The Annual Report
2021

Internet Watch Foundation

Contents page

Homepage

In 25 years

- 1,800,000 reports have been assessed by IWF analysts
- 970,000 child sexual abuse reports have been actioned for removal.

As each report contains at least one, and sometimes thousands of images, this equates to millions of criminal images removed from the internet.

About IWF > Who we are

We detect, disrupt, remove, and prevent online child sexual abuse material using our expertise and resources as effectively as possible.

The Internet Watch Foundation (IWF) is a technology-led, child protection organisation, making the internet a safer place for children and adults across the world.

We're a not-for-profit organisation working closely with police, governments, and NGOs globally, who trust our work.

Child sexual abuse images and videos are just as much a weapon as a knife.

We actively search for this imagery and for the past 25 years, we've given people a safe place to report it to us, anonymously, now covering 50 countries including the UK.

We assess every report we receive. If it shows the sexual abuse of a child, we make sure the image or video is removed from the internet.

To do this effectively, we develop technology-for-good: We provide bespoke services, products and datasets to our industry Members to prevent the imagery from re-appearing and make it harder for offenders to find and share.

We care. 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 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 remove this material for good. And to show every child there is someone out there who cares enough to help.

About IWF > Chair's Foreword

It didn't surprise me that the IWF has had another record year. The sad truth is that there is a proliferation of images and videos of child sexual abuse on the internet.

I am constantly impressed that the team's energy and commitment to meet the scale of the challenge never seems to falter and in fact, they are always looking for new and innovative ways to tackle the problem.

Having been Chair for four years, I know that this is an organisation, supported by an active and engaged Board, that is never going to stand still whilst there remains a single image or video on the internet of a child being sexually abused.

Over the past year, this record work has taken place against the backdrop of both continued lockdowns and impending future regulation through the Online Safety Bill. This Bill will not only impact on the work of our Members but on the work of the IWF itself.

Working collaboratively has been our overriding approach to this to ensure that we get 'good' regulation which actively helps to fight online child sexual abuse. We must not undo any of the work and relationships that the IWF has forged around the world over the past 25 years on behalf of all the children who have been sexually abused and had their images circulated. The IWF's credibility and track record speaks for itself which is why we need to be part of the solution.

This is why I have been working closely with the IWF team on a programme of engagement and consultation with the Government, Parliamentarians, Ofcom and of course our Members. Regulation can only be effective with the close involvement and cooperation of the internet industry. The IWF is a trusted broker between the regulator and the industry.

Any role that the IWF plays in the future will be with the support of its Members, which is why I have worked closely with the Chair of IWF's Funding Council and a working group of Members to review our governance arrangements. This has resulted in some changes being made which provide the IWF with the formal independence it needs from industry to undertake discussions about possible future functions in the regulatory regime. It also provides reassurances to the Members that we will not change our remit or fees without their agreement.

Another challenge during the year was to ensure that if companies introduced end-to-end encryption onto their platforms that there were also necessary child safety protections in place. The IWF supports encryption in principle and does not demonise technology per se, but is also clear that any introduction of end-to-end encrypted services that lead to an inability to detect child sexual abuse must be set against having child safety mitigations in place. The IWF stands ready to work with technology companies to achieve this and is exploring potential technical solutions.

As Chair I lead the Board of Trustees and I know I speak for them all when I say we have complete confidence in the team. Year after year we see how the IWF is a really well run organisation. Behind the big numbers produced by the Hotline, are excellent financial, HR, communications, membership and technical functions who all play their part. This doesn't mean they are complacent or have ever said 'job done' because the challenge grows daily but rather than getting ground down by it, they rise to meet every new challenge.

About IWF> CEO's Foreword

Marking 25 years of combatting child sexual abuse imagery on the internet is bittersweet; I'm so proud of this organisation – which I have led for more than 10 years now – and equally sad at the large volumes of criminal imagery we're finding.

I asked Professor Hany Farid, who's dedicated his professional life to creating technology to help stop this imagery, for his reflections on the past 25 years, and he didn't hold back. We've also captured stories from our analysts. We're breaking new ground in this battle, and it's important to capture the voices of those resilient individuals who work to stem the repeated abuse of sexually abused children.

In 2021 the UK's National Crime Agency revised their estimate of the number of people who pose a sexual threat to children in the UK. They put it between 550,000 to 850,000. Whilst it's a great achievement that thanks to our work, and that of UK hosting companies, such little child sexual abuse material is hosted in the UK, it means very little when so many of its population want to view it, and when year-on-year our numbers only show that the situation is getting worse.

This year, we were able to find so much more of this material than ever before. We could do this thanks to huge strides within our Hotline to work more efficiently, using technology better and being able to employ an additional two analysts.

Additionally, we've developed a way to reduce the number of off remit reports being presented to our analysts with an improved reporting process for the public. This has saved our analysts needing to assess nearly 10,000 off remit reports, allowing them instead to focus on their proactive searching for this material.

We launched IntelliGrade – a world first which allows our dedicated team of graders, funded by a Thorn grant, to quickly assess and 'hash' (create digital fingerprints) child sexual abuse images from the UK Government's Child Abuse Image Database (CAID). What's new, is that this grading process allows the hashes to be compatible with multiple legal jurisdictions around the world. And at the same time, we're adding large volumes of metadata which allows us to understand more about the sexual abuse happening to the children pictured, and provides a way for technology companies to build and train the tech of the future.

Tackling child sexual abuse material is ever challenging, but by working collaboratively and forging great partnerships with technology companies, governments globally, law enforcement and the third sector makes it possible to do this effectively.

Finally, a word for our team of dedicated analysts: They spend each and every day assessing some of the most challenging content imaginable. They do this because they know that for every image or video they remove, it stops that child being revictimised and gives that child some hope.

About IWF > Home Secretary

The Rt Hon Priti Patel MP

Home Secretary

Online Child Sexual Exploitation and Abuse is a truly abhorrent crime and the United Kingdom is determined to be a leader in the global initiative to stamp it out.

Tragically, the severity of online CSEA offending only deepened during the pandemic. And as we return to normality, offenders are continuing to take advantage of the increased amount of time children are spending online and our ever greater reliance on technology for communication, entertainment and education as they carry out their despicable acts.

Since I became Home Secretary, the Home Office has launched its Tackling Child Sexual Abuse Strategy. The Government is also introducing the Online Safety Bill, a world-leading piece of legislation that will make the UK the safest place in the world to be online for both children and adults.

The Internet Watch Foundation remains instrumental in safeguarding children from vile predators. This annual report provides valuable insight into the changing nature of online child abuse and the blurring of lines between children's physical and digital lives.

I was pleased to see the launch of the Report Remove tool in June, a pioneering online resource allowing children to request removal of images of them that have been circulated online without their consent. This will empower victims of child sexual abuse to protect themselves from being traumatised once again.

However, this report also draws our attention to the shocking fact that more cases of Child Sexual Exploitation were investigated by the IWF in 2021 alone than in the first 15 years of its existence. This highlights the industrial scale at which these monstrous criminals are working.

So I welcome the Internet Watch Foundation's continued work on these issues because, while this is a complex area, few things are more important than the protection of our children from the most repugnant of criminals.

About IWF > Chris Philp MP

Chris Philp MP

Minister for Tech and the Digital Economy

The 25th anniversary of the IWF is a moment to both acknowledge all that the IWF has achieved during that time, but also to recognise the continued prevalence of appalling child sexual exploitation and abuse online.

The IWF has demonstrated the action that can be taken through: investing in new technologies to detect child sexual abuse online; working with companies to help them take responsibility for what is online; and setting up and running the hotline that allows content to be reported, investigated, and removed as quickly as possible.

Addressing the issue of online safety has been a top priority of mine since I became Minister for Tech and the Digital Economy. We have now reached a major milestone in our mission to make the UK the safest place in the world to be online with the government's introduction of the Online Safety Bill into Parliament. The strongest protections in our legislation are for children and tackling the abhorrent exploitation and abuse online will be a collective effort.

The IWF has a vital role in supporting companies to take steps to improve safety, as well as empowering users. As this report demonstrates, in this connected world, the work carried out by the IWF is more important than ever.

About IWF > Professor Hany Farid

Lessons learned from two decades of combatting CSAM

Professor Hany Farid, University of California, Berkeley

This annual report marks the 25th anniversary of the founding of the IWF. On this milestone, I offer my reflections on the lessons learned from two decades of combatting child sexual abuse material (CSAM).

Prior to 2000, and the rise of the internet, the United States' National Centre for Missing and Exploited Children (NCMEC) believed the global distribution of CSAM to be largely contained. By early 2000, however, the internet became a breeding ground for child predators, resulting in an explosion in the global distribution of CSAM. In early 2000, the average age of a child involved in CSAM was 12 (it is now a mere eight). The Technology Coalition was created in 2003 with the explicit mission to "build tools and advance programs that protect children from online sexual exploitation and abuse." By 2008, however, the Technology Coalition had been unable to find or agree upon any viable tools to combat CSAM.

Despite phenomenal innovations and growth in the technology sector, little had been done for nearly a decade to contend with the online threat to children around the world.

It was in this shadow of 2008 that my collaboration with Microsoft began, leading a year later to the deployment of photoDNA. In thinking about technological solutions, we focused on what was best for victims, what was technologically feasible, and what would be palatable to the technology sector to deploy on their services.

In hearing from victims, we know that in addition to the horror of the original abuse, the continued sharing of photos and videos of their abuse leads to life-long trauma. Our initial approach, therefore, was focused on disrupting the redistribution of previously identified content, as opposed to identifying all possible forms of CSAM (a more ambitious but not technically feasible approach). By extracting a distinct and resilient digital signature from an

image – a so-called robust or perceptual hash – previously identified content can be automatically and accurately detected, removed, and reported. This approach, while more limited in scope, was technically feasible and would, we hoped, be the beginning of the development of a suite of technologies to combat CSAM.

The resulting photoDNA technology was initially deployed on Microsoft's network in 2009 and now, more than a decade later, is in wide use by most major online services. In recent years, NCMEC's CyberTipline reports receiving tens of millions of reports annually of online CSAM, the vast majority of which are initiated by a photoDNA match. Similarly, the Canadian Centre for Child Protection (C3P) employs photoDNA in their web crawler Arachnid, allowing for the automatic detection of millions of pieces of CSAM. And, the IWF has amassed more than one million unique CSAM image hashes which are shared with industry and law enforcement globally.

Despite the eventual success of photoDNA, its development was marred by years of obstructionism and inaction. And, more generally, the past two decades has seen at best a lethargic, and at worst a negligent, response to emerging threats to children online.

The technology sector has, for example, yet to settle on a video-based hashing technology with an industry-shared hash database. Gaming and anonymous chatting services routinely connect children with predators who then sextort their young victims. The live-streaming of child sexual abuse has emerged as the latest threat against children and yet there has been no concerted effort to combat this latest weaponization of technology against children. And, highly addictive products are routinely marketed to increasingly younger children, exposing them to illegal, inappropriate, dangerous, and unhealthy content.

The technology sector is not aggressively combatting these threats, and in some cases are developing other technologies that would make protecting children online even more difficult.

Following a trend in other messaging apps, for example, Facebook recently announced plans to move all their messaging services to an end-to-end encrypted system (E2EE). This move would prevent anyone, including Facebook, from directly seeing the content of any personal communication. A fully E2EE pipeline would render technologies like photoDNA impotent. While E2EE provides users with some added privacy, the associated risks are not insignificant. In announcing his plans, Mark Zuckerberg conceded it came at a cost: "At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services. Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion."

To partially address these concerns, in early 2021 Apple announced the development and planned deployment of NeuralHash, a client-side hashing technology meant to allow hashing technologies like photoDNA to operate within an E2EE system. Apple's announcement was met with swift and fierce opposition from privacy groups leading to a moratorium on its deployment. This trend has continued on the technology, policy, and regulatory side where privacy is pitted against child safety – with many seemingly blissfully unaware that preventing the distribution of CSAM is a privacy issue for child victims.

For over two decades, the technology sector has created phenomenally complex and impactful technologies, giving rise to trillion-dollar valuations for shareholders. These titans of

tech have invested enormous amounts of time and money into developing and deploying technologies to secure our devices from spam, malware, and other cyber threats. When it comes to child safety and other online harms, however, this same industry has been maddeningly slow at ensuring the well-being of our most vulnerable citizens.

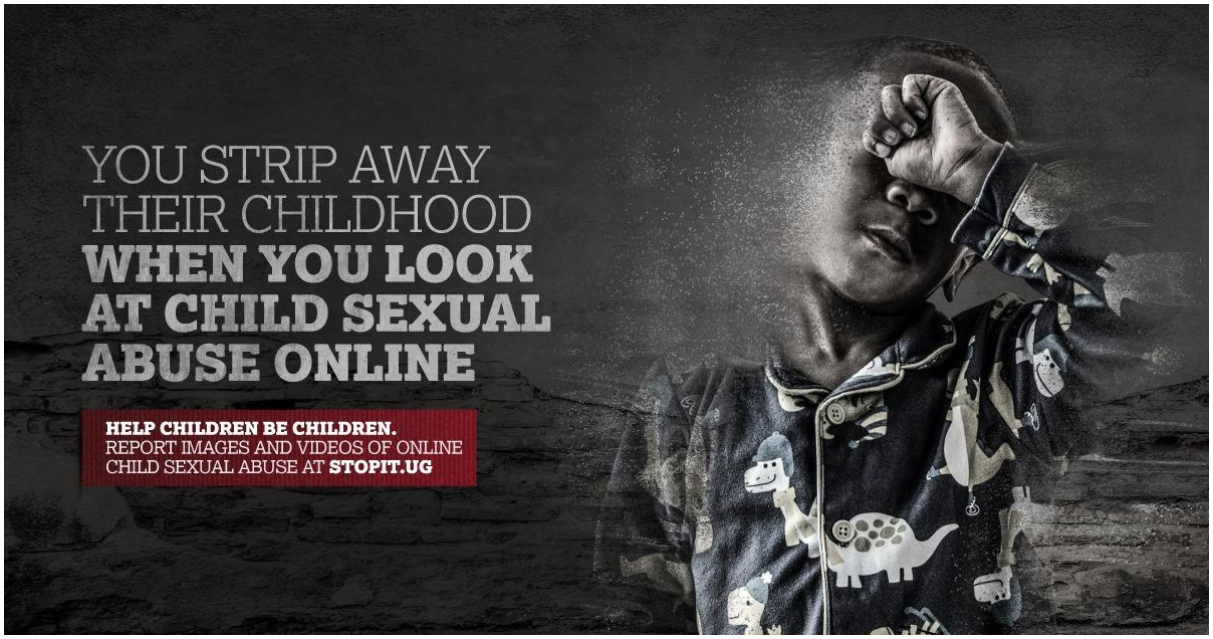
How, in 20 short years, did we go from the promise of the internet to democratize access to knowledge and make the world more understanding and enlightened, to the litany of daily horrors that is today's internet? A combination of naivete, ideology, wilful ignorance, and a mentality of growth at all costs, have led the titans of tech to fail to install proper safeguards on their services. The limitations to protecting children and vulnerable populations online are fundamentally not technological in nature. They are, rather, one of corporate priorities, a lack of appropriate regulation, and virtual monopolies leading to a stifling of new ideas. In the next 20 years, we can and we must do better: we need not repeat the mistakes of the past two decades. History will rightfully judge us harshly if we fail to act.

About IWF > 2021 Highlights

January

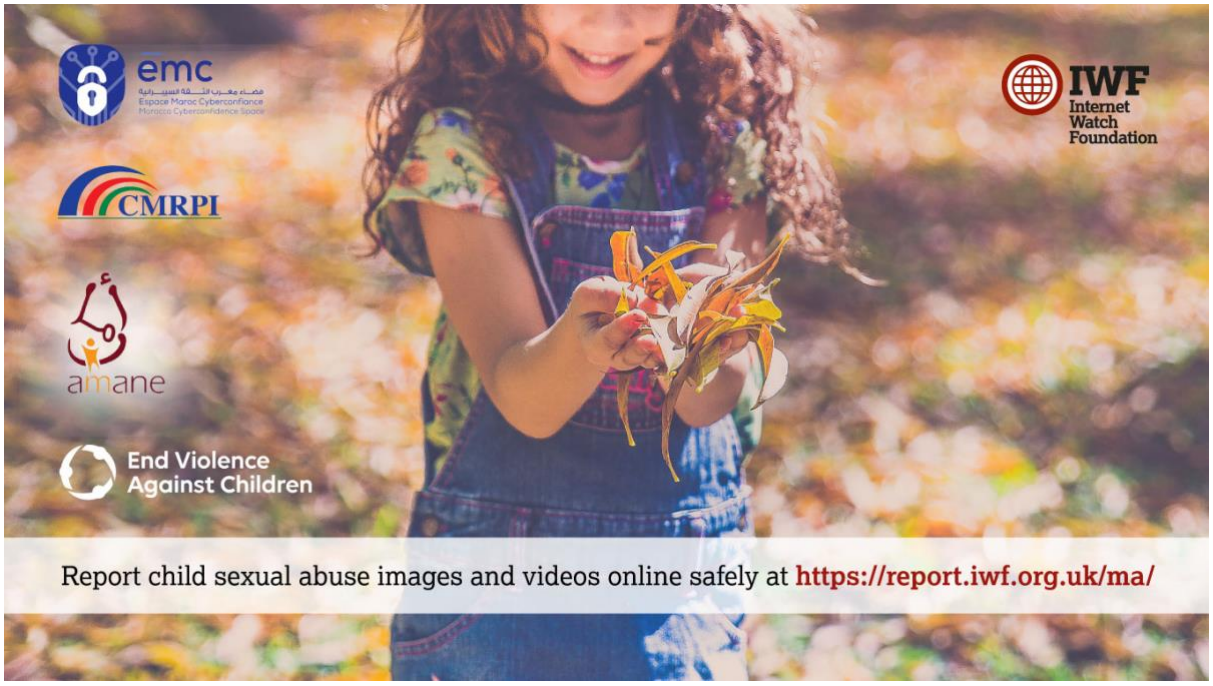
Kenya reporting portal:
We launched a reporting portal in Kenya.

February



Uganda and Zambia campaign: We launched a new project to help boost internet safety in Uganda and Zambia.

Safer Internet Day: We celebrated and promoted Safer Internet Day with our colleagues at the UK Safer Internet Centre. The theme was "An internet we trust: exploring reliability in the online world".



Morocco reporting portal: We launched a reporting portal in Morocco.

March

Guatemala reporting portal: We launched a new reporting portal in Guatemala.

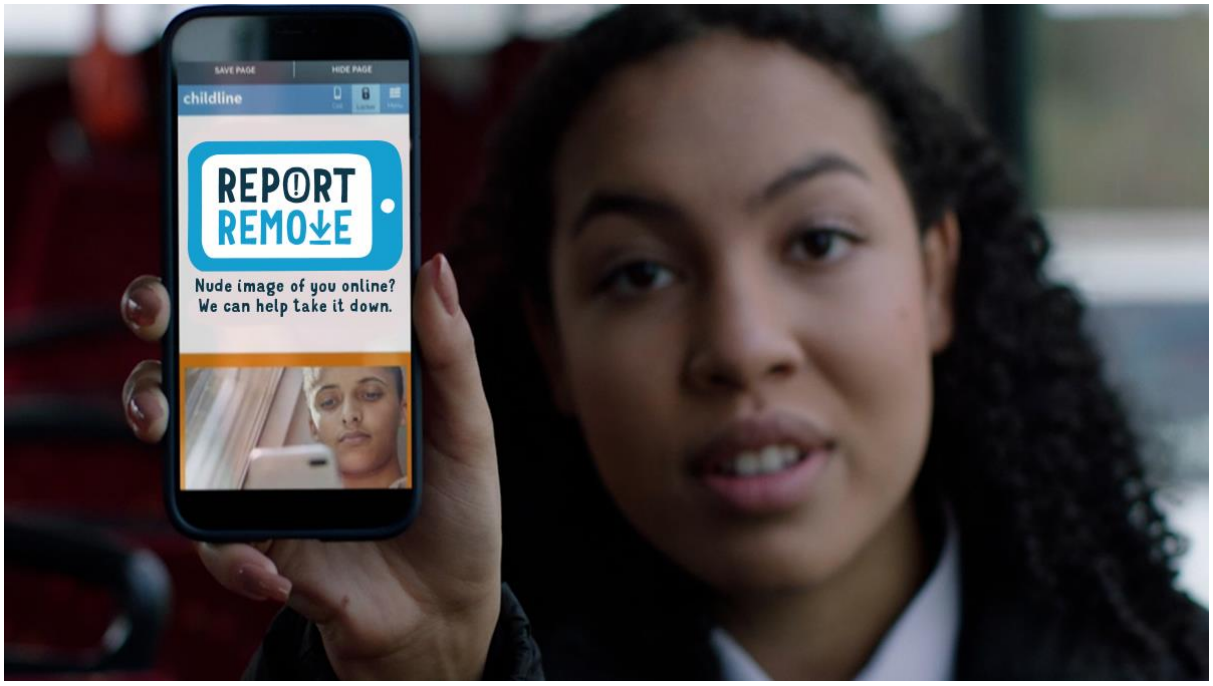
April

Self-generated campaign launch: We want to prevent the creation of sexual imagery of children which has been captured via webcam/device camera after they've been groomed and coerced online. We launched a campaign to help teenage girls and their parents understand more about this crime, and how to better protect themselves.

June

New taskforce: A new IWF Taskforce was recruited to grade and 'hash' two million child sexual abuse images from the UK Government's Child Abuse Image Database (CAID) thanks to a grant from international child protection organisation Thorn. Read our press release.

Tunisia reporting portal: We launched a reporting portal in Tunisia. Pictured is Imen Zahouani Houimel, the Minister of Women, Family and Seniors of the Republic of Tunisia.



Report Remove tool: Childline and the IWF launched a new tool to help young people remove nude images that have been shared online.

Argentina reporting portal: Argentina launched its first reporting portal to report images and videos of child sexual abuse. Read our press release.

September

APPG on social media: This All Party Parliamentary Group launched its report, "Selfie Generation: What's behind the rise of self-generated indecent images of children online?" The APPG secretariat is run by IWF on behalf of the UK Safer Internet Centre.

October

Digital Communications Awards 2021: We took the top prize in the DCA's Purpose Driven Communications category for our work campaigning to raise awareness of the rise of “self-generated” online child sexual abuse material. Read our press release.

UKSIC funding:

The UK Safer Internet Centre received £5.1 million of funding from Nominet in order to continue its vital work helping children and young people stay safe online. Read our press release.

November

Welsh Government: Welsh Government became the first government to join IWF. They also joined our award-winning campaign to help educate and protect parents, carers, and teenage girls regarding online grooming and coercion.

December

IntelliGrade: Our IntelliGrade tool was named one of the “21 Things That Made the World a Better Place in 2021” in Wired. Read our press release.

ICMEC + IWF reporting portal: We have partnered with ICMEC to launch a portal to report child sexual abuse material for people who don’t have access to a national reporting mechanism. Read our press release.

About IWF > Caring for our people

“Despite the great challenges with lockdowns, and vast increases in the amount of child sexual abuse content that we detected online, our Hotline team remained resilient and determined.” Heidi Kempster, Deputy CEO and Chief Operating Officer.

People are at the heart of IWF

In 2021 we detected more child sexual abuse material than ever before. So much so, that we found more of this imagery in 2021, than in the first 19 years of IWF’s operation.

Whilst that’s a great demonstration of impact, it requires us to think harder than ever about how best to keep the people who do this work resilient, protected and cared for.

Despite the challenges presented to us by Covid, we remained open throughout and shielded our Hotline team by keeping all other staff at home. We continued our policy of “family comes first” to give all our staff the flexibility and reassurance they needed to manage their home and work life.

Our gold-standard welfare system

It’s been widely acknowledged that IWF’s approach to welfare is of a high standard, and we’re proud of this. It’s enabled talented and experienced staff to stay happy and healthy in their roles – some people have been with us for more than a decade.

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 described in an independent audit as “outstanding”.

