal partnership, we swiftly assisted their investigation by confirming the images were criminal which contributed to the offender's conviction. The Caymans Islands Portal is now integrated into the RCIPS mobile phone app, meaning that citizens can easily connect with the Reporting Portal whenever they need it.

Caring for our people

At the IWF, people are at the heart of everything we do. Our Internet Content Analysts are quite simply the best. And 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. What they do is a tough job. It takes a special person to be able to view disturbing images of children each working day.

Just 13 analysts assessed almost 230,000 reports in 2018. Whilst they're trained to identify criminal imagery, they're exposed to all sorts of hideous content they often don't expect to see.

It's our job to look after these incredible people and we take this responsibility very seriously. The health and emotional wellbeing of our analysts is our top priority.

So, IWF have a gold-standard welfare system in place.

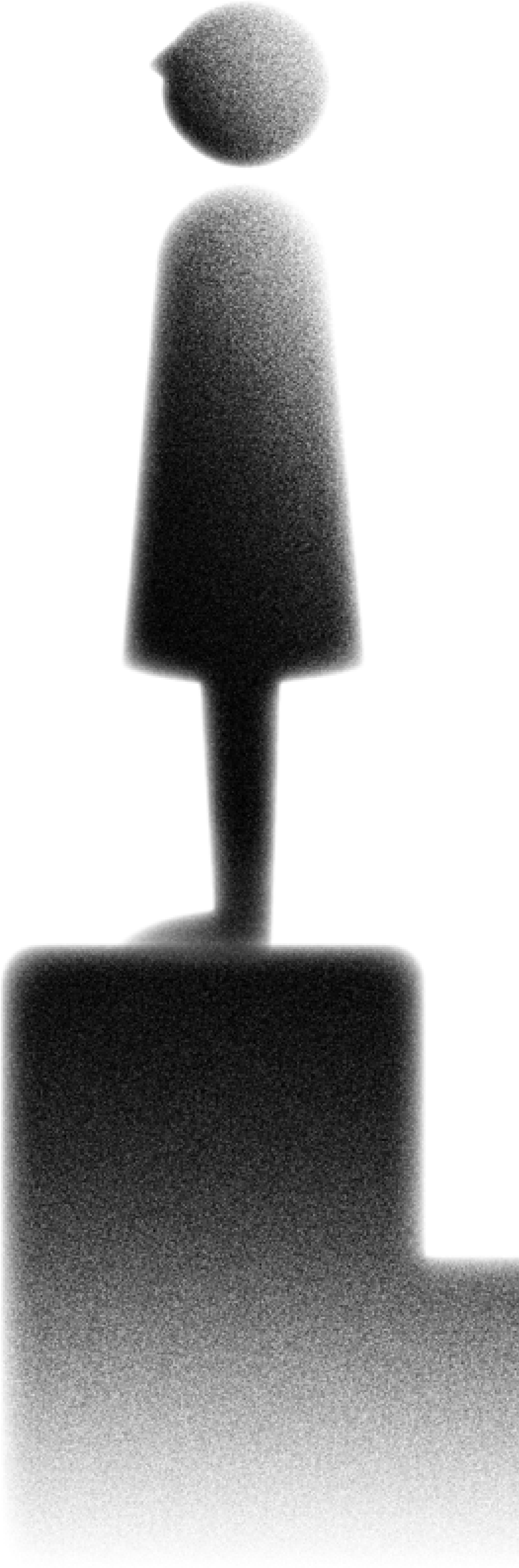
All new analysts go through a specially-developed training programme to help them mentally process and cope with exposure to disturbing images.

Our analysts' working hours are strictly monitored; they take regular timetabled breaks and are encouraged to take more breaks as and when they need.

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.

We go the extra mile for our staff, because they go the extra mile for you. It's the right thing to do.

Heidi Kempster, COO



UK Safer Internet Centre

The UK Safer Internet Centre is a European Commission funded project, delivered by Childnet International, SWGfL, and the IWF.

Together we encourage the responsible use of technology and make the internet a safer environment for children and young people with:

1. An Awareness Centre run by Childnet International 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.
2. A Helpline, by SWGfL, offering independent advice to professionals working with children and young people with online safety issues such as privacy concerns, inappropriate behaviour and grooming.
3. A Hotline, by the IWF, to anonymously and safely report and remove online child sexual abuse imagery and videos, wherever they are found in the world.

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, policymakers and other stakeholders, to join together in helping to create a better internet.

In 2018, it was themed 'Create, Connect and Share Respect: A better internet starts with you'.

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 said they learned about safety features online such as reporting or privacy.
- Three quarters said they would be more careful about what they do or say on social media.

The UK Safer Internet Centre can be found at www.saferinternet.org.uk

UK Safer Internet Centre

Childnet International

SWGfL

IWF Internet Watch Foundation

Once there was a knock at the door

One day the child who lay awake
wondering about the other
invisible children heard a knock at the door.
There were new voices
she had not heard before and they
seemed like kind voices.
As they came nearer, she wondered
what they would say if they could see her.
Then she heard someone say,
‘Are you OK? We are here to help’.
Their eyes were looking
straight at hers.

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 will enable 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.

Criminally obscene adult content: Images and videos that show extreme sexual activity that's criminal in the UK.

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

linx

WePROTECT GLOBAL ALLIANCE
END CHILD SEXUAL EXPLOITATION ONLINE

End Violence Against Children
THE FUND

To be continued

**Our work continues every hour of every day.
Follow us on social media for updates.**

Internet Watch Foundation

Discovery House
Chivers Way
Histon
Cambridge
CB24 9ZR

E media@iwf.org.uk
T +44 (0) 1223 20 30 30
F +44 (0) 1223 86 12 15

Internet Watch Foundation
@IWFHotline

#onceuponayear

iwf.org.uk

Charity number: 01112398
Company number: 03426366

INHOPE

UK Council for Internet Safety

ISO 27001
BUREAU VERITAS
Certification

Co-financed by the Connecting Europe Facility of the European Union

UK Safer Internet Centre

‘The child decided she must be invisible. Sometimes, when she was finally alone at night, she wondered how many other invisible children were out there.’

This is the story of a year in the life of the Internet Watch Foundation.

We identify images and videos showing the sexual abuse of children, wherever they are found on the internet. We then work globally to get them removed.

The children in these pictures and videos are real. The suffering captured in this imagery and the knowledge that it could be shared online 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.

IWF
Internet
Watch
Foundation