Our analysts’ working hours are restricted; they take regular timetabled breaks and are encouraged to take more breaks as and when they need. Overtime is not allowed.

Each month they have individual mandatory counselling sessions and all employees who see criminal imagery have an annual full psychological assessment. Everyone who works for us is offered counselling support.

But we’re not complacent. At the end of 2021, we scoped a review of our Hotline recruitment process to be carried out by a consultant clinical psychologist in 2022. This will help us to build upon the best practice approach we already take and ensure we safeguard the mental health of our people.

About IWF > Our policy work

In the UK

Online Safety Bill

The Government has been continuing to develop its approach to online safety in 2021. In the Queen's Speech in May, the Government committed to bringing forward a Draft Online Safety Bill for pre-legislative scrutiny.

In July, a joint committee of both of Houses of Parliament was established to scrutinise the legislation, which was Chaired by Damian Collins MP.

We responded to the Committee's call for evidence in September 2021, sharing our perspective on the draft Bill, recommending:

- That the regulatory regime builds on the existing expertise of organisations like us who have been essential in removing illegal content from the internet and reducing UK hosting of CSE/A material over the past 25 years.
- That the Government and Ofcom set out the process for which organisations could be appointed as co-designated bodies to assist the regulator.
- That the Government ensures the Bill is appropriately integrated with law enforcement, particularly when it comes to illegal harms.

You can read our response to the draft Bill.

In December when the Committee reported back, they concluded that we had made a "persuasive case" for co-designation and that scrutiny of the Bill could have been improved if more details about how co-designation and the timelines for when decisions might be made were published alongside the Bill.

We will continue to engage with Ofcom and the Government in 2022 to ensure that the Bill is effective in protecting children from harm online from day one.

The Lord Clement-Jones CBE

DCMS Select Committee

Susie Hargreaves, our CEO, was invited to give evidence to the DCMS Select Committee in October 2021 about online safety and online harms.

She set out our response to the draft Online Safety Bill and highlighted some of the trends that we've seen, for instance the dramatic increase in "self-generated"/ "first-person produced" indecent images of children.

Susie also mentioned our concerns about companies introducing end-to-end encryption (E2EE) without effective mechanisms in place to continue removing illegal content and said that we would like to see age verification for adult websites.

Securing replacement funding as EU Funding ends

In December 2021, the funding the IWF and our partners in the UK Safer Internet Centre (UKSIC) received from the European Union came to an end, ending a decade's worth of EU funding. Therefore, we focused our efforts on securing the £1.3 million of funding per annum which had previously been provided by the EU - a figure which amounted to 50% of the Centre's funding.

After lengthy negotiations with the UK Government, politicians and other key stakeholders, the .UK Domain registry, Nominet, pledged £5.1m to help fund the UKSIC for the next three years, allowing us to continue our work to ensure that children can use the internet safely, illegal and harmful content is removed and users continue to be protected online.

We would like to thank all Parliamentarians who signed an open letter asking for the Government to replace our funding, which was vital in helping us make our case.

APPG on Social Media

Throughout the past year, as part of the UK Safer Internet Centre, we ran the Secretariat for the All-Party Parliamentary Group (APPG) on Social Media. We helped them to conduct an inquiry into the increased number of "self-generated"/ "first-person produced" indecent images of children.

The inquiry received written evidence from 18 individuals and organisations, as well as research reports and documents to support the final recommendations. There were also four oral evidence sessions with academics, children's charities, law enforcement and industry.

The inquiry concluded in September 2021 and made 10 recommendations, including:

- Tech companies should not introduce encryption unless they can guarantee that they can still remove illegal content and cooperate with law enforcement in the same way they do now.
- The RSE curriculum should facilitate constructive conversations about healthy relationships in a digital age, that avoid blaming children.
- The Home Office should review all relevant legislation to ensure it is as easy as possible for children to have their images removed from the internet and ensure that they can have confidence in the removal process.

You can read the full report here.

We would particularly like to thank Chris Elmore MP who chaired the APPG up until his recent appointment as a shadow DCMS minister in December. We would also like to thank both Minister, Victoria Atkins MP, and Shadow Safeguarding Minister, Jess Phillips MP, for their ongoing support throughout and for speaking at the launch and report stages of the inquiry.

Safer Internet Day

For Safer Internet Day in February 2021, we ran a virtual event with politicians where children from St. Patrick's College, Dungannon, were able to discuss their views on this year's theme: "An internet we can trust exploring reliability in the online world." The event was chaired by Dr. Lisa Cameron MP, a Vice Chair of the APPG on Social Media and included contributions from the Shadow Digital Minister, Chi Onwurah MP and Will Gardner, CEO of Childnet International. Over 30 MPs and Peers also supported Safer Internet Day by tweeting their support online.

Safer Internet Day reached more children and young people with internet safety resources and messaging than ever before: 51% of children throughout the UK and 38% of their parents.

Safety Tech Challenge Fund

We were delighted that the Department for Digital, Culture, Media and Sport (DCMS) and the Home Office launched their Safety Tech Challenge Fund in 2021 to encourage the development of new technologies to stop the spread of child sexual abuse material in encrypted channels.

Five projects were awarded an initial £85,000 from the Fund, including a partnership between the IWF, Cyan Forensics and Crisp Thinking.

Violence against Women and Girls

In 2021 the Home Office opened a consultation to inform their new strategy to tackle violence against women and girls. Given that over 90% of the victims our analysts see are young girls, we believe we have a unique expert contribution about the online aspects of this issue.

You can read our submission here.

Centre for Social Justice Report - Unsafe Children

In March 2021, the Centre for Social Justice published its report, Unsafe Children. The Commission was Chaired by the current Health Secretary, Rt. Hon. Sajid Javid MP and made over 100 recommendations on how the online and offline response to CSE/A could be prevented or improved further.

IWF CEO, Susie Hargreaves, served as a Commissioner on the report and spoke on a panel to promote the report and its findings at the Conservative Party Conference in Manchester in October.

l-r: Patrick Cronin, PA Consulting; Tom Morrison-Bell, Google; Susie Hargreaves OBE, IWF; Olivia Robey, Centre for Social Justice; IWF Champion Miriam Cates MP; Victoria Green CEO and Rhiannon, Marie Collins Foundation

Relationship with Law Enforcement and the Crown Prosecution Service (CPS).

Throughout the year we continued to work closely with our law enforcement partners, specifically the National Crime Agency Child Exploitation and Online Protection command (NCA CEOP) and the National Police Chiefs' Council (NPCC). Our CEO is a member of the NCA's Strategic Governance Group and our Hotline Director is a member of the NCA's Prevent group. In addition, the CEO sits on the Crown Prosecution Service Child Sexual Exploitation and Abuse (CPS CSEA) Advisory Group. By working closely, we ensure we share crucial data which informs the operations of the IWF.

EU

CSAM Directive

The EU is looking to update the 2011/93 directive on *combating the sexual abuse and sexual exploitation of children and child pornography*.

We submitted responses to two consultations on this subject in April and October. We recommend that the European Commission pursue both new legislation on prosecuting offenders, protecting victims, and preventing offences in addition to non-legislative measures. We particularly believe that the current directive should be replaced by a regulation to solve some of the current transposition issues.

You can read our submission here and here.

Digital Services Act

The European Commission has been making progress during 2021 on the introduction of a Digital Services Act (DSA) that will modernise the e-Commerce directive and this relates to the removal of illegal content and other online safety issues.

We welcome this move and would like to see a clearer legal role for hotlines in Europe. We think that hotlines should be given trusted flagger status and be given permission to proactively search for content. We believe this could dramatically increase the amount of illegal content that is identified and actioned.

As 2021 ended, both the European Parliament and European Council negotiating positions were established and it is anticipated that trialogue negotiations on the file will begin in January 2022. The IWF has been meeting with MEPs and attaches during December 2021 to ensure our views are represented ahead of the trialogues.

You can read our response to European Commission's public consultation on the DSA here.

International

UN Consultation

The IWF responded to a Call for Inputs for the report of the UN Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material.

You can read our response here.

Philippines

The Senate in the Philippines passed a Bill on Special Protections against Online Sexual Abuse and Exploitation of Children in May 2021, which is now being discussed by the House of Representatives. This sets out new duties for ISPs, including that they:

"Develop and adopt a set of systems and procedures for preventing, blocking, detecting, and reporting of OSAEC committed within their platforms, which are compatible with the services and products they offer, including the maintenance and management of an updated list of

URLs containing child sexual abuse and exploitation material by partnering with organizations that maintain the most comprehensive list of URLs with CSAESM, and those with hashes of the same, such as the Internet Watch Foundation and/or INHOPE hotline."

You can read the Bill here.

UN Internet Governance Forum

In December, the IWF's Senior Policy and Public Affairs Manager spoke at the United Nations' Internet Governance Forum on the Dynamic Coalition on Children's Rights in the Digital Environment.

The session was entitled: "Regulate or prevent to protect children: A false Dichotomy." The session concluded that Child Rights groups must find a shared voice to improve coordination and help build consensus around ways to balance child protection and regulation that is respective of fundamental human rights such as privacy online.

You can read the report from the session here.

EURODIG

In July, IWF CTO, Dan Sexton spoke on a panel at the European Dialogue on Internet Governance. The panel explored the theme: "Can privacy, security and encryption co-exist?"

Further details of the session and the transcript can be found here.

World Economic Forum Global Coalition for Digital Safety

In September, IWF CEO, Susie Hargreaves joined the inaugural meeting of the Global Coalition for Digital Safety. The forum brings together senior leaders from the technology industry, Government Ministers, and online safety experts from all over the world.

The Group has three workstreams:

1. Content moderation
2. Regulation
3. Business Models and Co-operation

The group produced a white paper: advancing digital safety; A framework to align global action in June 2021.

Complaints

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

In 2021 we received 4 complaints regarding the inclusion of a URL on our URL List, and 1 for the receipt of a Notice and Takedown. None of these was upheld.

2021 Trends & Data > Headline summary

In 25 years...

1,800,000 reports have been assessed by IWF analysts

970,000 child sexual abuse reports have been actioned for removal.

As each report contains at least one, and sometimes thousands of images, this equates to millions of criminal images removed from the internet.

In 2021...

This year we assessed 361,062 reports and 7 in 10 (252,194 reports) of those led us to finding imagery online of children being sexually abused.

We were able to find 64% more of this criminal material in 2021 due to some significant improvements we made within our Hotline – to our working practices and procedures, the technology that we're using and not to mention making best use of our hugely skilled and experienced Analyst team we have.

2021 was the year that we saw sexual abuse imagery of girls being shared more widely than any previous year. Girls were seen in 97% of the imagery we helped to remove.

That's not to say we didn't see imagery of boys; we did. And for the first time this year we took a more detailed look at what this imagery can tell us.

Almost 7 in 10 instances of child sexual abuse involved 11-13 year olds. And when we see imagery of babies, toddlers and young children aged 6 and under, they are more likely to be suffering category A child sexual abuse over categories B, or C.

"Self-generated" child sexual abuse, where someone captures a recording via a phone or computer camera of children who are often alone in their bedrooms, is now the predominant type of child sexual abuse imagery we're finding online – just over 7 in 10 reports include this type of content.

6 in 10 actioned reports specifically show the sexual abuse of an 11-13 year old girl who has been groomed, coerced or encouraged into sexual activities via a webcam. Sadly, we've seen instances of children aged 3-6 being contacted and abused in this way.

For the first time we've looked at the prevalence of female offenders in the imagery that we see. We've seen how this imagery most often involves children aged 7-10 years old, and that boys are most often seen being abused by a female offender.

We've published a deeper analysis into the abuse of domains in relation to child sexual abuse, as we believe a greater focus in this area could have a significant and positive impact on thwarting the distribution of child sexual abuse material on the internet.

We now have more than 1million unique image hashes of child sexual abuse. And around a third of those include detailed metadata on the type of sexual activity seen. We've published this breakdown which puts into real words the crimes being inflicted upon children.

We encourage you to use our data and information to inform your own work and understanding of the prevalence, distribution and fight to eliminate online images and videos of child sexual abuse.

Trends and data > Total number of reports

In 2021, we assessed a webpage every one-and-a-half minutes. Every two minutes, that webpage showed a child being sexually abused.

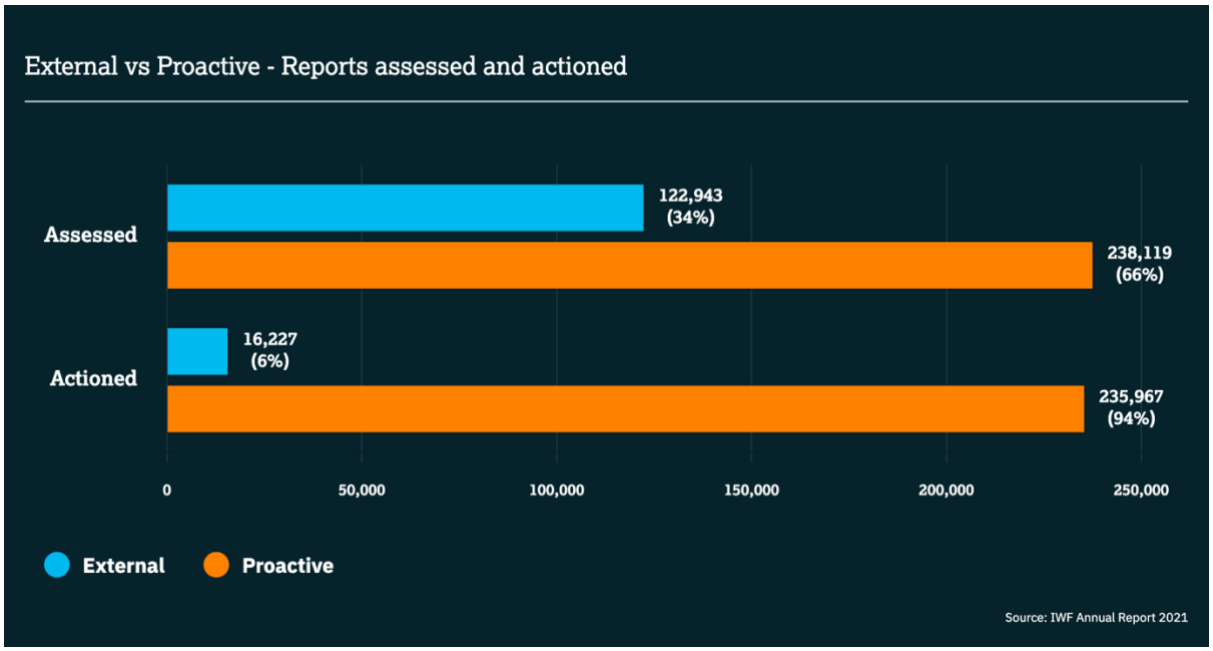
People report to us at iwf.org.uk, or through one of the 49 Reporting Portals around the world, in multiple languages. All reports are assessed at our headquarters in the UK. We also actively search the internet for child sexual abuse imagery. We call this, 'proactive searching'.

- **361,062 reports were assessed by IWF** (20% increase from 2020):
  - 360,834 were reports of webpages and
  - 228 were reports of newsgroups.

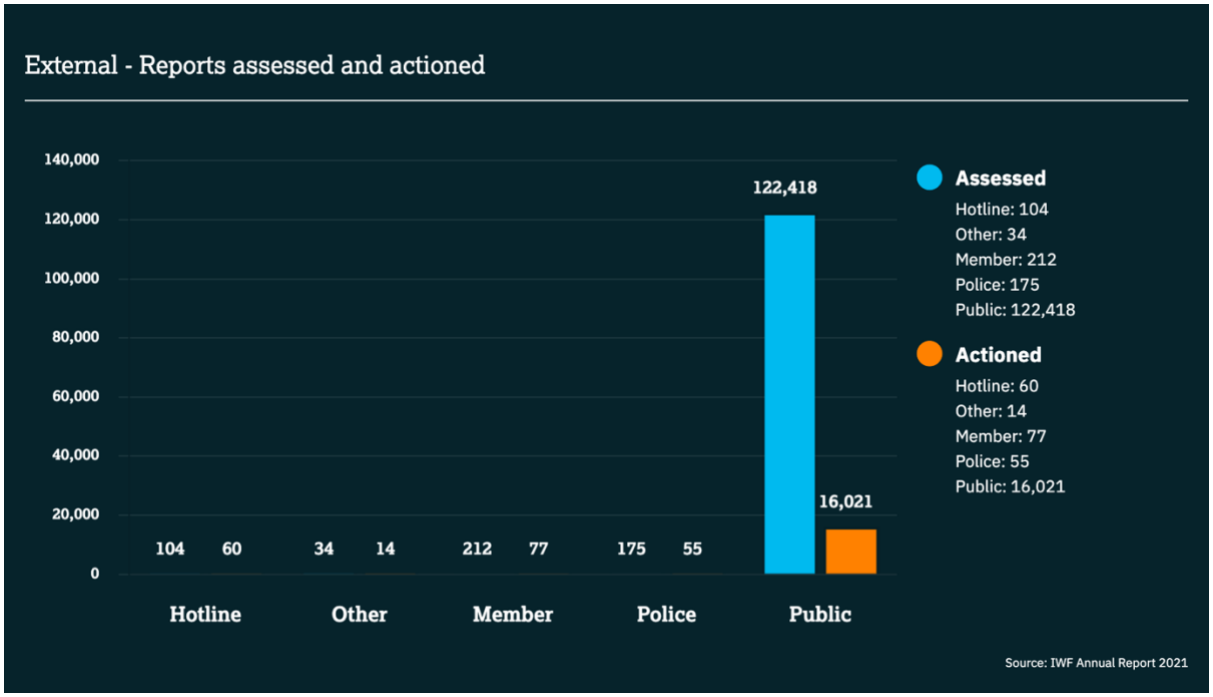
- **252,194 URLs (webpages) were confirmed as containing child sexual abuse imagery having links to the imagery or advertising it** (64% increase from 2020).
- Additionally, 5 newsgroup reports were confirmed as containing child sexual abuse imagery.
- No reports were confirmed as UK-hosted non-photographic child sexual abuse imagery.

You can read more about UK-hosted and globally-hosted child sexual abuse material.

Child sexual abuse imagery reports



This chart compares proactively sourced reports (where our analysts search for content) and those reports which came to us via external sources.



This chart shows a breakdown of the external sources which report into us and report numbers from each source.

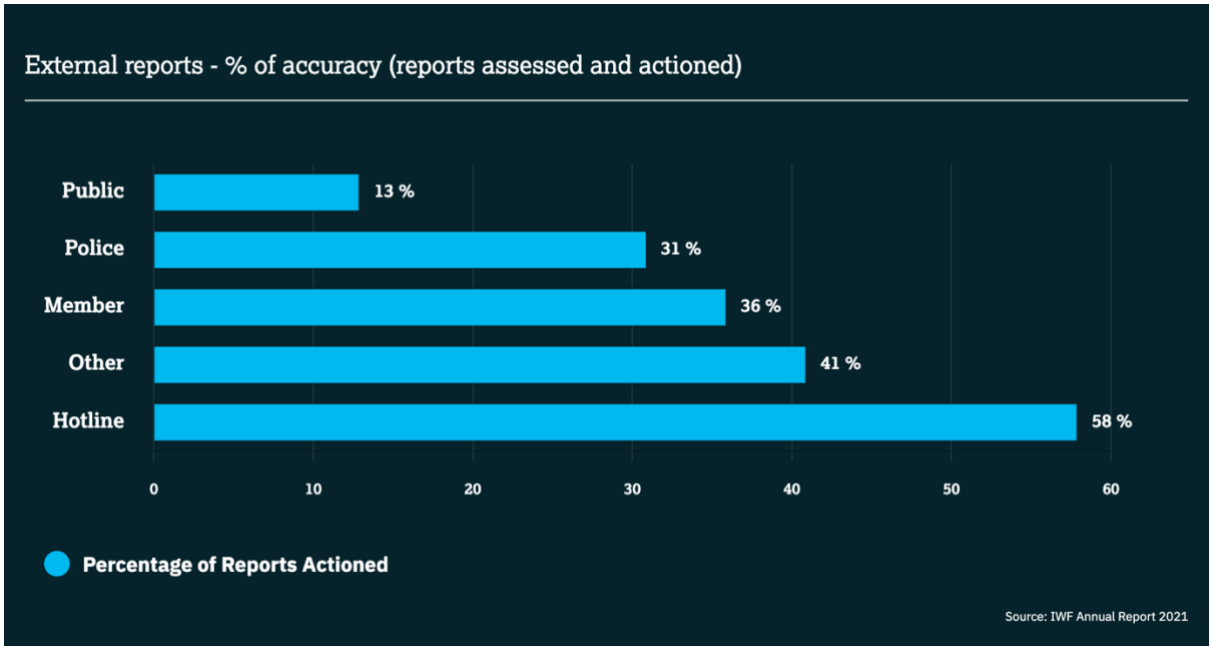


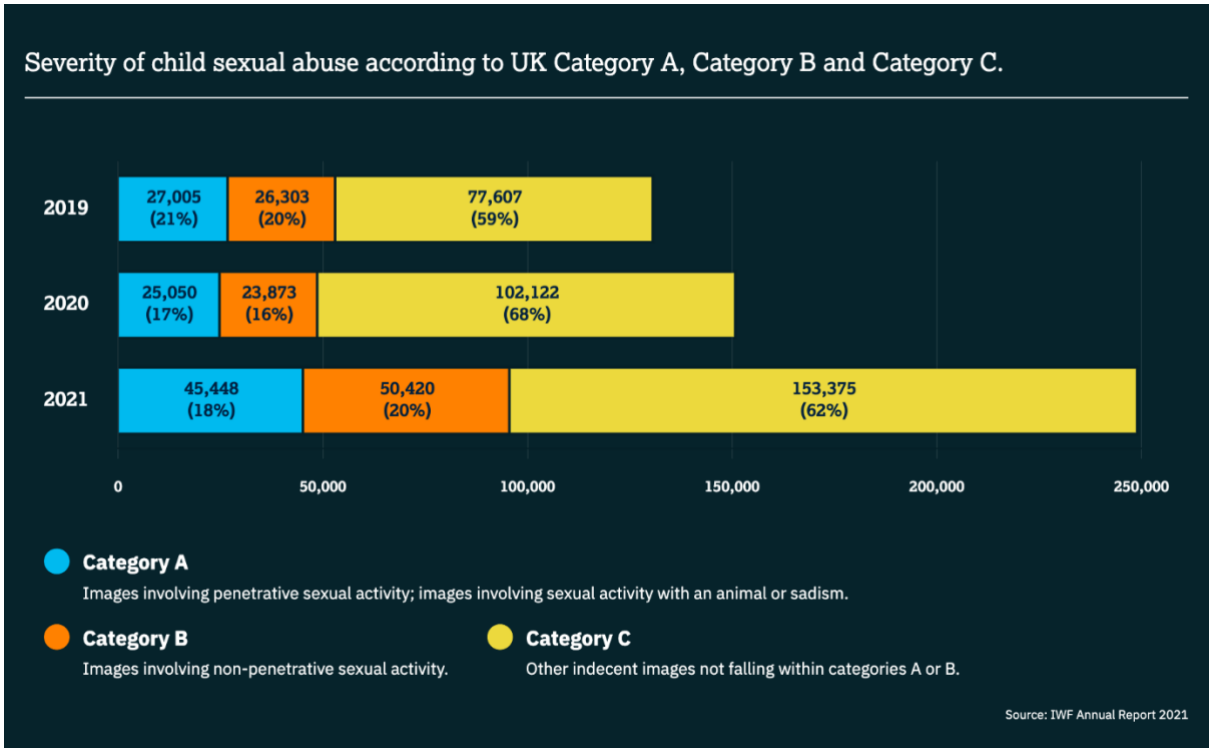
Chart showing the percentage of reports which were actionable (contained child sexual abuse material) from each external source.

Public report source accuracy

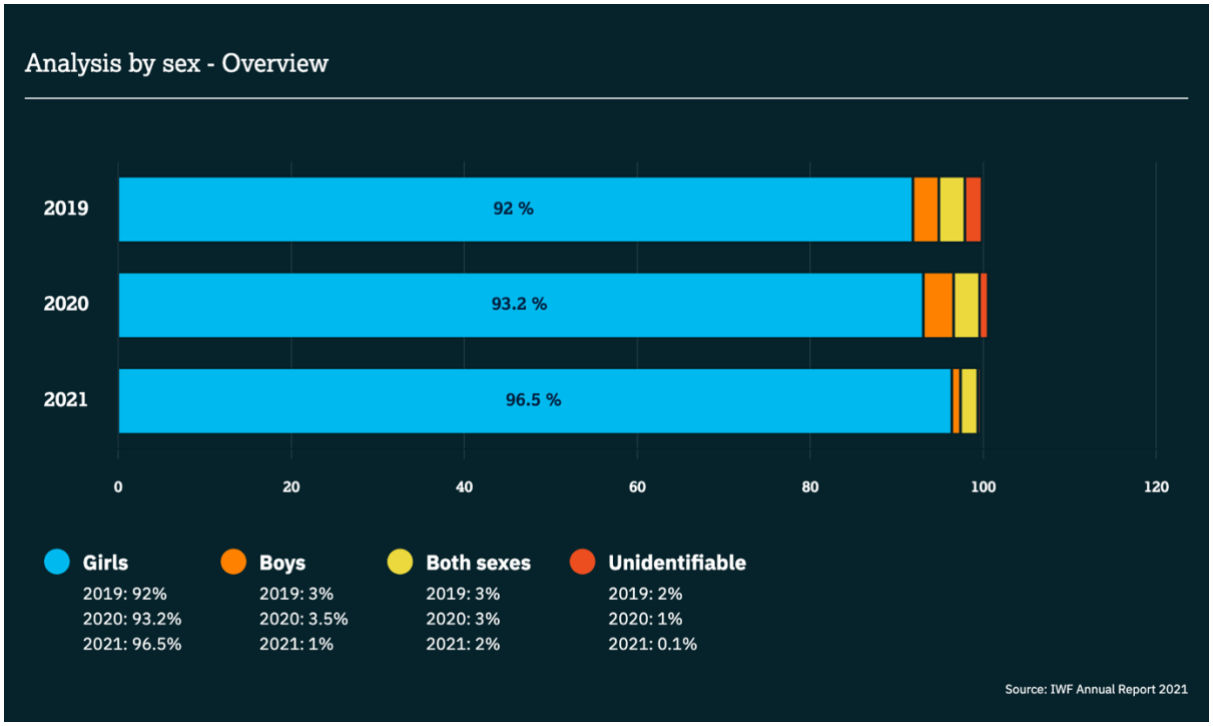
122,418 reports were assessed by our Hotline which came from the public. **29% (29% in 2020) of these reports correctly identified child sexual abuse content.** This figure includes newsgroups and duplicate reports (where the same criminal URL has been reported multiple times).

Note: Each year, a number of these are adverts or links to child sexual abuse material.

Severity of child sexual abuse according to UK categories A, B and C

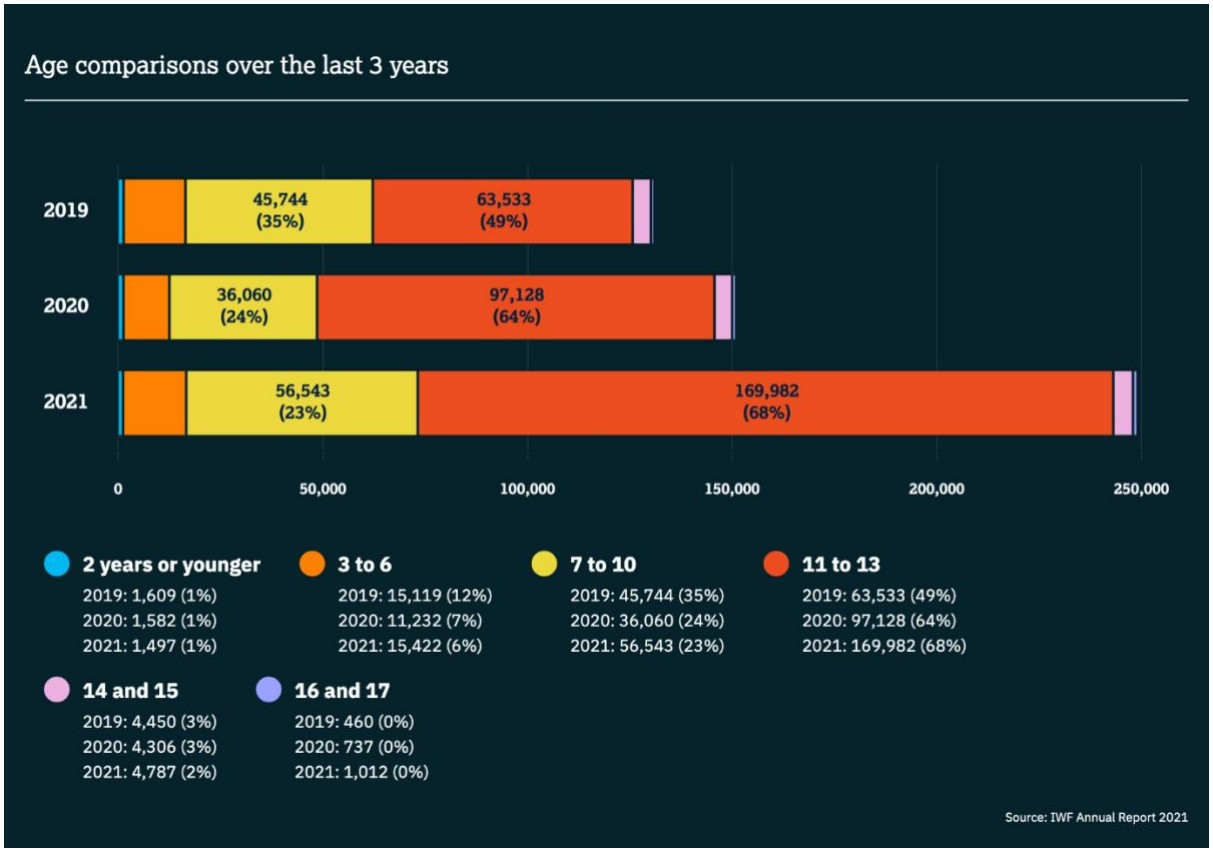


Analysis by Sex – overview



We've looked more closely at the figures relating to the sexual abuse of boys here.

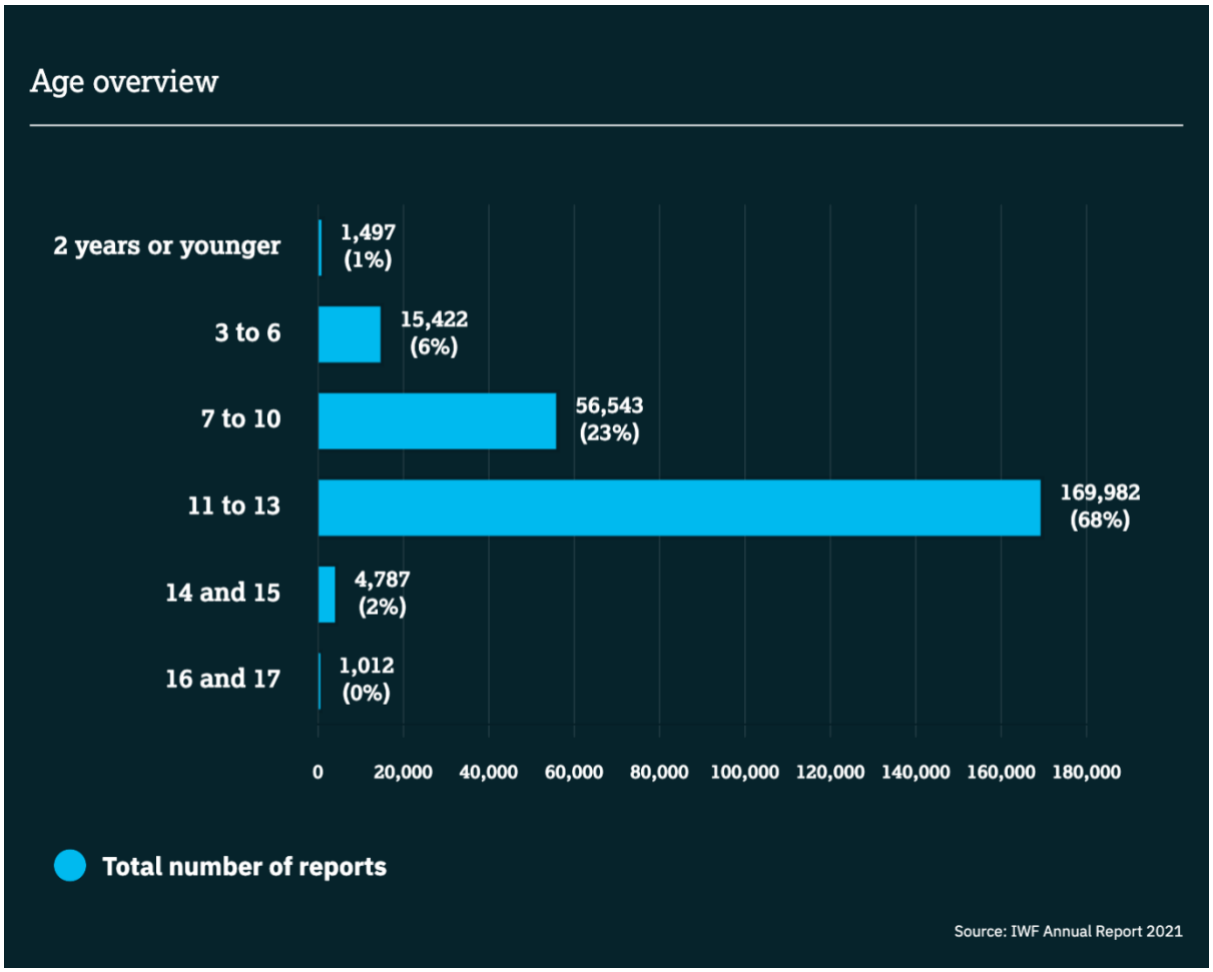
Analysis by age – overview



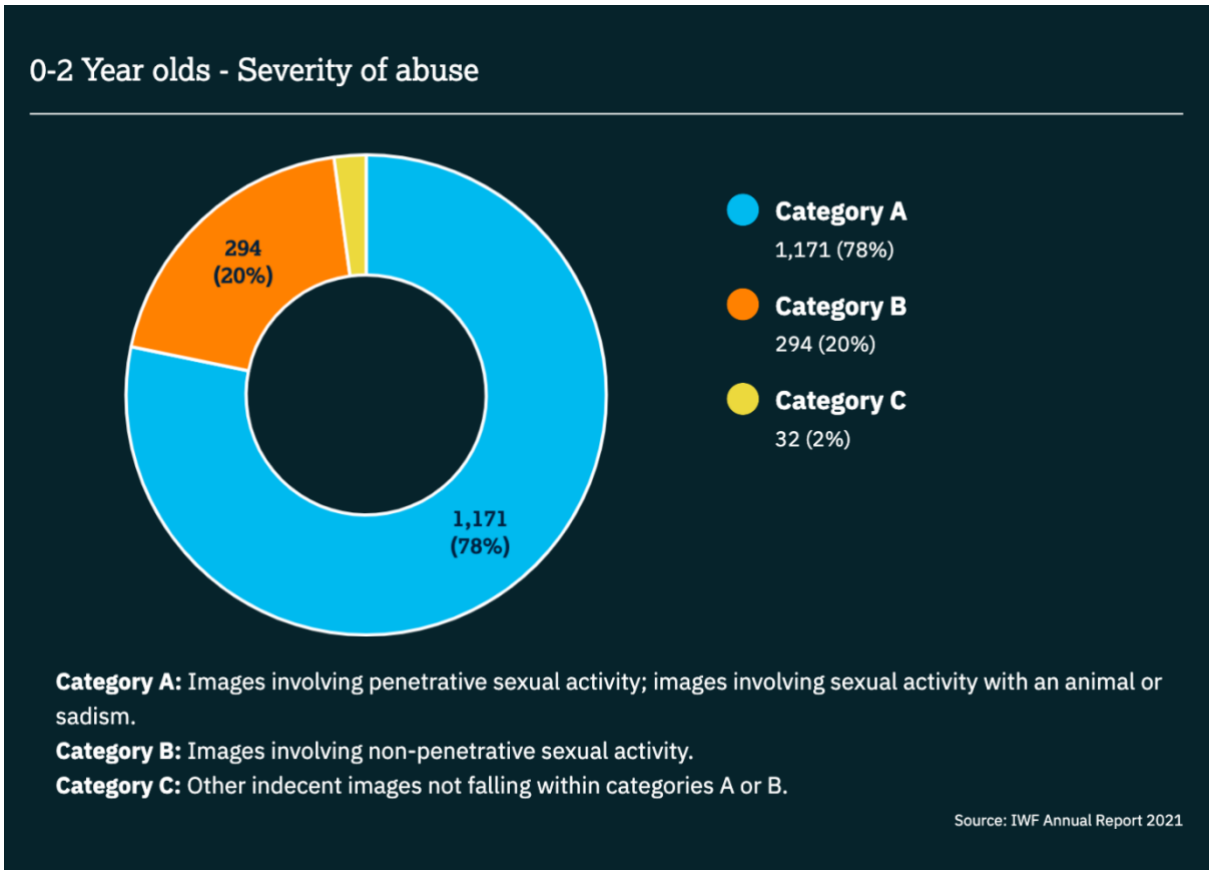
You can see our in-depth age analysis relating to sexual abuse when the abuser is physically present, and sexual abuse which is captured in a "self-generated" nature.

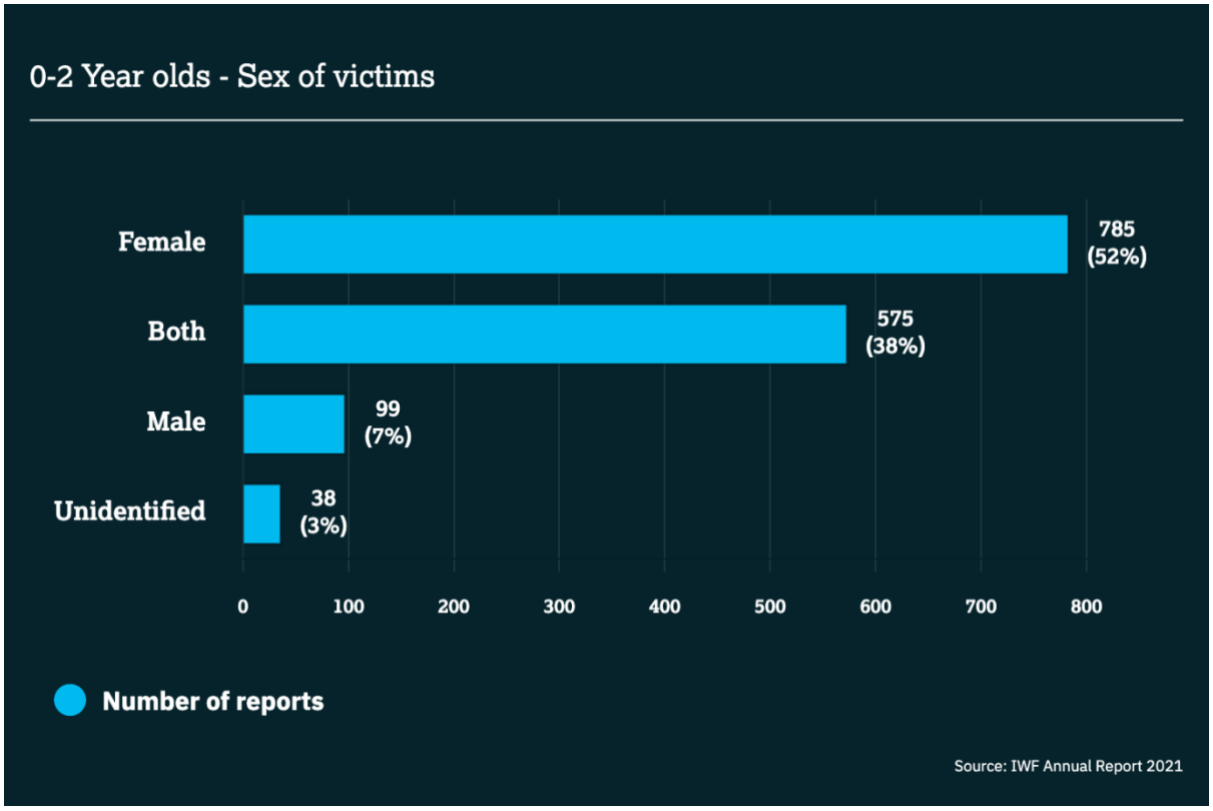
2021 Trends & Data > Analysis by age

Overview of all ages



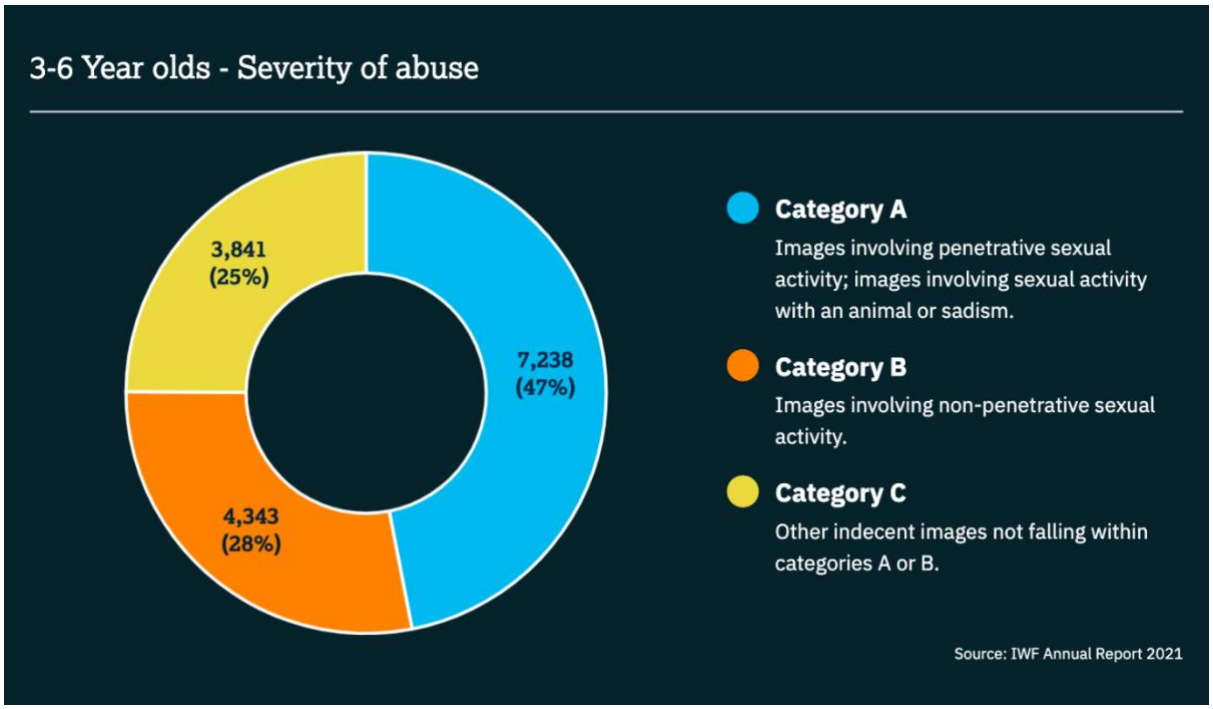
0-2 years: Babies and toddlers

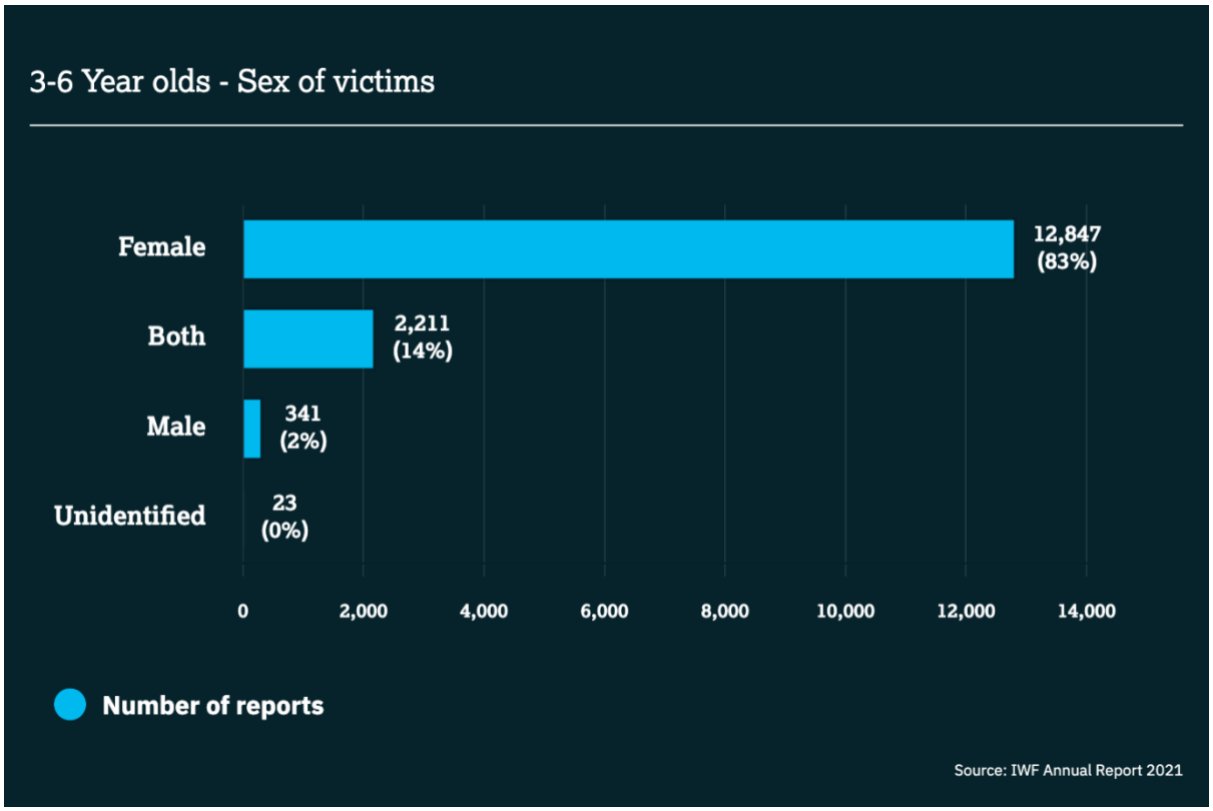




Every year, we see a high proportion of Category A images showing the most severe, sadistic forms of sexual abuse involving babies, toddlers and even newborns. In 2021, we also saw an increase in the number of Category B images, indicating that an adult abuser is present in the images.

3-6 years: Young children

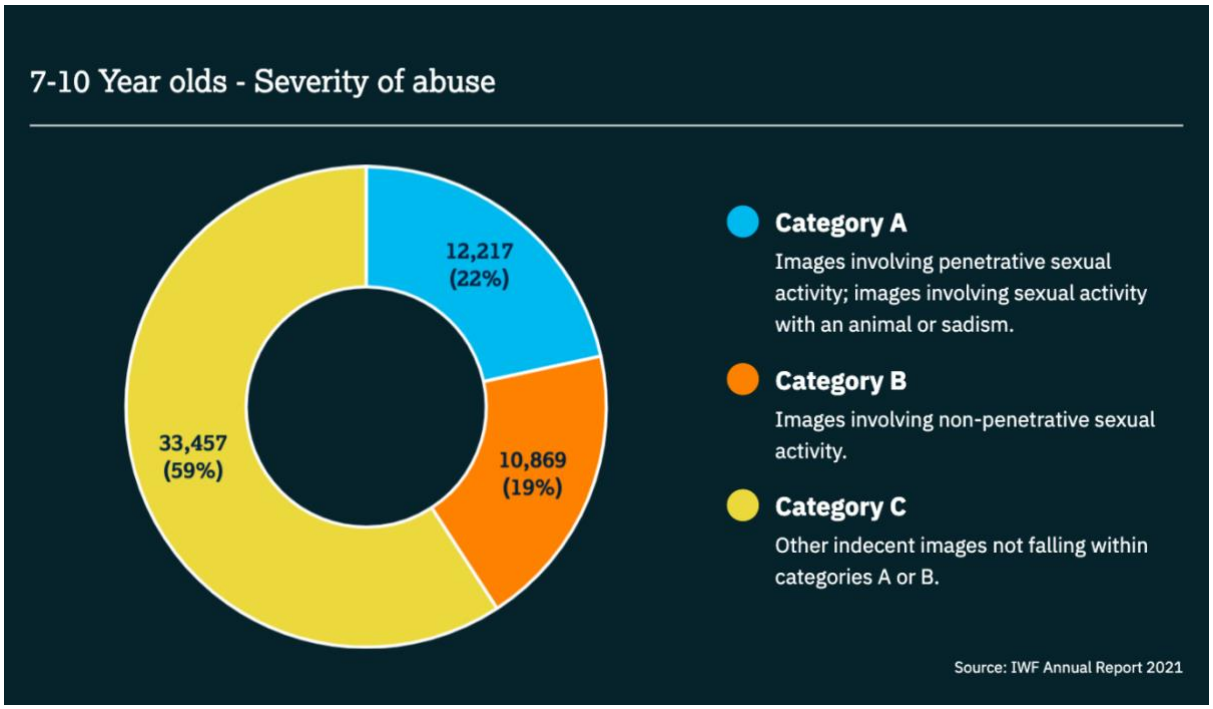


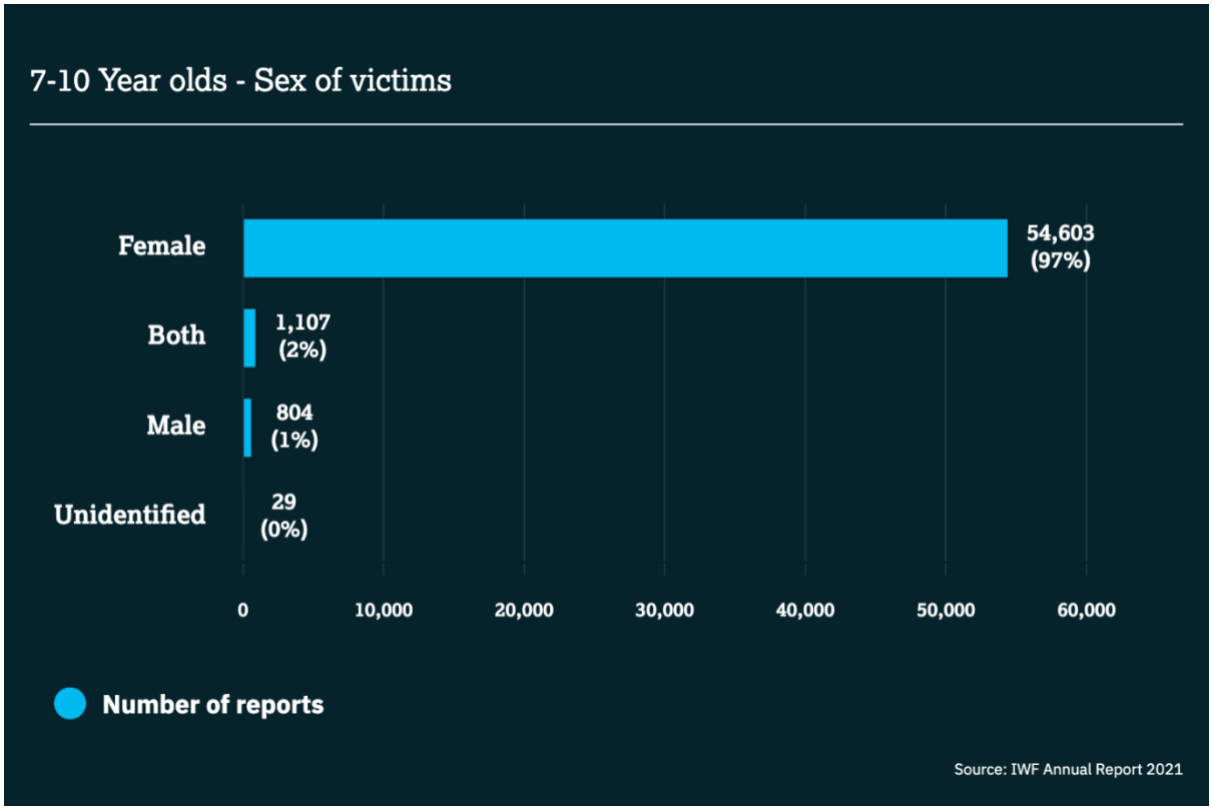


We saw a high proportion of boys aged 3-6 appearing in sexual abuse imagery, often with a female sibling. Criminals will coerce children into bringing their younger siblings online with them, exploiting the opportunity to abuse more than one victim in the same household.

You can read more about our data on the sexual abuse of boys here.

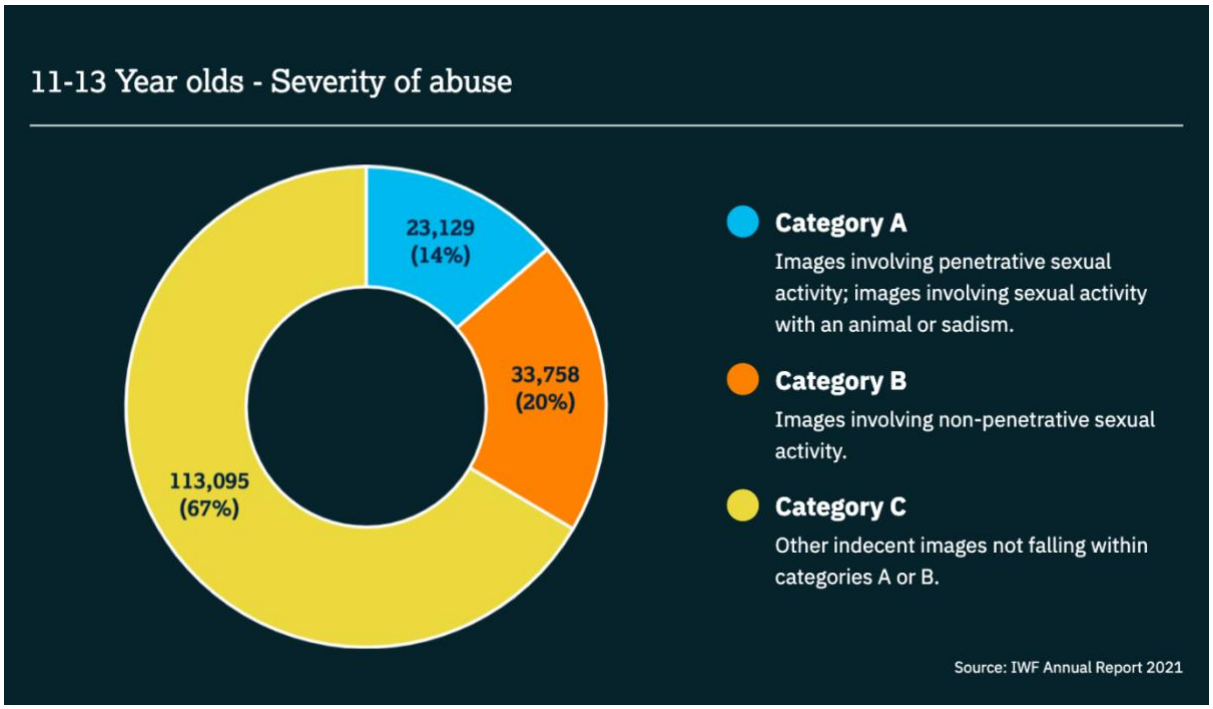
7-10 years: Pre-pubescent children

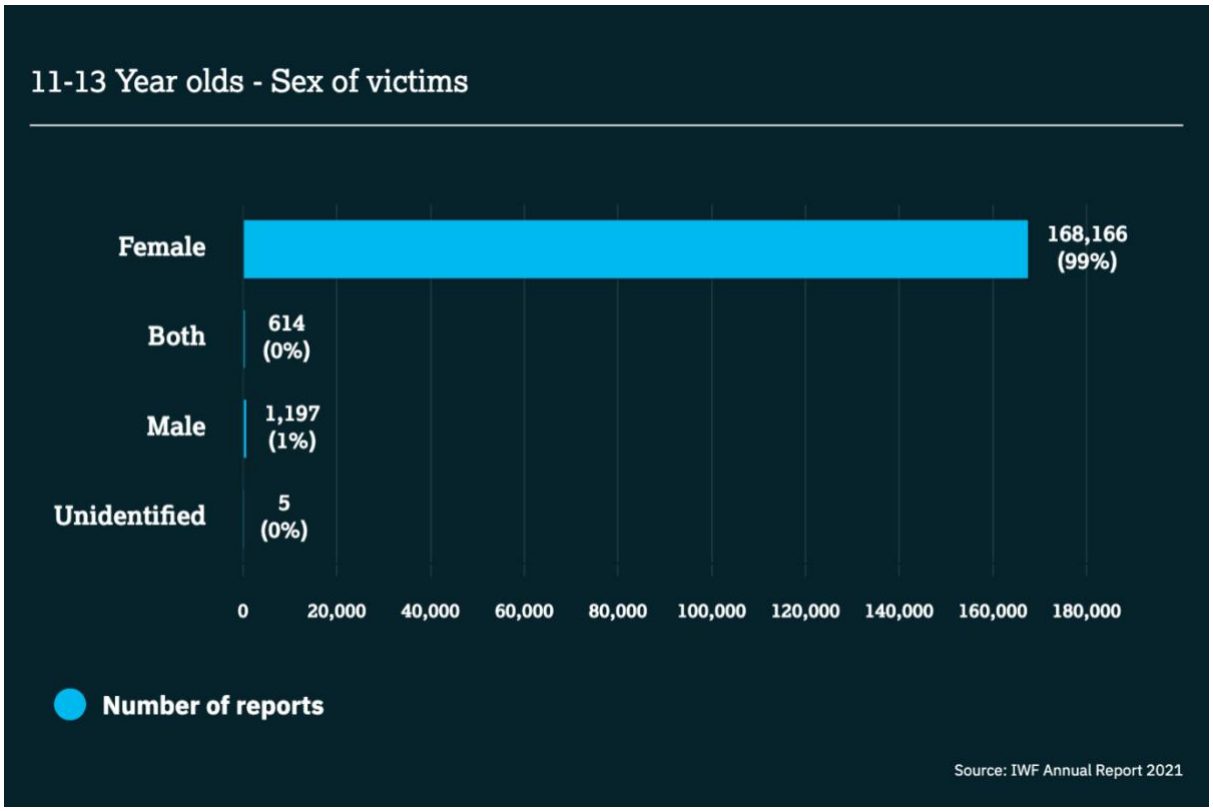




In 2021, we sadly saw a three-fold increase in “self-generated” imagery showing 7-10-year-olds. Children have spent an increasing amount of time online during the pandemic, leaving them vulnerable to grooming and coercion by abusers who manipulate them into recording their own abuse on camera.

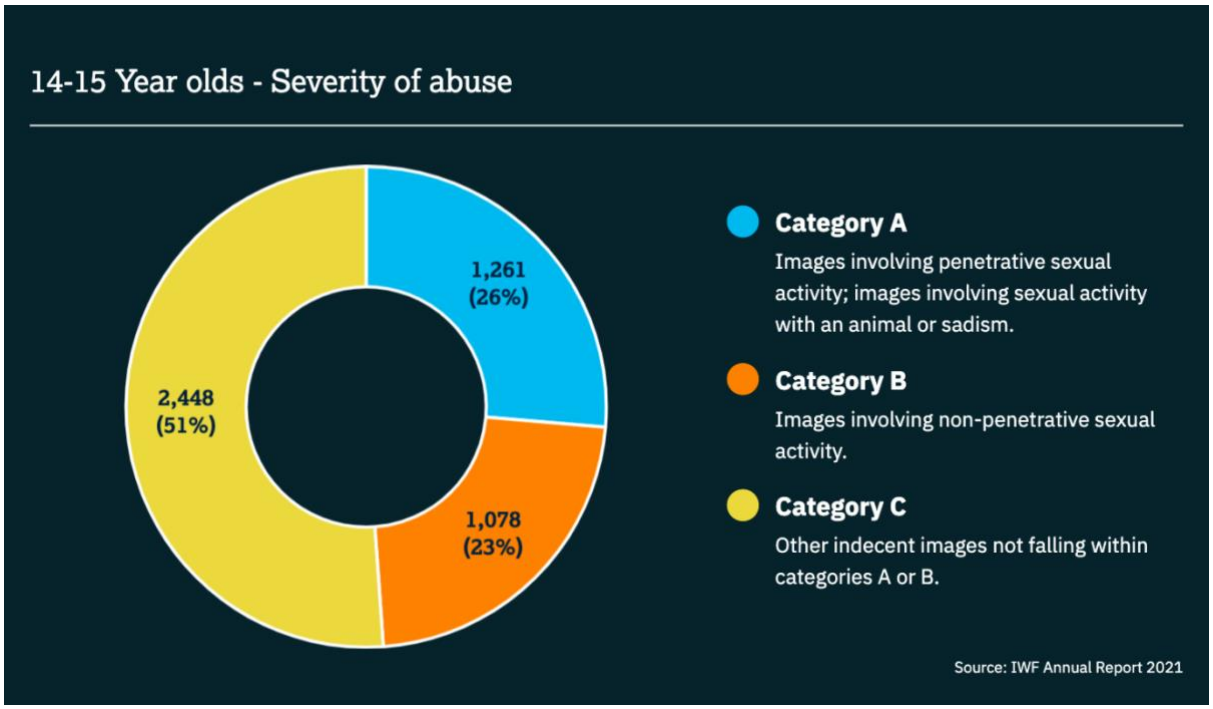
11-13 years: Older children

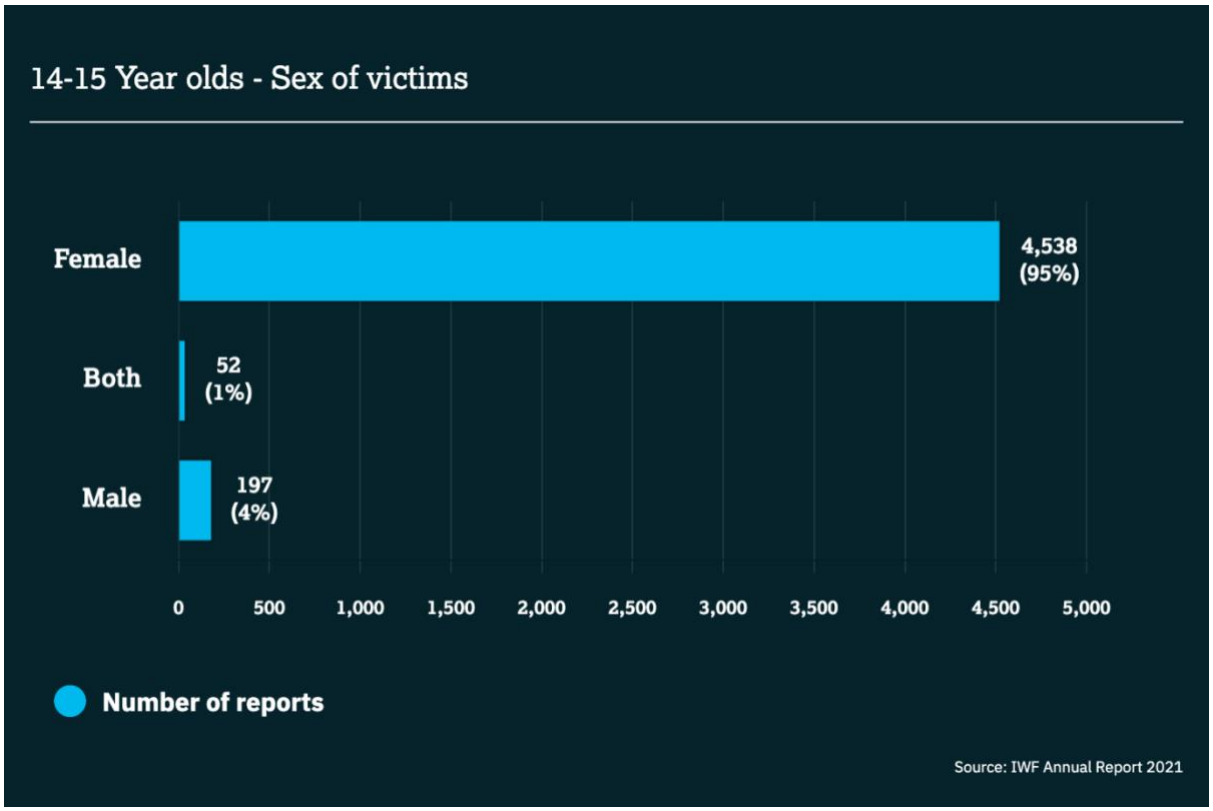




Life is increasingly lived online, and older children are often quick to explore new technology. As in previous years, we have seen more children aged 11-13 in “self-generated” child sexual abuse imagery, created using webcams or smartphones, than any other age group. These devices can act as an open door into children’s homes, often their own bedrooms.

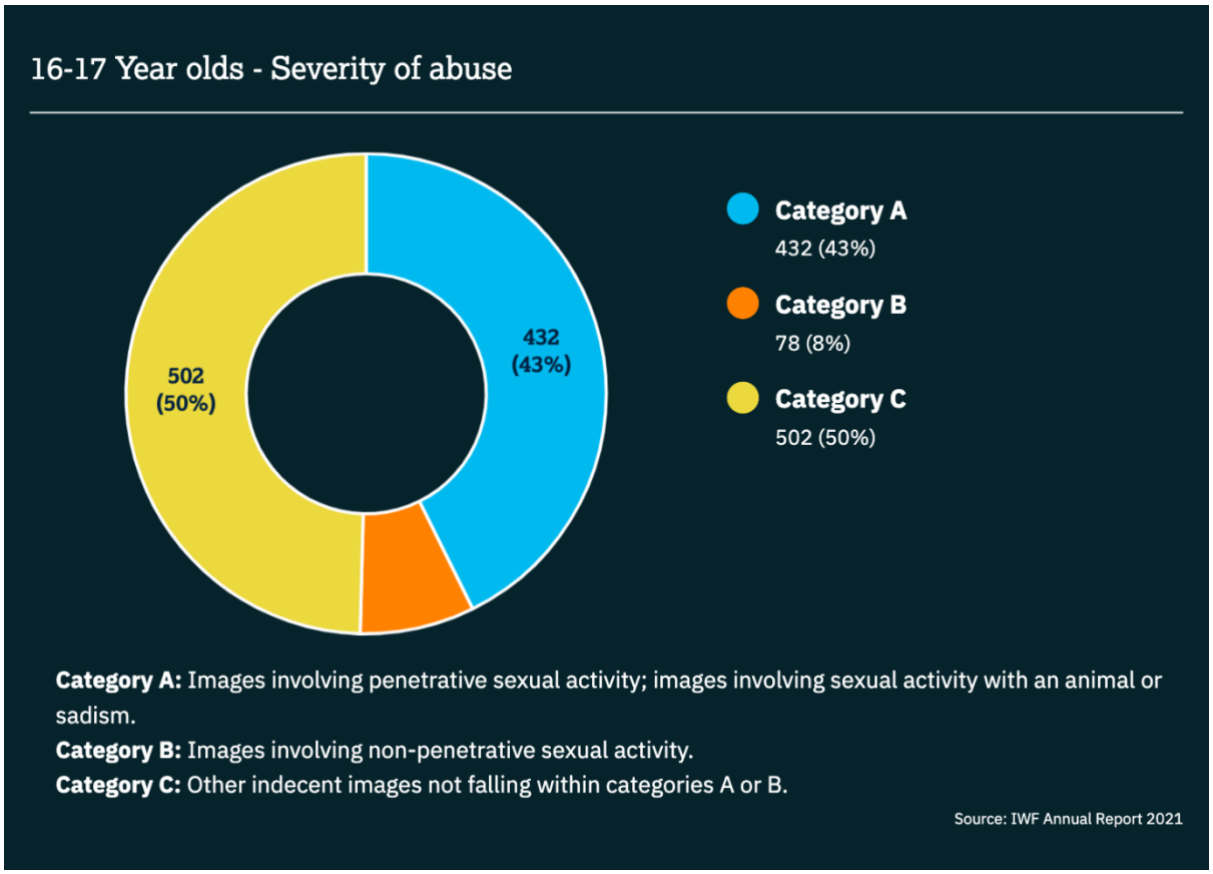
14-15 years: Teenagers

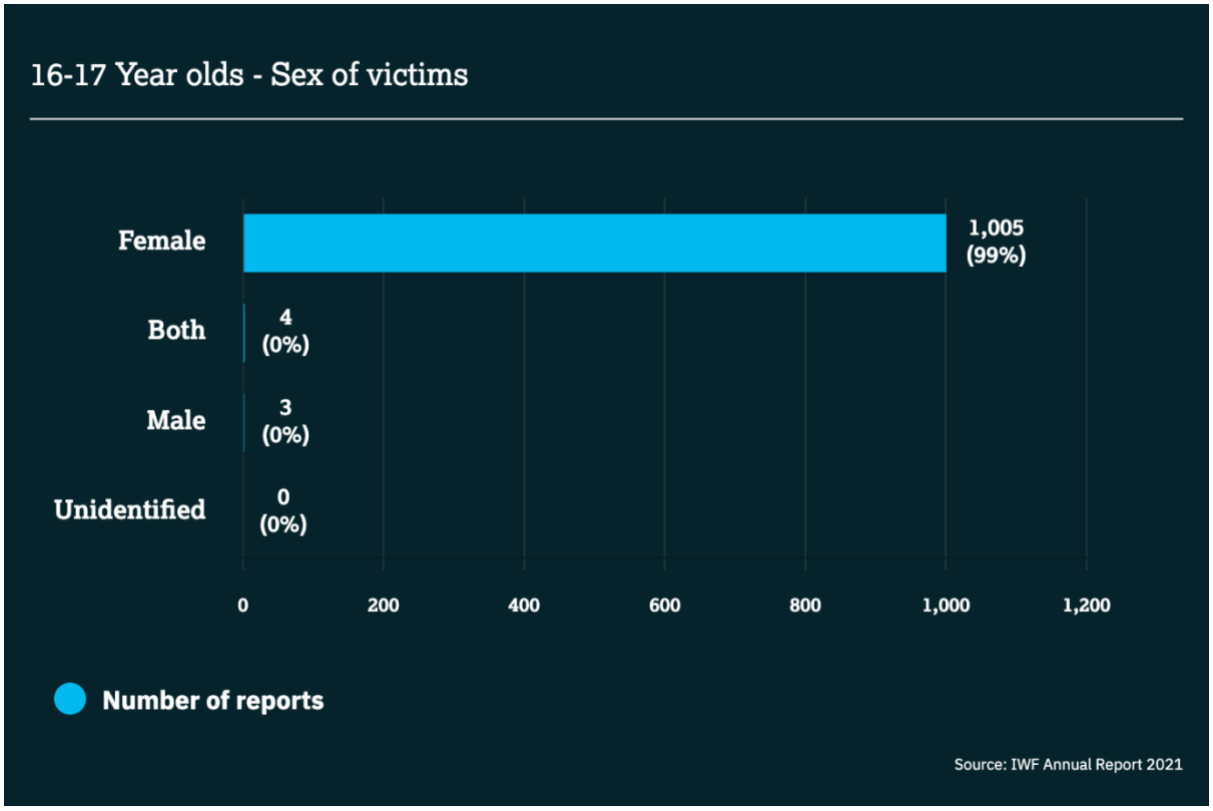




The pandemic has continued to impact teenagers' social lives, with many spending more time than ever online. Criminals will target children – girls in particular – and manipulate them into performing sexual acts on camera. These images are then shared across the internet, with the devastating result of re-victimising the child every time these images are viewed.

16-17 years: Teenagers





In many cases, the images we see of 16-17 year olds are “self-generated” and have initially been shared consensually with a boyfriend or girlfriend before being shared further online. As it can be difficult to assess the age of older teenagers accurately, we can only remove sexual imagery of them when their age has been verified. In 2021, we were able to remove more criminal images of older teenagers thanks to the launch of Report Remove which enables children to report their own sexual imagery to us, via Childline.

Trends & Data > Self-generated child sexual abuse

Overview

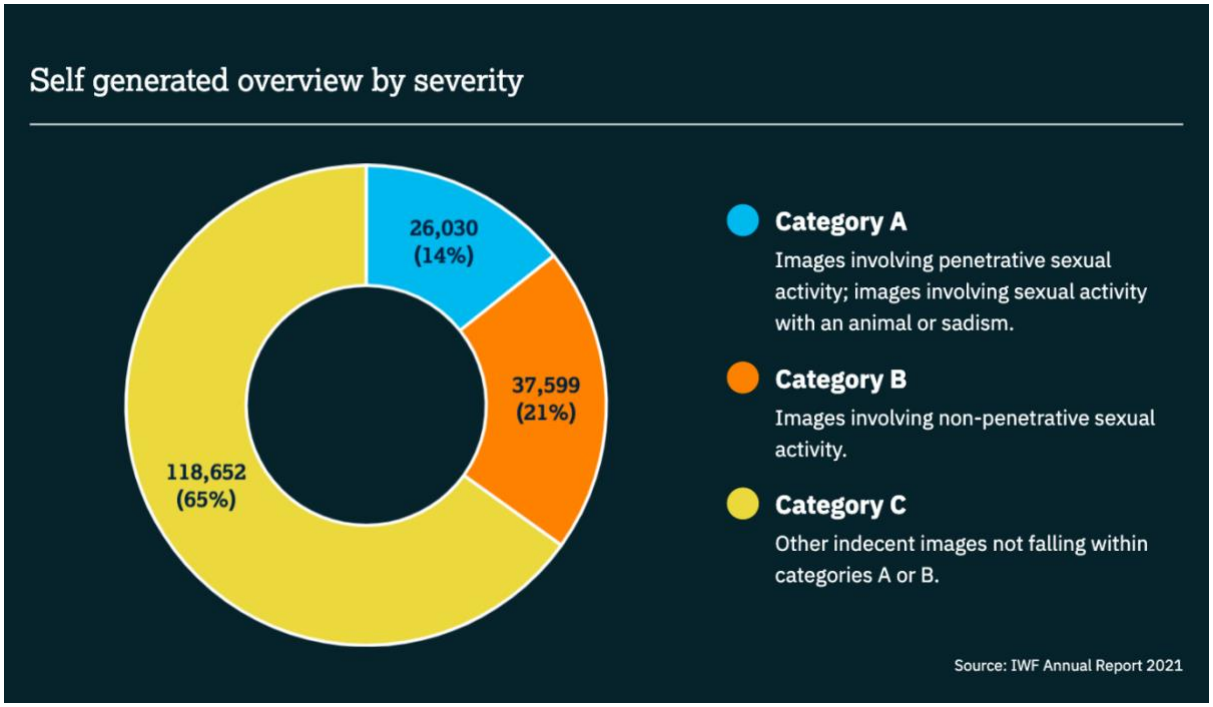
We continue to see an exponential increase in what is termed “self-generated” child sexual abuse content, created using webcams or smartphones and then shared online via a growing number of platforms. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves. The images and videos predominantly involve girls aged 11 to 13 years old, in their bedrooms or another room in a home setting. With much of the world subject to periods of lockdown at home due to COVID-19, the volume of this kind of imagery has only grown.

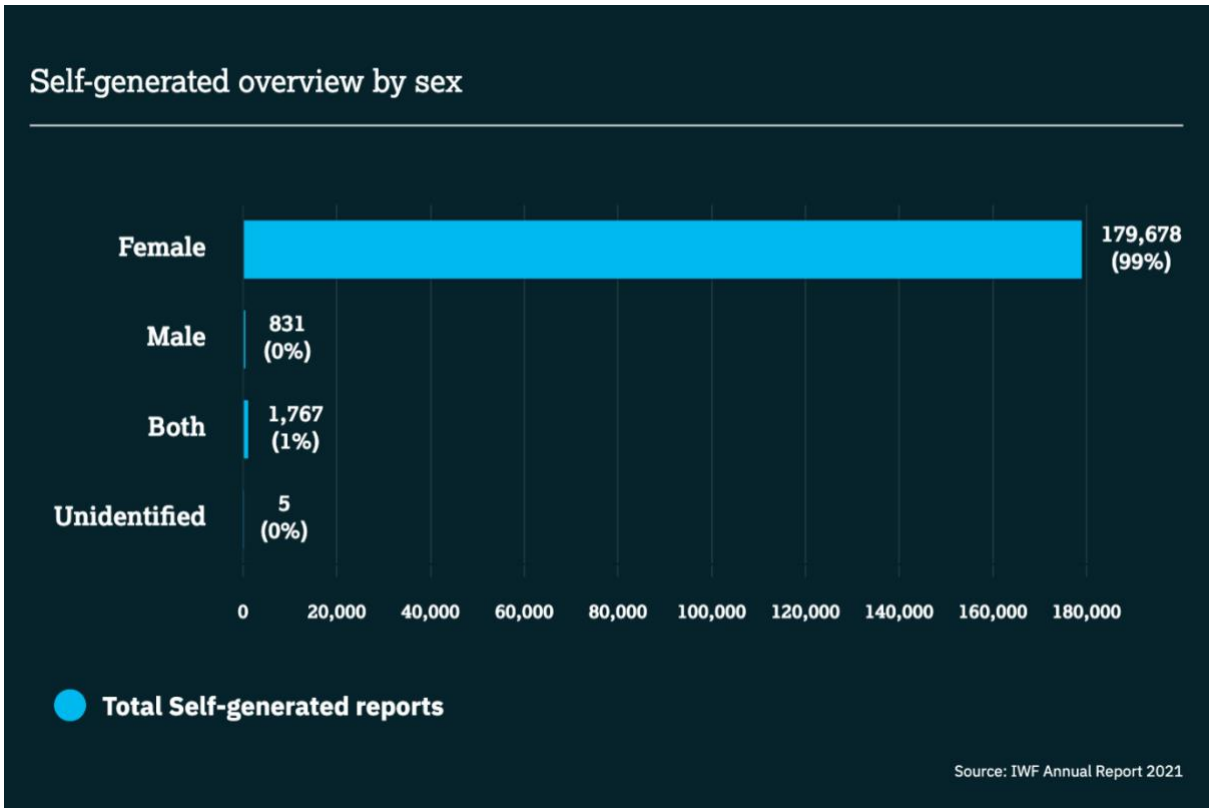
- In 2021, 147,188 reports included an 11-13 year old girl, who had been captured in either still images or videos in this way.
- This represents 59% of all actioned reports and 81% of self-generated child sexual abuse reports.

Frequently, these child sexual abuse images and videos have been produced using live streaming services, then captured and distributed widely across other sites by offenders. Once captured, these images and videos can be recirculated for years after they were originally created.

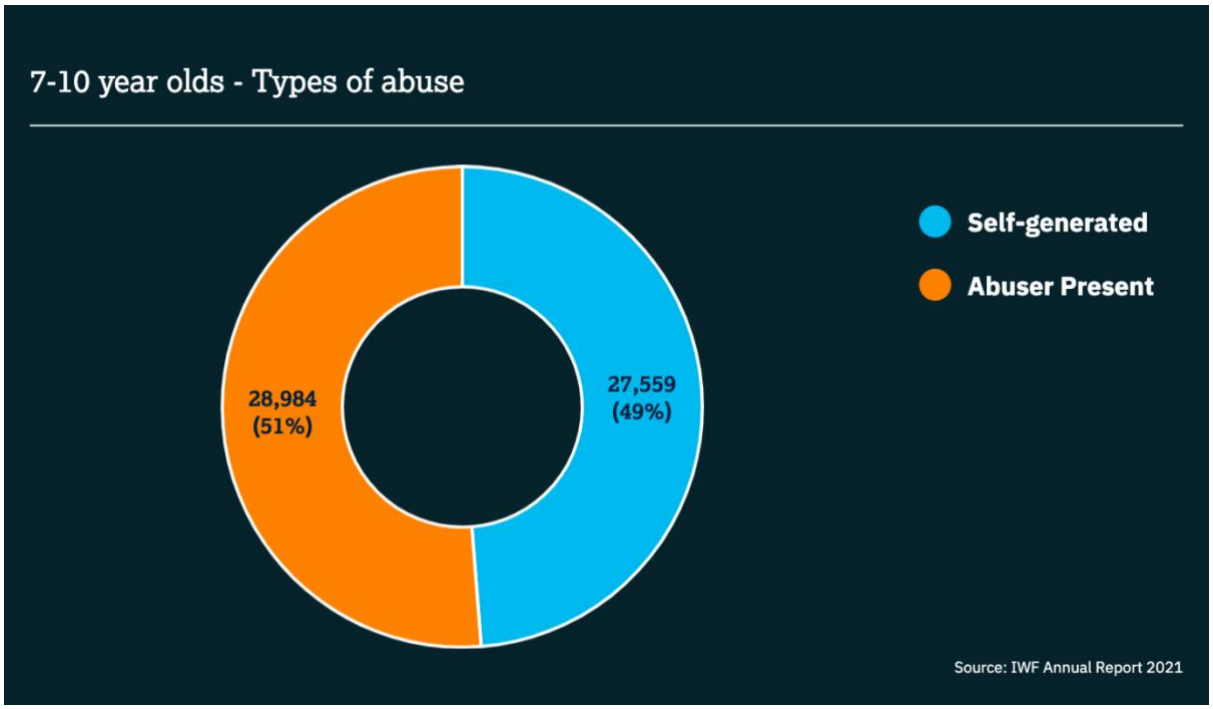
- Of the 252,194 webpages actioned during 2021, almost three quarters (182,281 or 72%) were assessed as containing self-generated imagery. This is a 28 percentage point increase on 2020 when 44% of actioned reports (or 68,000) were self-generated.
- This represents a 168% increase from 2020 to 2021 in the proportion of actioned webpages displaying self-generated imagery.

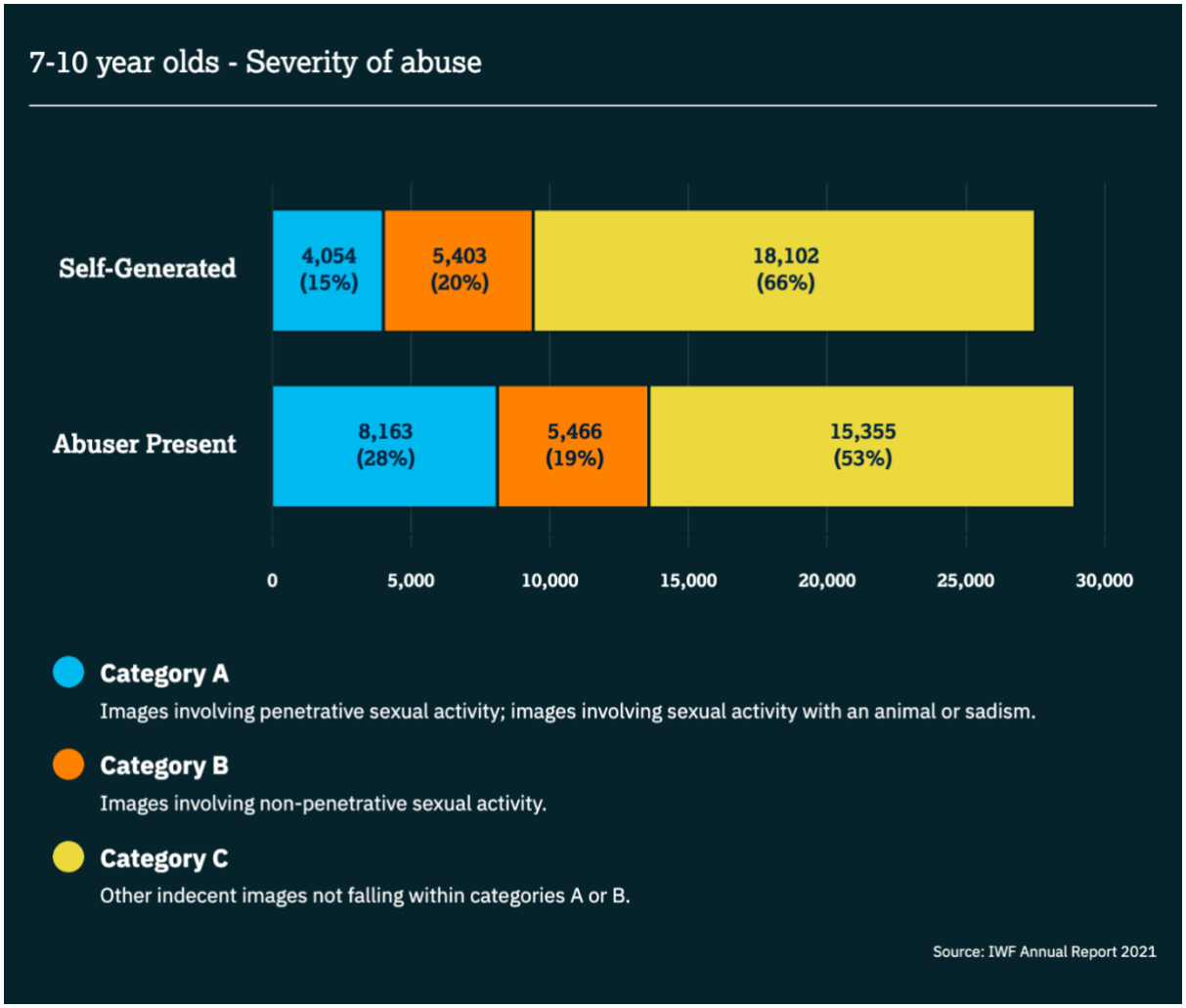
Our analysts noted a number of very young children, aged 3-6 years old being sexually abused in this way. You can read our snapshot study here.

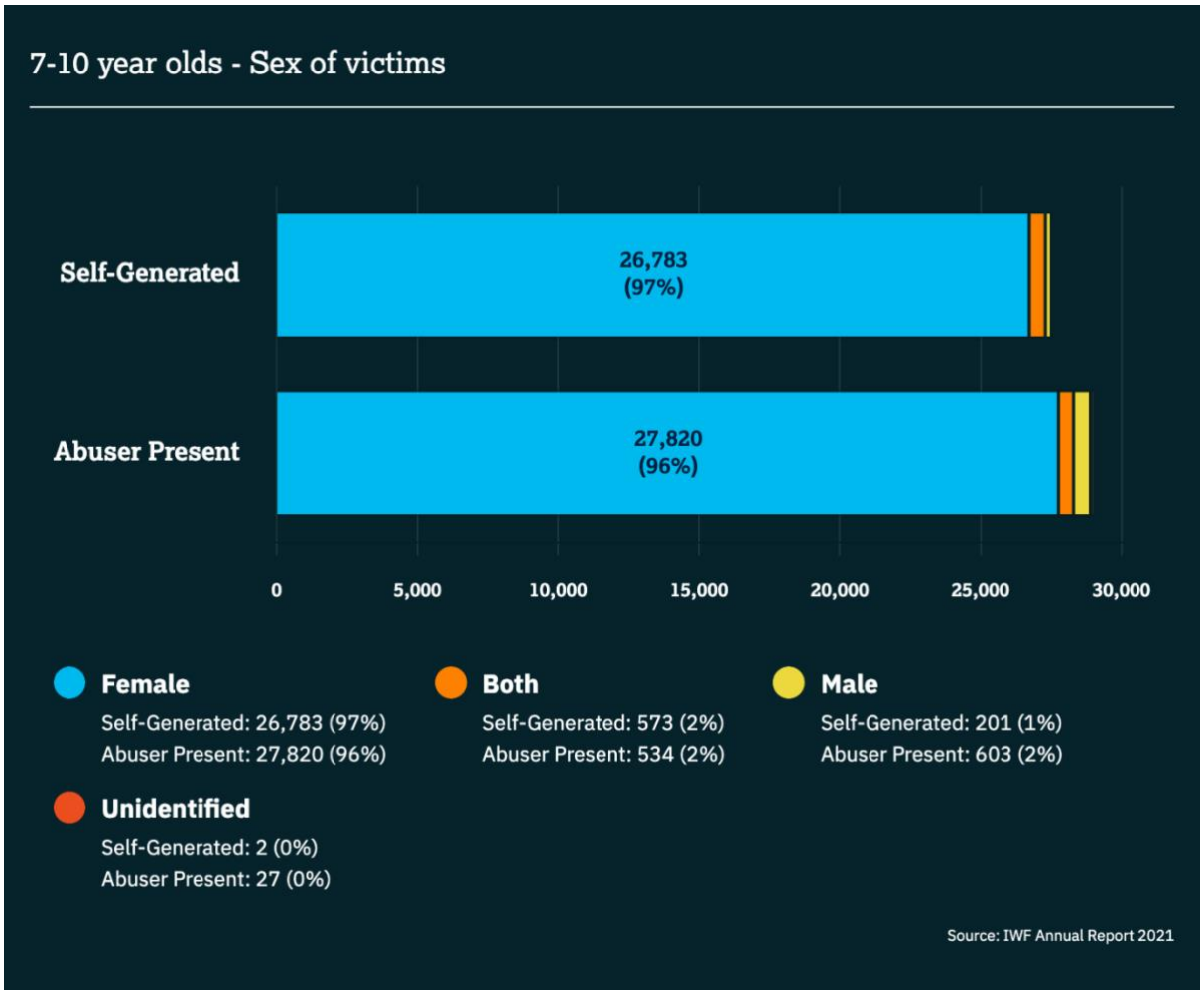

Self generated overview by severity
26,030 (14%)
37,599 (21%)
118,652 (65%)
Category A
Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.
Category B
Images involving non-penetrative sexual activity.
Category C
Other indecent images not falling within categories A or B.
Source: IWF Annual Report 2021


Self-generated overview by sex
Female
179,678 (99%)
Male
831 (0%)
Both
1,767 (1%)
Unidentified
5 (0%)
0
20,000
40,000
60,000
80,000
100,000
120,000
140,000
160,000
180,000
Total Self-generated reports
Source: IWF Annual Report 2021

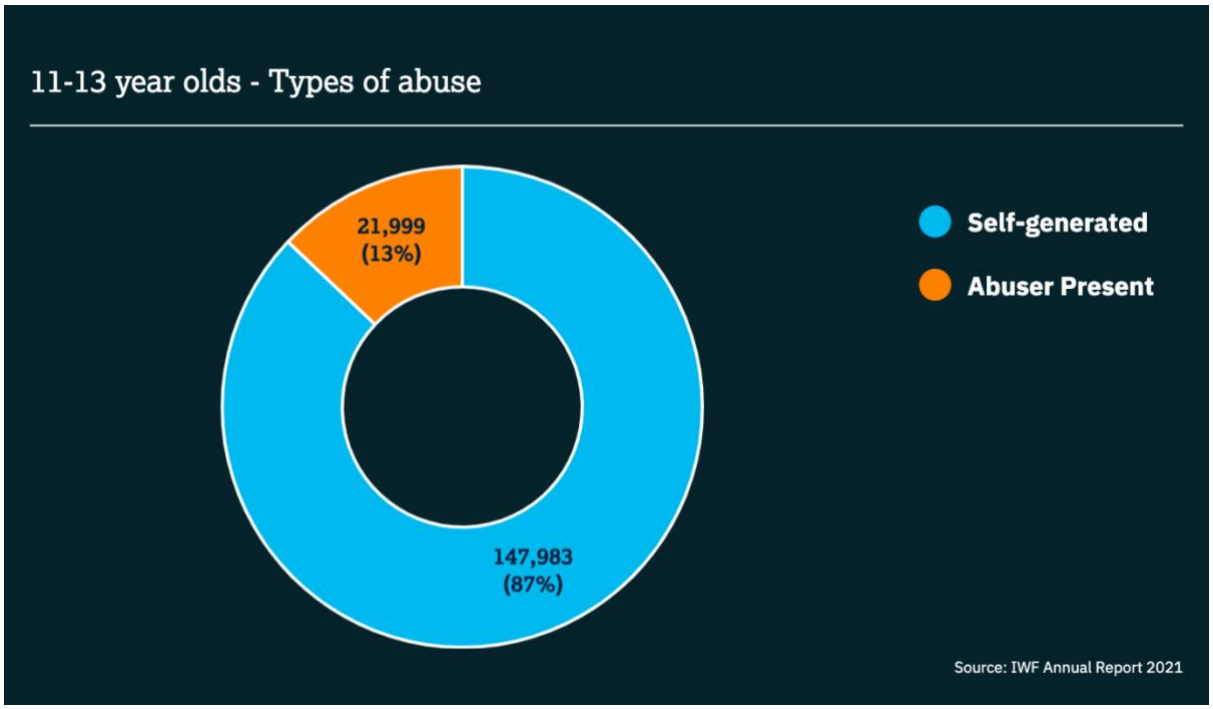
7-10 years: Pre-pubescent children

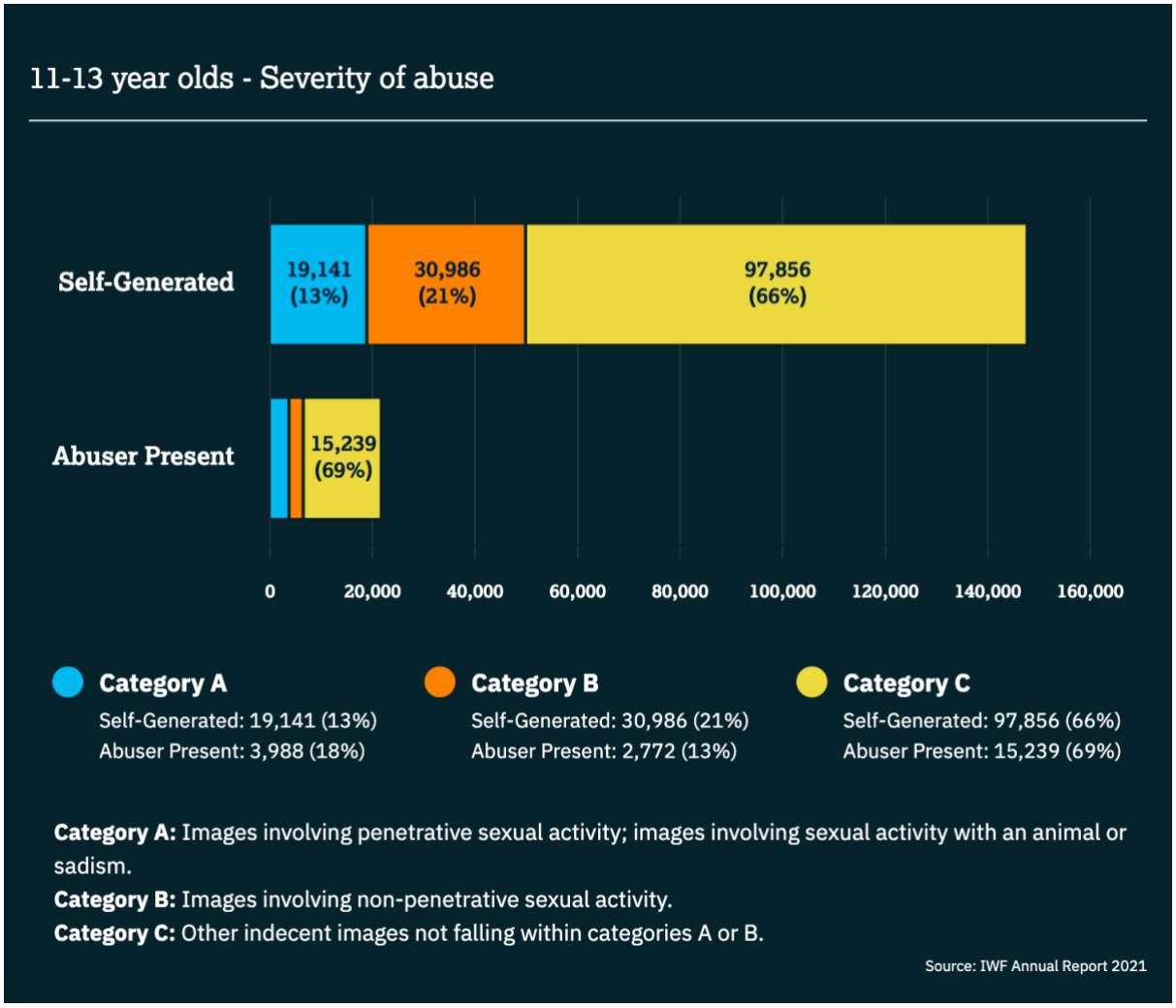


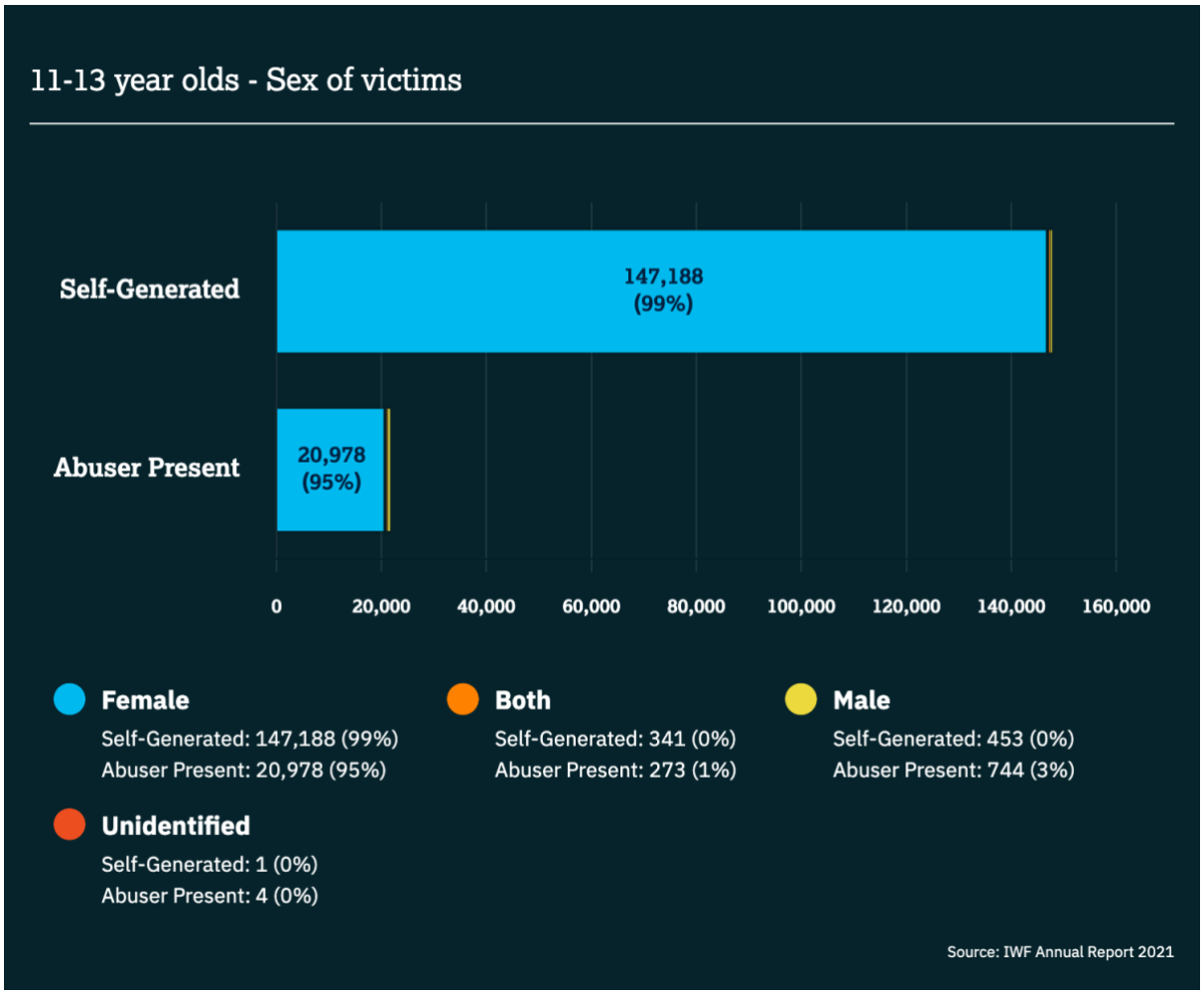



7-10 year olds - Sex of victims
Self-Generated
26,783
(97%)
Abuser Present
27,820
(96%)
0
5,000
10,000
15,000
20,000
25,000
30,000
Female
Self-Generated: 26,783 (97%)
Abuser Present: 27,820 (96%)
Both
Self-Generated: 573 (2%)
Abuser Present: 534 (2%)
Male
Self-Generated: 201 (1%)
Abuser Present: 603 (2%)
Unidentified
Self-Generated: 2 (0%)
Abuser Present: 27 (0%)
Source: IWF Annual Report 2021

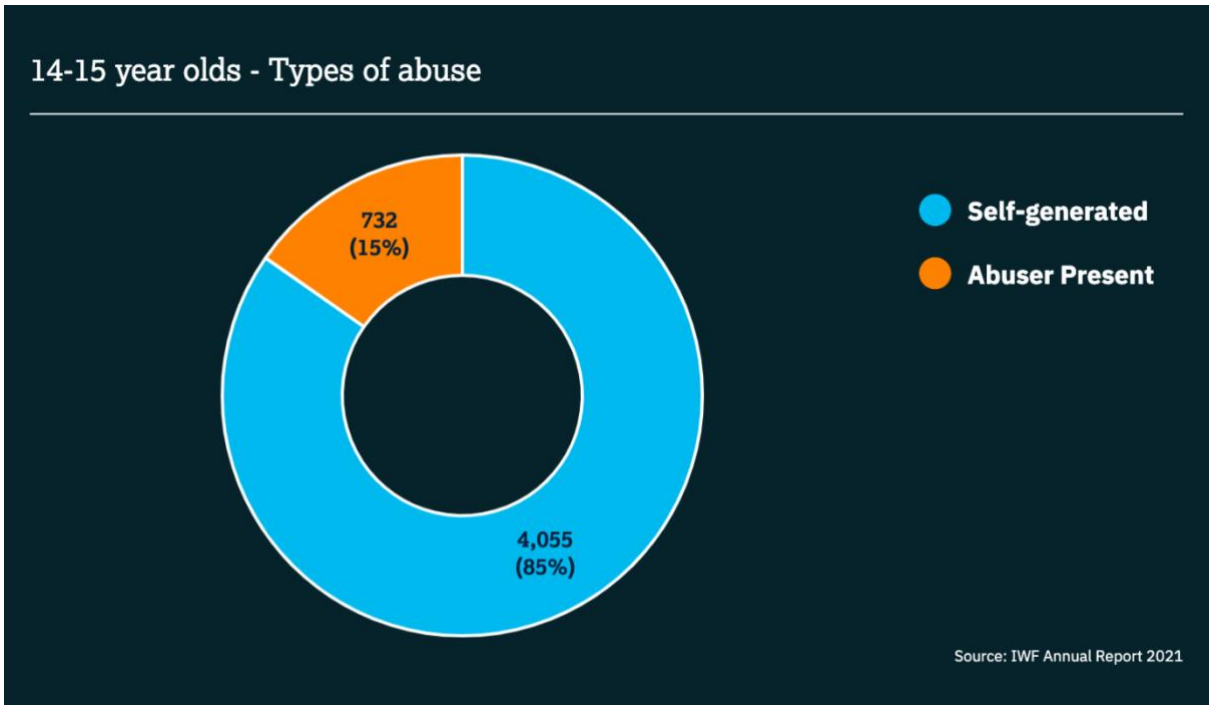
11-13 years: Older children

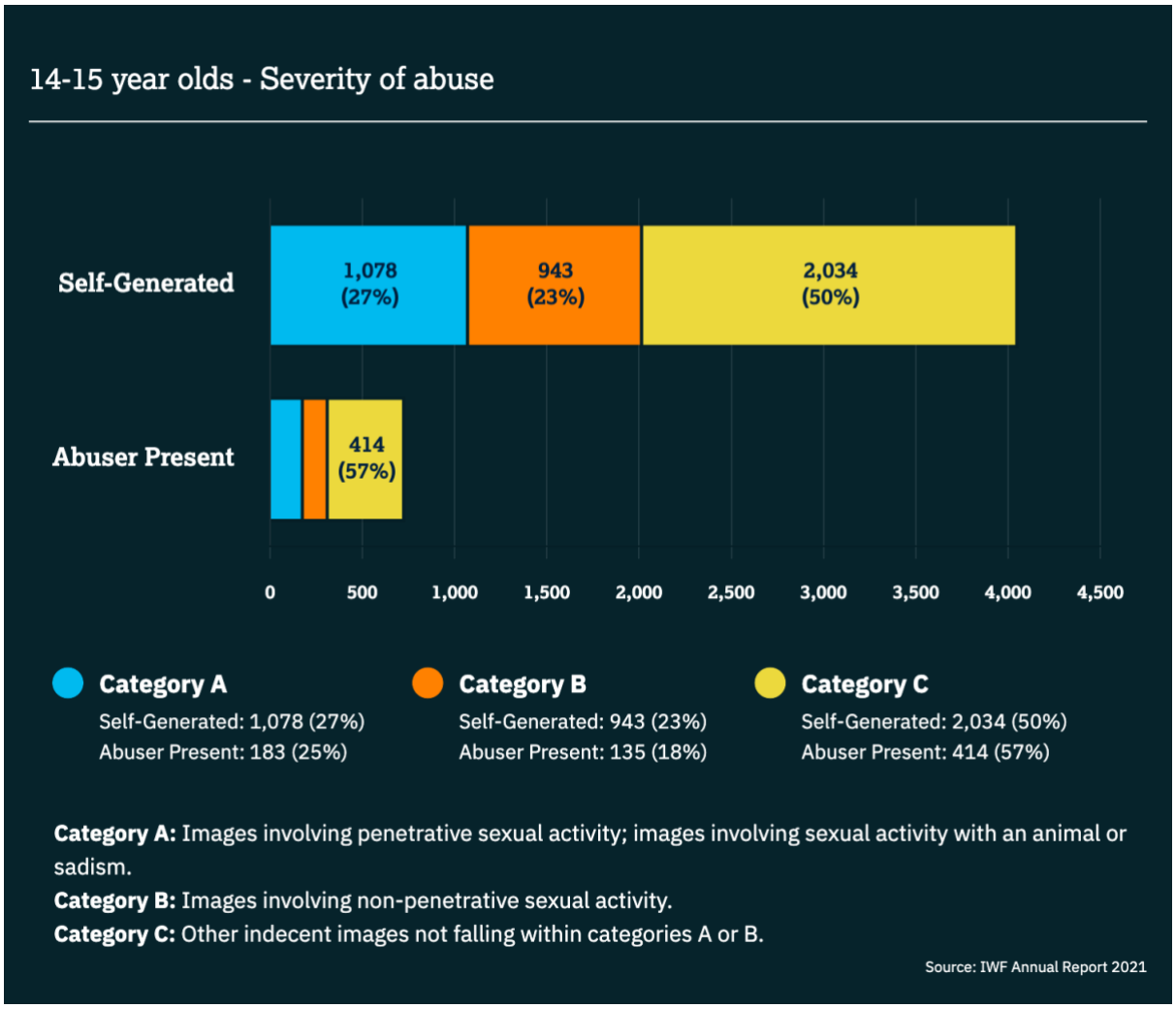


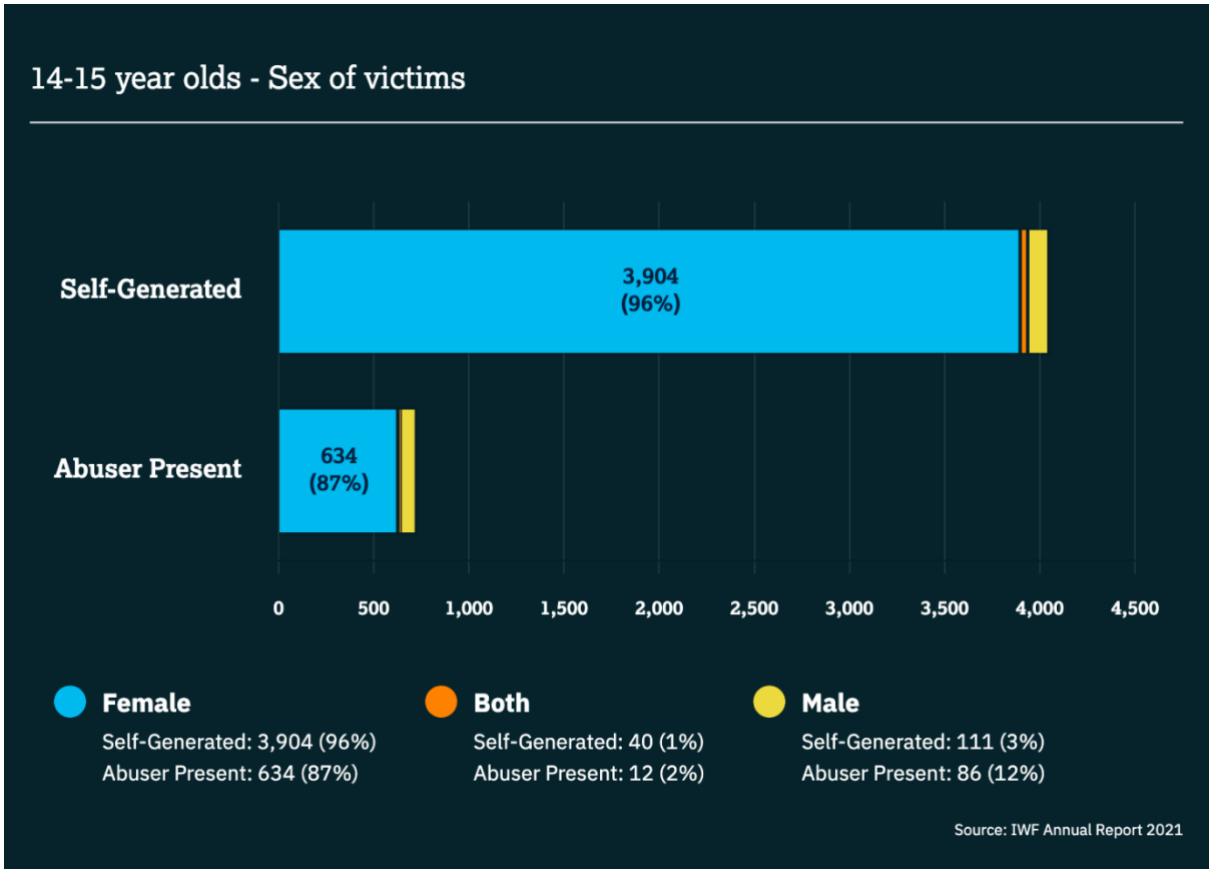



11-13 year olds - Sex of victims
Self-Generated
147,188
(99%)
Abuser Present
20,978
(95%)
0
20,000
40,000
60,000
80,000
100,000
120,000
140,000
160,000
Female
Self-Generated: 147,188 (99%)
Abuser Present: 20,978 (95%)
Both
Self-Generated: 341 (0%)
Abuser Present: 273 (1%)
Male
Self-Generated: 453 (0%)
Abuser Present: 744 (3%)
Unidentified
Self-Generated: 1 (0%)
Abuser Present: 4 (0%)
Source: IWF Annual Report 2021

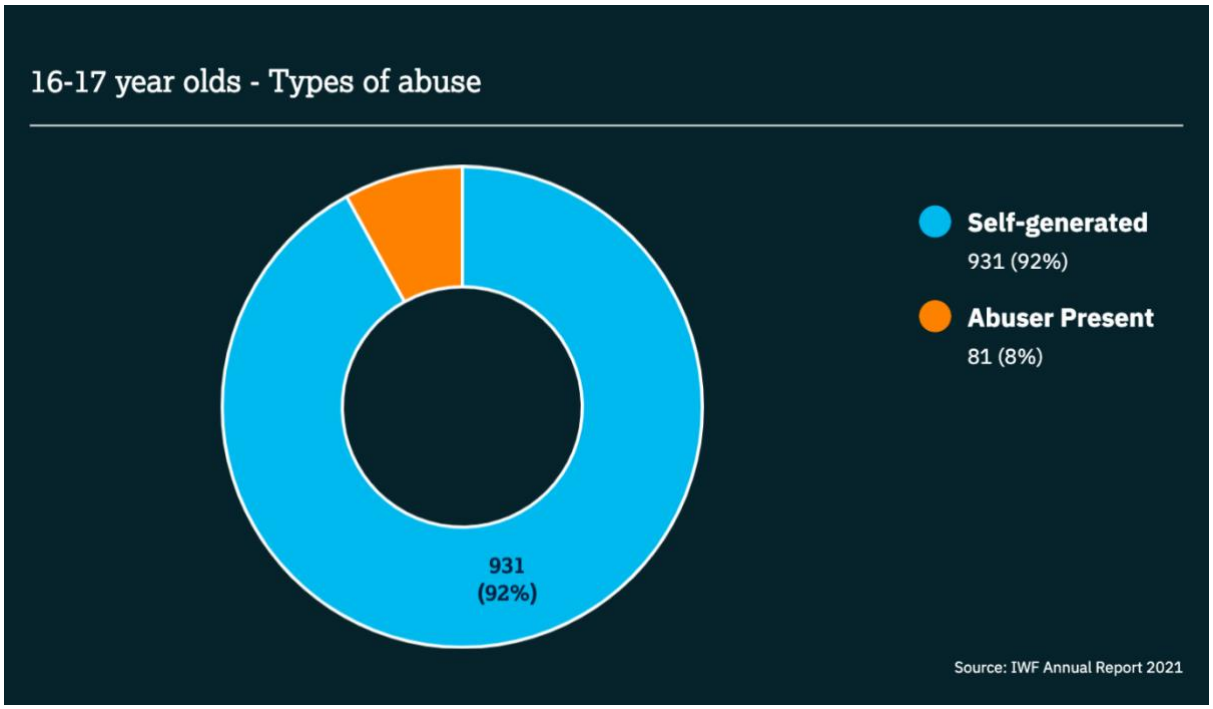
14-15 years: Teenagers

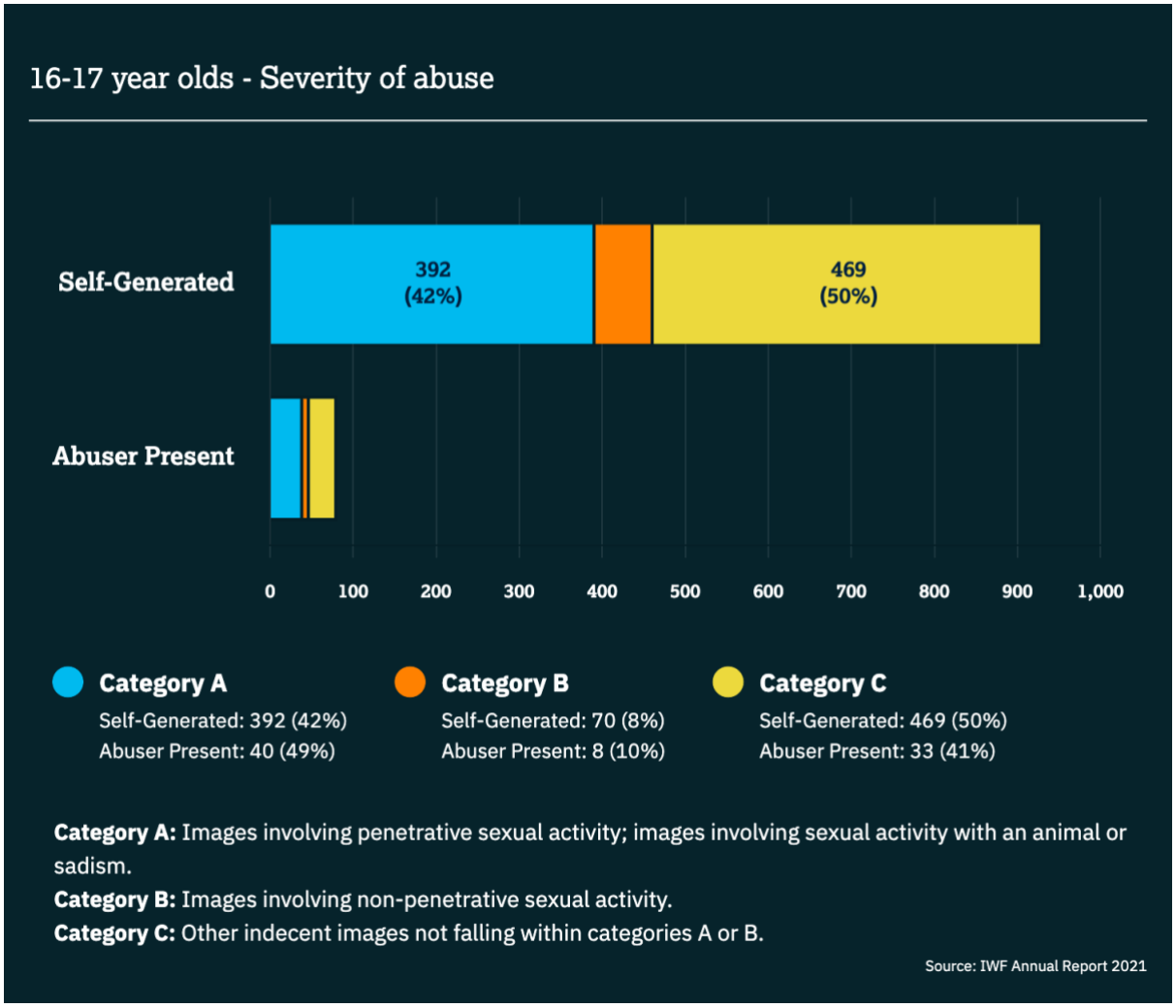


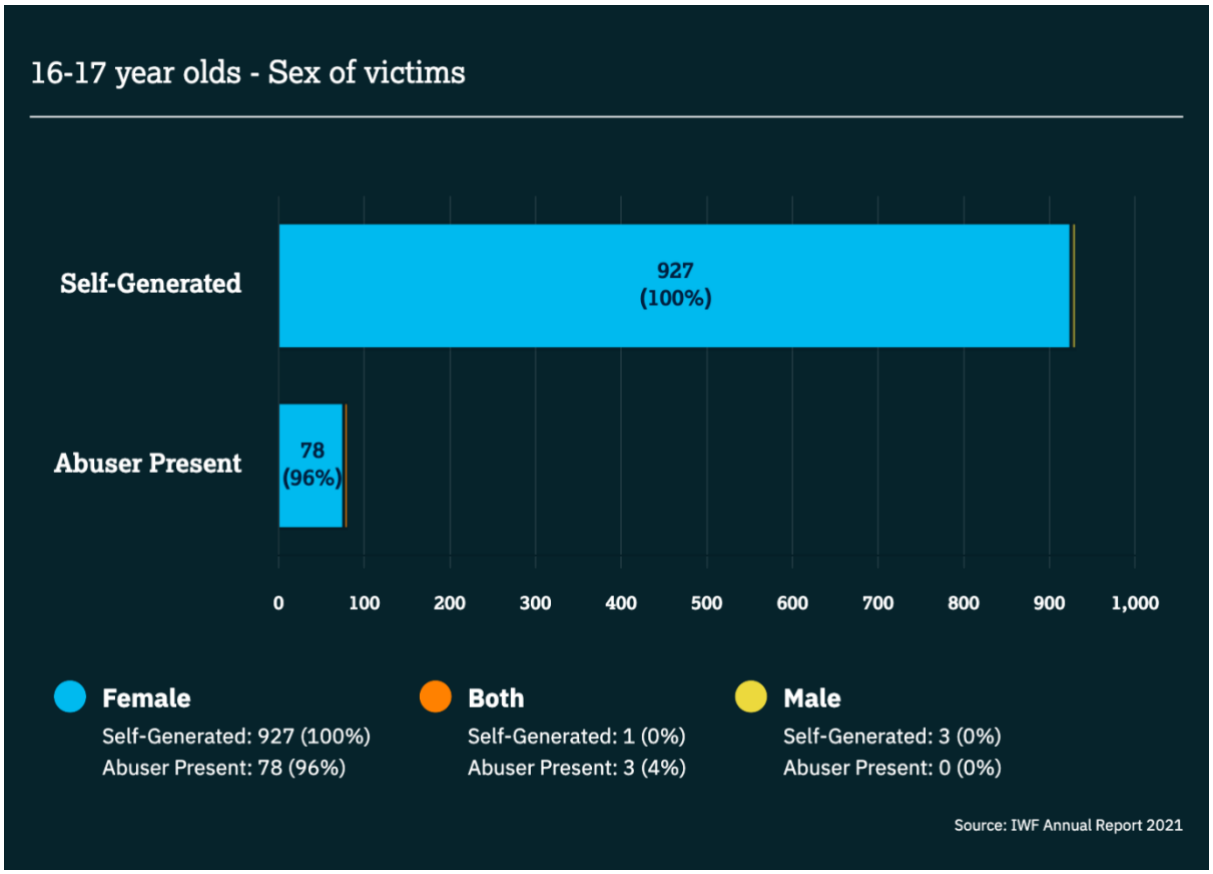



14-15 year olds - Sex of victims
Self-Generated
3,904
(96%)
Abuser Present
634
(87%)
0
500
1,000
1,500
2,000
2,500
3,000
3,500
4,000
4,500
Female
Self-Generated: 3,904 (96%)
Abuser Present: 634 (87%)
Both
Self-Generated: 40 (1%)
Abuser Present: 12 (2%)
Male
Self-Generated: 111 (3%)
Abuser Present: 86 (12%)
Source: IWF Annual Report 2021

16-17 years: Teenagers






16-17 year olds - Sex of victims
Self-Generated
927
(100%)
Abuser Present
78
(96%)
0
100
200
300
400
500
600
700
800
900
1,000
Female
Self-Generated: 927 (100%)
Abuser Present: 78 (96%)
Both
Self-Generated: 1 (0%)
Abuser Present: 3 (4%)
Male
Self-Generated: 3 (0%)
Abuser Present: 0 (0%)
Source: IWF Annual Report 2021

Trends and data > “Self-generated” sexual material of 3–6 year old children

An IWF snapshot study

In 2021 we saw a number of “self-generated” child sexual abuse reports involving much younger children than noted before. We decided to do a snapshot study to learn more about it.

“Self-generated” child sexual abuse content is created using webcams or smartphones and then shared online via a growing number of platforms. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves. The images are created of children often in their bedrooms or another room in a home setting and no abuser is physically present but may be present virtually via the internet.

Over the period of one month between 11 October and 10 November, we asked analysts to record specific instances of self-generated content where at least one of the children was understood to be aged 3-6.

Assessment:

- During this time **51 reports** were found to include a child aged 3-6 which was deemed to contain self-generated content.
- Averaged out over 23-days (workdays), this equates **to 2 instances being found each day**.
- 35 of these reports were found to be either duplicate images or videos or to contain the same child/children on more than one occasion.
- Several images/videos were found to have the same naming convention: Of the 51 images and videos found, 31 of these followed the same naming convention found across 3 different sites. 20 of these were within the duplicates mentioned above.

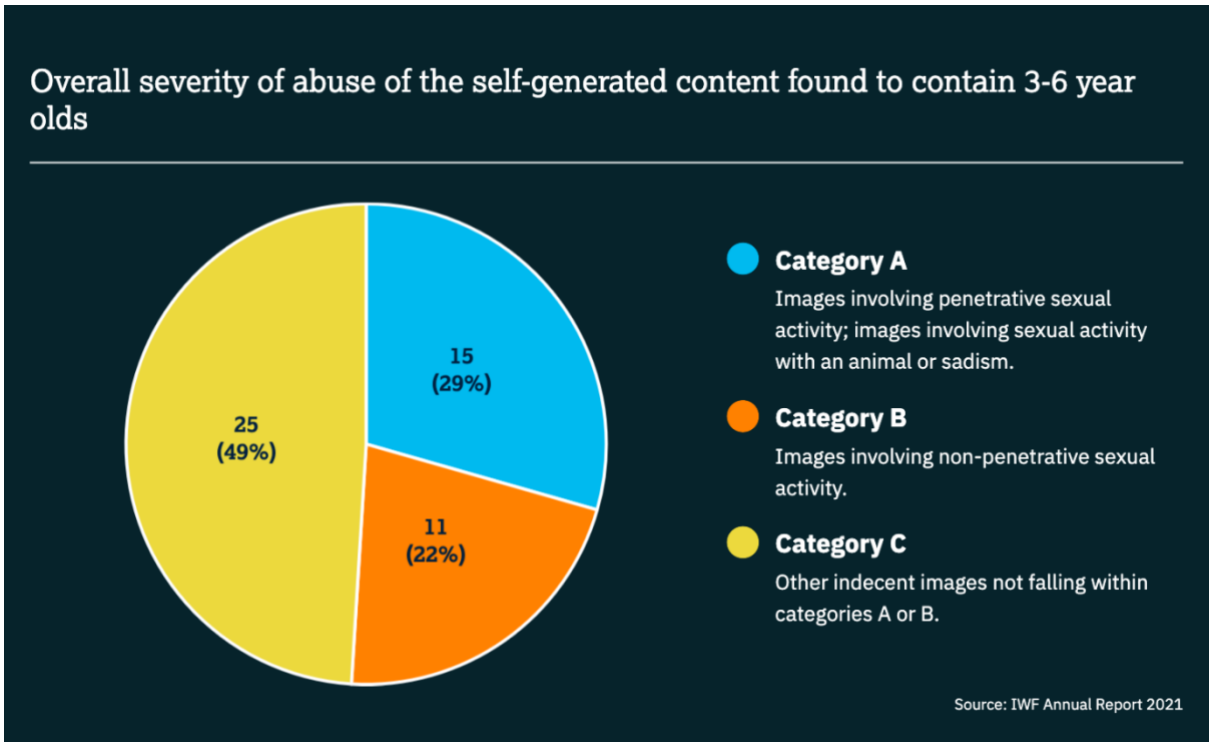
Sexes and age relevance:

- Three in every four instances (76% or 39 images/videos) showed girls; the remaining 12 instances showed boys.
- Almost three in every five instances (57% or 29 images/videos) involved either a sibling or friend. Of these cases:
    - In 7 out of 10 (69% or 20 images/videos) the additional child was 7-10 years old;
    - In 3 out of 10 (28% or 8 images/videos) the additional child was 11-13.
    - In the 1 remaining instance, the children were within the same age range (3-6).
- In just over 1 in 10 instances (12% or 6 images/videos) we saw a lone child nearer the lower end of 3-6 age group. Predominantly, in 6 in 10 instances (61% or 31 images/videos) the children were nearer the higher end of this age bracket.

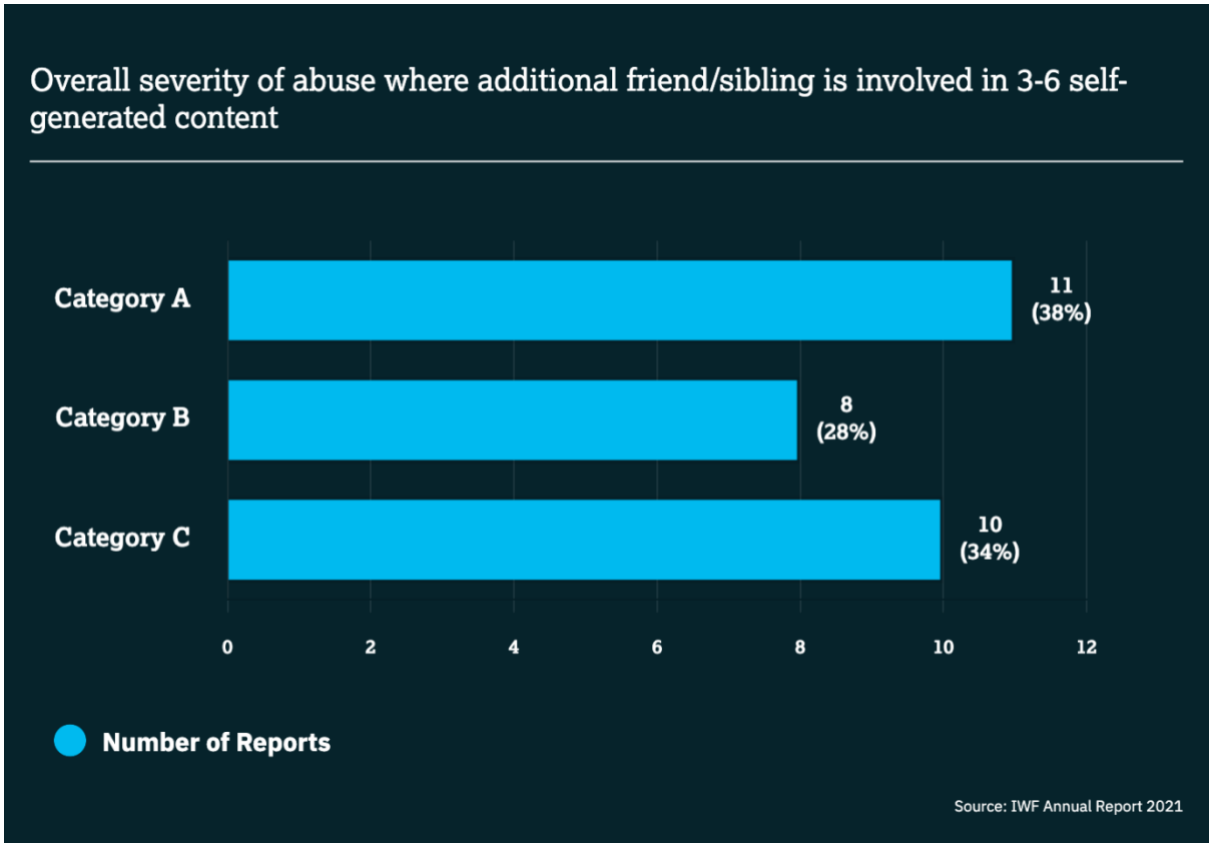
Severity:

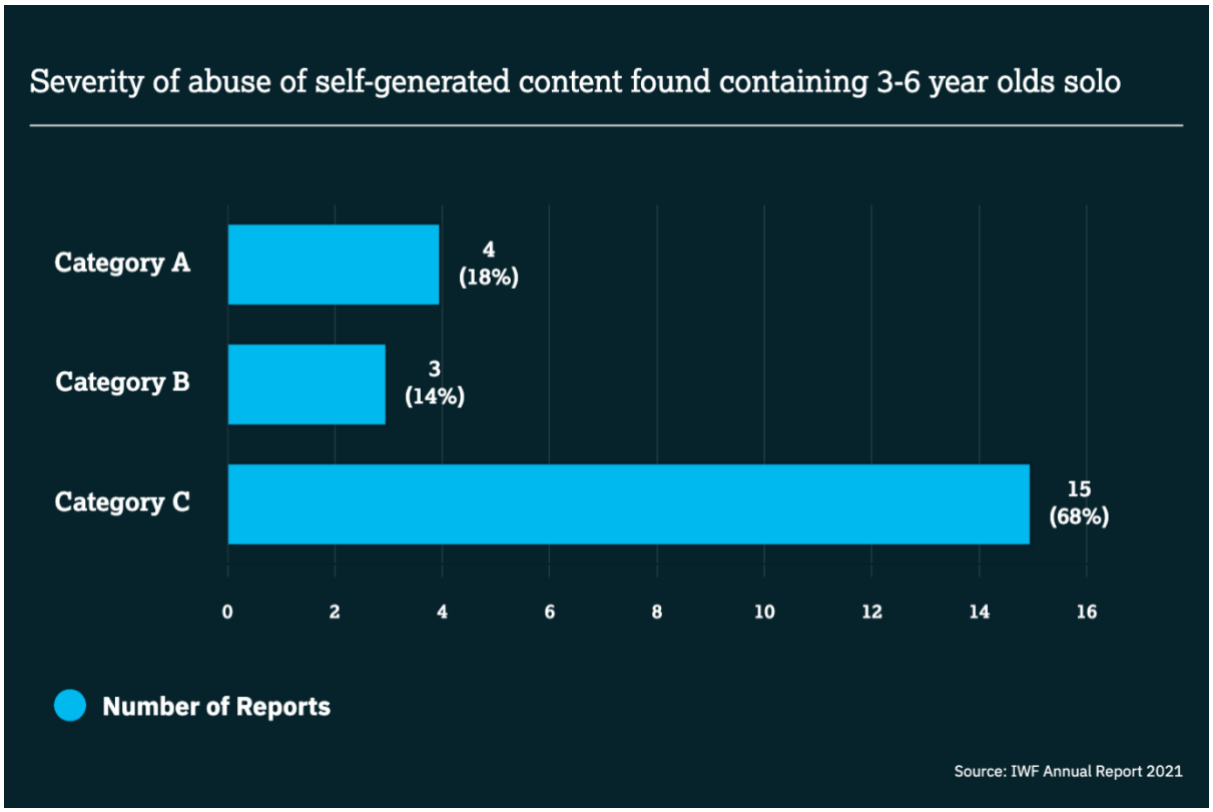
In the UK, child sexual abuse is categorised according to the Sentencing Council’s Guidelines:

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



Category C was found to make up almost half (49%) of the content found overall.


Overall severity of abuse where additional friend/sibling is involved in 3-6 self-generated content
Category A
11 (38%)
Category B
8 (28%)
Category C
10 (34%)
0
2
4
6
8
10
12
Number of Reports
Source: IWF Annual Report 2021


Severity of abuse of self-generated content found containing 3-6 year olds solo
Category A
4 (18%)
Category B
3 (14%)
Category C
15 (68%)
0
2
4
6
8
10
12
14
16
Number of Reports
Source: IWF Annual Report 2021

Comparison of severity where children are solo verses the abuse that involves an older sibling:

When siblings or friends were involved, we saw a relatively even split across the severity categories of child sexual abuse. The majority of instances, however, involved Category A abuse accounting for nearly 2 in every 5 instances (38% or 11 images/videos). When children were alone, we most often saw Category C activity.

Unfortunately, predators seem to prey on young children and use the trust and formed bond between the victims to extend the abuse further, and in these cases, to reach much younger children. On the videos we heard the children encouraging each other or being the role model to follow.

Observations from the videos:

It is sometimes wrongly assumed that children are aware that what is being asked of them is wrong or inappropriate. When referring to 3-6 year old children, they do not understand the inappropriateness of what they're being asked to do, especially when led by a sibling or friend.

With each study we perform there is always an element of the data that stands out and below are some of the stark realities of what we see:

- Some young children appear to be "performing" as if it's a show. It's evident this is not the first time this has happened to them and they are obviously trying to "please" an audience, unaware of the inappropriateness being asked of them. They have no concept of the abuse that is happening to them; we see them giggling, as if it's just a little bit naughty with no apparent thought of what offenders will do with that content.

- There were several videos and images that showed children intently looking into the camera, assumingly reading, or viewing something to then replicate it. Their faces were immersed and full of concentration, showing no emotion, demonstrating that these innocent children are being coerced into performing these acts with no understanding of their severity. In many of the videos, phones can be heard buzzing and the children then pause to read and carry out a different request, often not hesitating at what is being asked of them.

- There was one set of two young children (boy and girl) along with other children in the room that couldn't be seen providing encouragement. The two children were performing a sexual act and, given their apparent confidence, we can assume that they must have seen this before. They change sexual positions and the boy (younger of the two) quotes lines such as "do you like that baby" and "love you".

- There was one compilation of child sexual abuse content that showed at least two girls aged 3-6. In all, there were more than 30 different children within the compilation, which was put together like a slideshow. It was accompanied by upbeat music.

- One video contained a young boy, aged four years old, whose sister was performing to a camera indicating what she was going to do to her brother. His face cannot be seen, but it was evident he was unaware what he was about to participate in. His reactions

alone suggest he is young, saying he is scared she will bite him and after the act was carried out he was heard saying “eww” suggesting he didn’t like it.

It’s not just one video or one image...

- A higher number of images were found in comparison to videos. Most of the videos were around 2 minutes long and the videos had been cropped to immediately display sexual activity of the child, with little lead in.

- We saw evidence that one instance of three videos initially uploaded together within a file was re-uploaded to a different cyberlocker within a short period of time, having been split, stored separately, and renamed in the process.

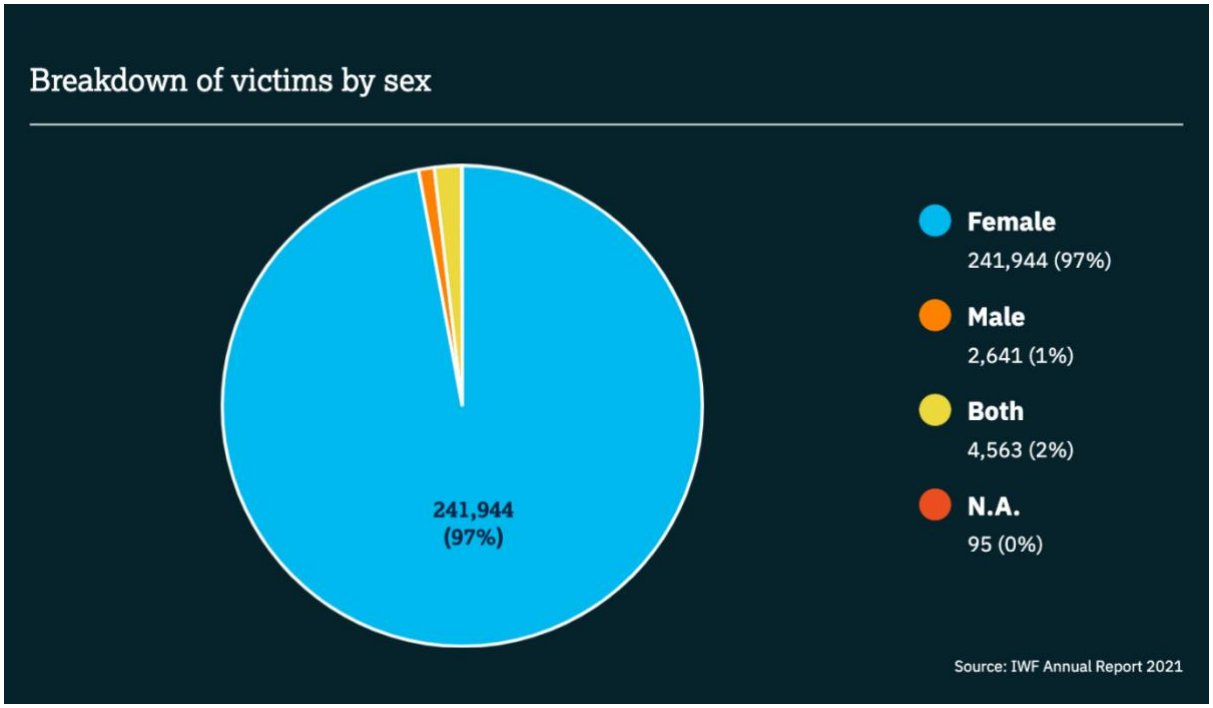
- In another instance, we saw how one original video was cut into still images, which were then shared more widely on individual URLs. The girl in the video was wearing a recognisable t-shirt making her easy to spot across multiple instances.

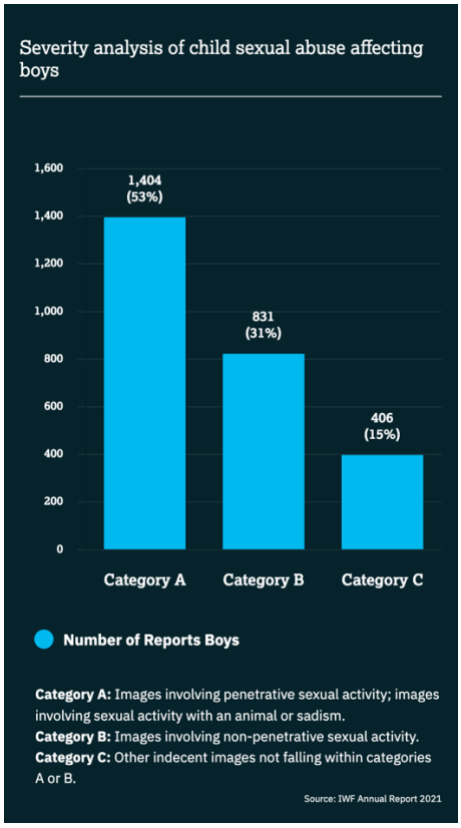
How does this study help our work?

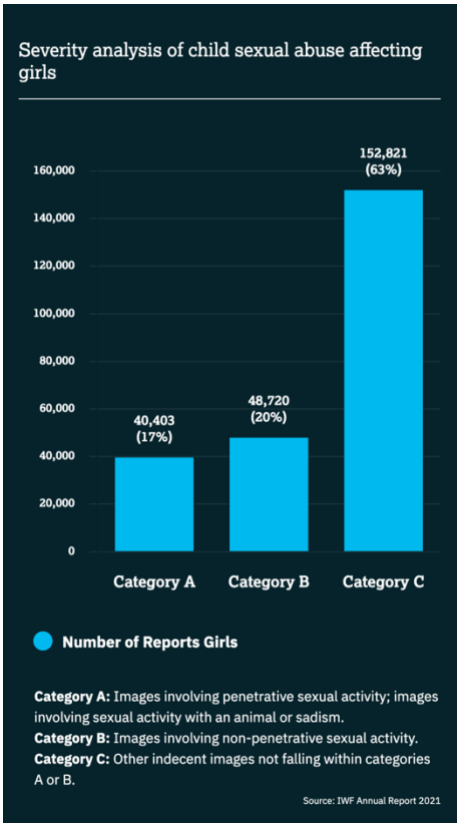
We hope that by understanding the crimes committed against children it will help our, and others’, knowledge of the problem and lead to new ways of tackling this criminality and protecting children.

Trends & Data > Sexual abuse of boys

In 2021, just 1% or 2,641 reports showed the sexual abuse of boys only. Within this subset of data, we can see that a higher proportion of the imagery of boys compared to girls shows category A child sexual abuse: 53% compared to 17%.







Trends and data > The prevalence of female offenders in child sexual abuse imagery

An IWF snapshot study

Internet Watch Foundation (IWF) is the UK body working internationally to identify and remove child sexual abuse images and videos online. Our annual statistics show that images featuring the sexual abuse of girls are most prevalent. And when our analysts see an offender, they are most often a man.

There has been no analysis of the prevalence of female abusers in the images and videos we see. Therefore, we carried out a focused analysis on a subset of data that involves female offenders for two months, between 1 April and 31 May 2021.

We found there to be a dominance of imagery featuring child victims aged 7 to 10 years old. We also discovered that boys are most often abused.

Method

During the data collection period, our analysts were asked to specifically monitor reports for images or videos that clearly involved an adult woman (or women) engaged in the sexual abuse of children.

Given that one report might contain one, or many tens or hundreds of individual images and videos, one of our quality assurance team separated out all the individual images and videos of relevance to this study to perform the analysis and recorded 504 instances.

In the UK, child sexual abuse is categorised according to the Sentencing Council's Guidelines:

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

We recorded the age of the child victim in each image or video. Where more than one child appears, we recorded the age of the youngest child, falling within these categories: 0-2, 3-6, 7-10, 11-13, 14-15, 16-17.

We also recorded the sex of the victim: Boy, girl, or both if the instance included a combination of male and female children.

It was not part of the study to try and establish where geographically the imagery had been recorded.

The data

We found that:

- Images showing a female abuser were seen on average 13 times per working day.
- In half of the images and videos (49%) showing a female abuser, she was abusing a boy.
    - Whilst there is no directly-comparative data, we can compare against *all* reports* actioned by IWF during 1 April – 31 May, and the whole of 2020.
        - 1 April – 31 May: 3% of *all* child sexual abuse reports which showed an offender present with a child showed a male victim.
        - For the whole of 2020: 4% of *all* child sexual abuse reports which showed an offender present with a child showed a male victim.

- Just over half of the content was Category A (53% or 267 instances) where the female abuser is seen engaging in penetrative sexual activity, sadism or bestiality.
    - 28% is based on images alone (74 images of 267 Category A instances)
    - 72% is based on videos (193 videos of 267 Category A instances).

      By comparison:
        - 1 April – 31 May: 26% of *all* child sexual abuse reports which showed an offender present with a child showed Category A content.
        - For the whole of 2020: 17% of *all* child sexual abuse reports which showed an offender present with a child showed Category A content.

- Category A content is most often seen in videos, rather than still images.

- In still images, female offenders are most often seen abusing children aged 7-10.

- In videos, female offenders are most often seen abusing children aged 3-6.

** One report of child sexual abuse may contain one, or many tens, hundreds or thousands of individual images. Please note that this study analysed individual images and videos of child sexual abuse. Where comparison data is provided, this is data based upon report analysis, not individual image/video analysis.*

Data tables

The below data tables show a breakdown of the results noting the severity of the abuse, the age of the victim, and the sex of the victim.

Category of abuse by number of images and videos			
Severity of abuse	**Number of images**	**Number of videos**	**Total**
Category A	74	193	267
Category B	162	65	227
Category C	10	0	10
Total	246	258	504

Ages of victims by number of images and videos			
Age of victim	**Number of images**	**Number of videos**	**Total**
0-2	12	30	42
3-6	60	110	170
7-10	102	79	181
11-13	26	29	55
14-15	46	10	56
Total	246	258	504

Sex of victims by number of images and videos			
Sex	**Number of images**	**Number of videos**	**Total**
Both	10	22	32
Girl	104	93	197
Boy	130	141	271
Unidentified	2	2	4
Total	246	258	504

Our analysts also observed that in assessing the video content within the 7-10 age bracket, 75% of those videos involved boys. Our broader statistics show that in the vast majority of cases, girls are the primary victims of child sexual abuse in the content we see during the course of our work, however this snapshot study reveals that in these particular cases involving women, it's boys who were more likely to be sexually abused.

There were duplicates of the same images and videos being shared across multiple sites, and one frequently seen set was indicative of an organised set up whereby children were sexually abused and filmed in what was likely either a hotel room or apartment involving more than one woman.

Some videos were up to 30 minutes long, and some were compilations of female offenders. Where there were compilations showing different women, for the purposes of this study, this was recorded as one video.

How does this study help our work?

We hope that by understanding the crimes committed against children it will help our, and others', knowledge of the problem and lead to new ways of tackling this criminality and protecting children.

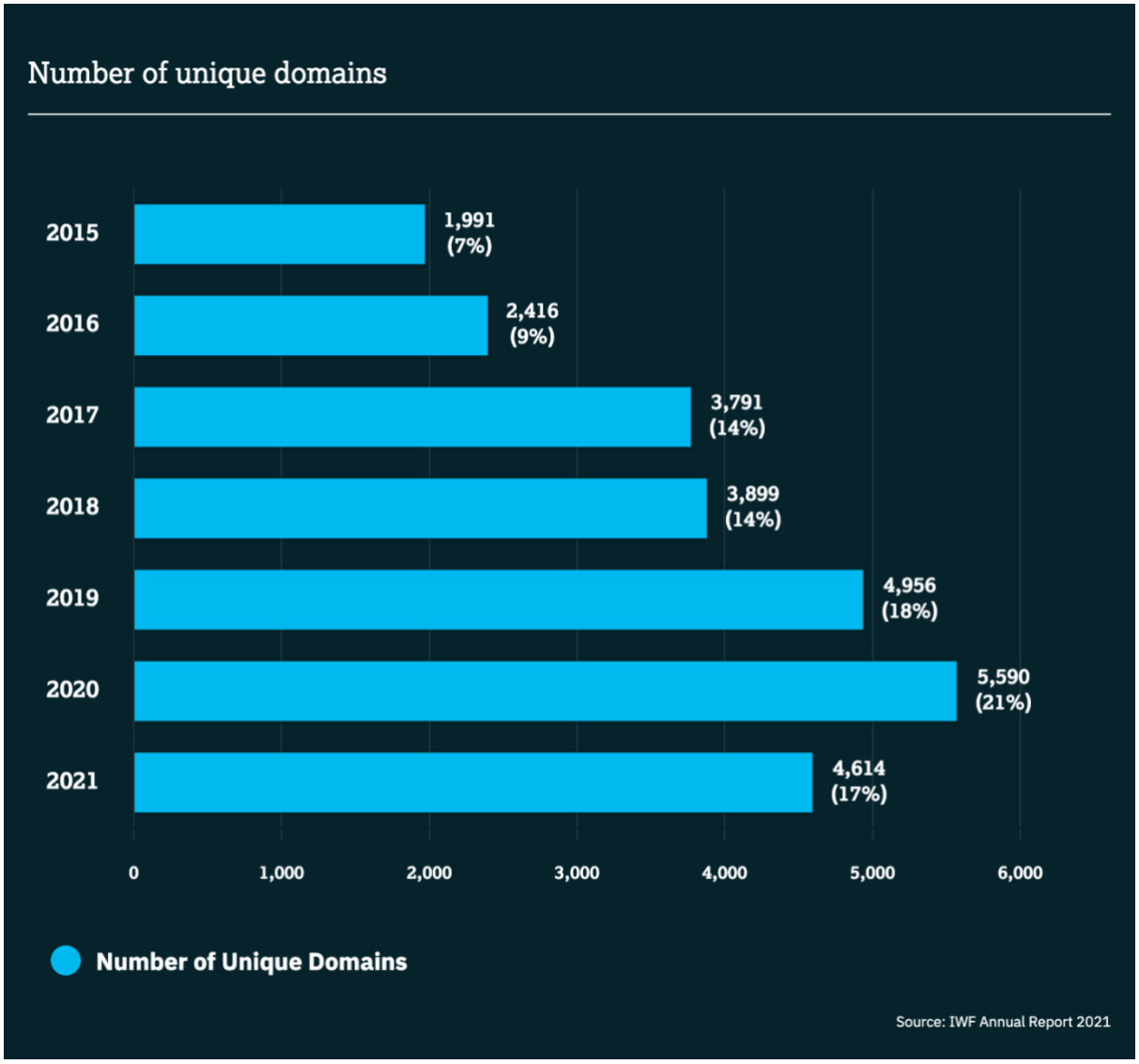
Trends & Data > Domain Analysis

For clarity, the diagram below sets out the domain naming conventions used throughout this report.

Despite the significant increase in the number of reports actioned in 2021, we observed a decline in the number of unique domains hosting child sexual abuse material.

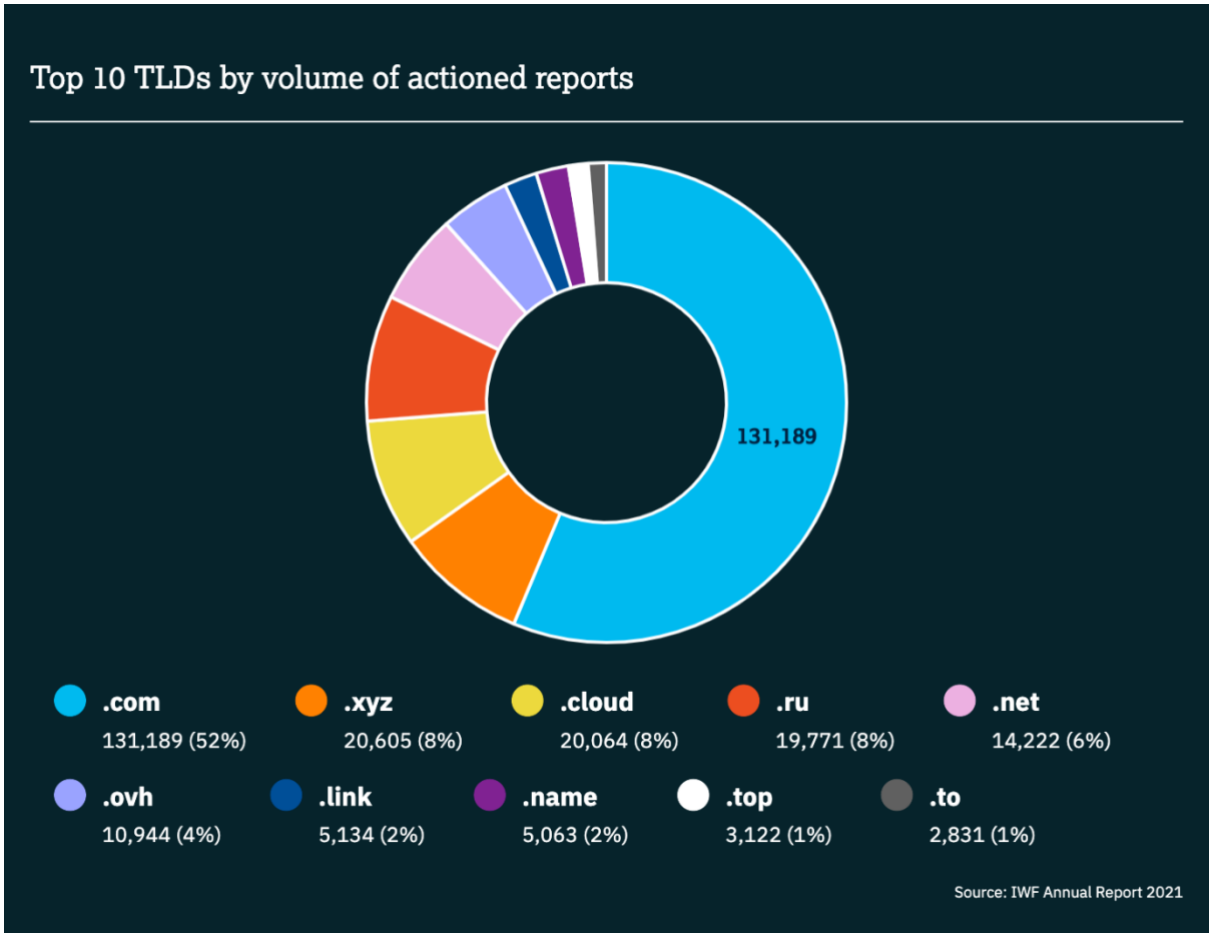
The number of unique domains fell from 5,590 identified in 2020 to 4,614, a decrease of 976 domains or 21%.

However, the number of unique domains created solely for the distribution of child abuse images for financial gain, made up 66% of all actioned domains, an increase of 6% on the previous year.



Websites containing child sexual abuse content were registered across 168 top level domains: 82 generic Top Level Domains (gTLDs), and 86 country code Top Level Domains. Domains were traced to hosting services in 56 countries.

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



Domain names

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.

Our monitoring of TLDs shows some significant changes in the top 10 listings for 2021. Notable changes include the .ovh gTLD that was actioned by the IWF for the first time in 2021 despite it being introduced as a new TLD in 2014 and has subsequently quickly risen into the top 10 listings.

The .xyz and .cloud TLDs were actioned at relatively low numbers in previous years but have both risen into the top 10 listings, replacing some of the previous higher listings including .net which has reduced from 23% to 6% of identified content.

The .ru country code TLD (ccTLD) doubled as an overall percentage of total content identified and in reporting terms saw a 238% increase in the volume of reports compared to 2020.

What can we do about this abuse?

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

View the case study

Volume of Second-level domains and dedicated commercial domains on each TLD

"www.badsite.com" - in this URL, the '.badsite' is the second level domain of the website address.

We have published data for the first time that gives additional insight into the scale and nature of TLD domains abused to show child sexual abuse material.

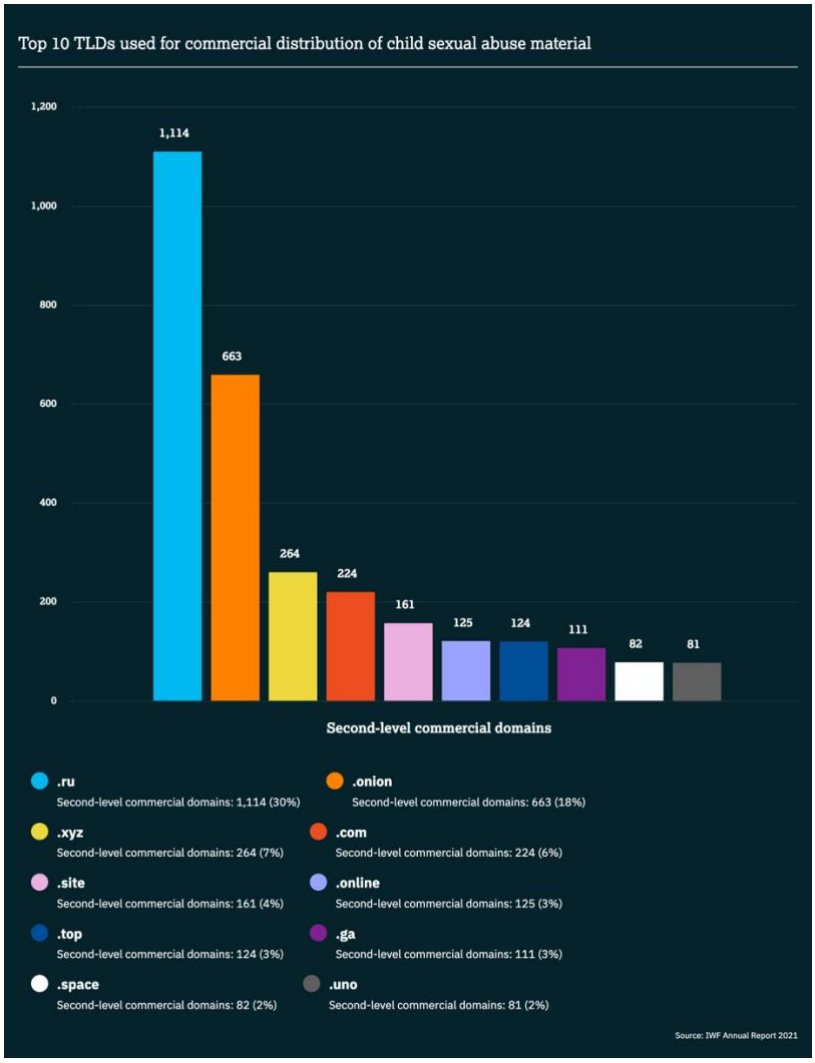
We are able to show the number of unique second-level domains found to be carrying child sexual abuse grouped by TLD.

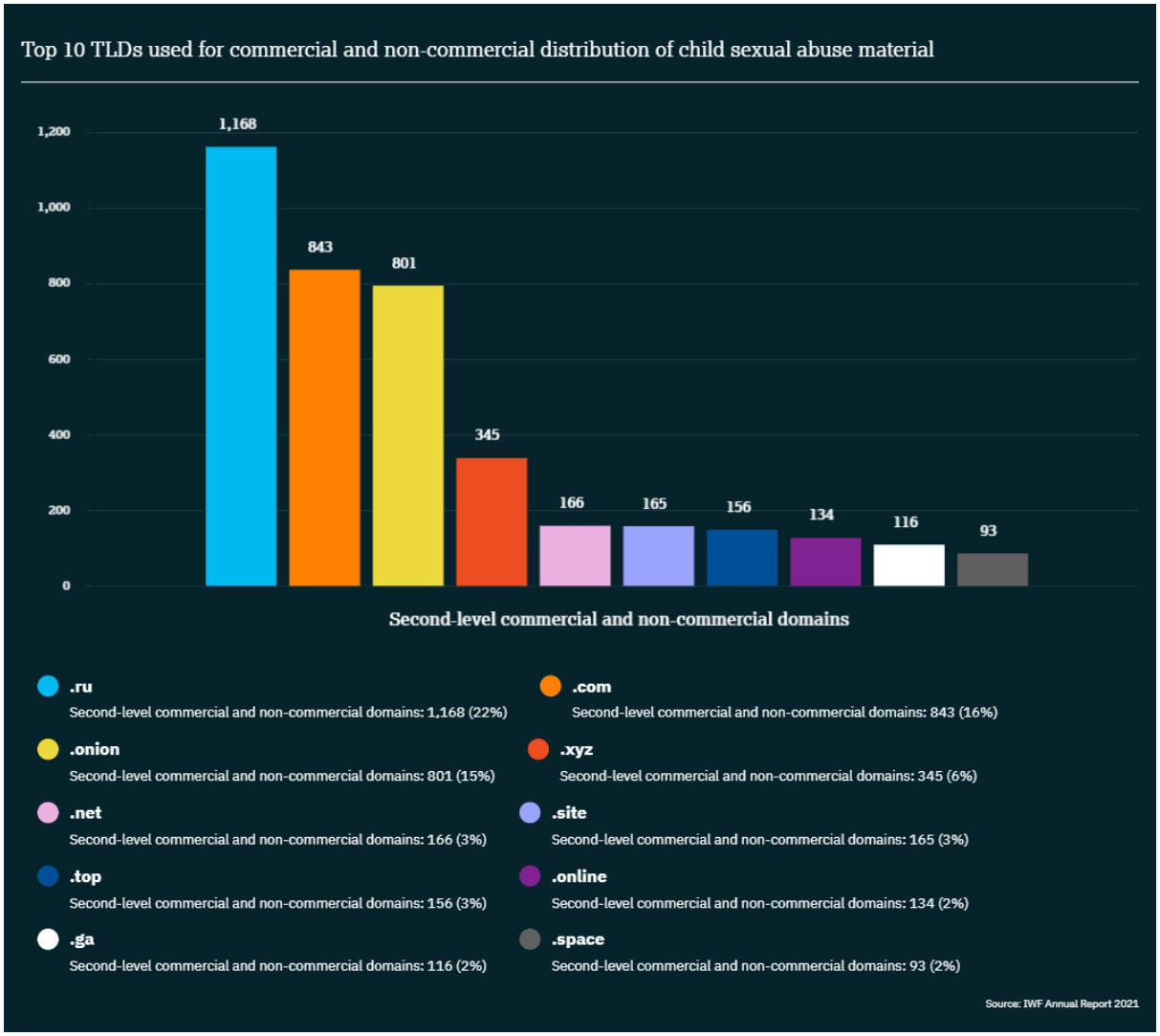
The charts show:

- The abuse of TLDs by those creating and registering dedicated commercial second-level domains to financially exploit and distribute child sexual abuse material, and,
- The number of TLDs that are abused on a combined commercial and non-commercial basis.

What can we do about this?

By understanding more about how second-level TLDs are specifically registered and used for the commercial distribution of child sexual abuse material, we can make them a point of focus for our work. We continue to research new ways to locate and remove these sites and disrupt the registration of new sites for this purpose.


Top 10 TLDs used for commercial distribution of child sexual abuse material
1,200
1,000
800
600
400
200
0
1,114
663
264
224
161
125
124
111
82
81
Second-level commercial domains
.ru
Second-level commercial domains: 1,114 (30%)
.onion
Second-level commercial domains: 663 (18%)
.xyz
Second-level commercial domains: 264 (7%)
.com
Second-level commercial domains: 224 (6%)
.site
Second-level commercial domains: 161 (4%)
.online
Second-level commercial domains: 125 (3%)
.top
Second-level commercial domains: 124 (3%)
.ga
Second-level commercial domains: 111 (3%)
.space
Second-level commercial domains: 82 (2%)
.uno
Second-level commercial domains: 81 (2%)
Source: IWF Annual Report 2021

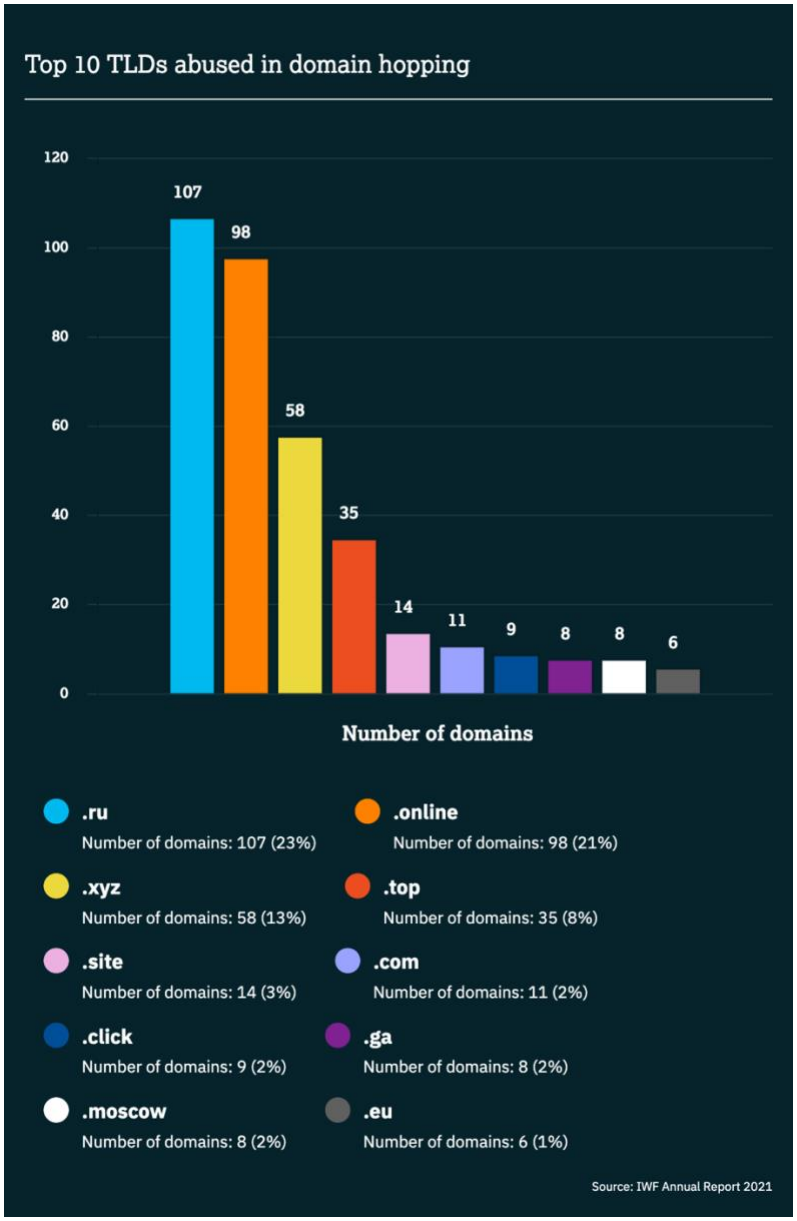

Top 10 TLDs used for commercial and non-commercial distribution of child sexual abuse material
1,200
1,000
800
600
400
200
0
1,168
843
801
345
166
165
156
134
116
93
Second-level commercial and non-commercial domains
.ru
Second-level commercial and non-commercial domains: 1,168 (22%)
.com
Second-level commercial and non-commercial domains: 843 (16%)
.onion
Second-level commercial and non-commercial domains: 801 (15%)
.xyz
Second-level commercial and non-commercial domains: 345 (6%)
.net
Second-level commercial and non-commercial domains: 166 (3%)
.site
Second-level commercial and non-commercial domains: 165 (3%)
.top
Second-level commercial and non-commercial domains: 156 (3%)
.online
Second-level commercial and non-commercial domains: 134 (2%)
.ga
Second-level commercial and non-commercial domains: 116 (2%)
.space
Second-level commercial and non-commercial domains: 93 (2%)
Source: IWF Annual Report 2021

Trends & Data > Top level domain hopping

What is Top-level domain hopping?

“Top-level domain hopping” is when a site (e.g. ‘badsite.ru’) keeps its second-level domain name (‘badsite’) but changes its top-level domain (‘.ru’), creating a whole new website with different hosting details but retaining its ‘name brand’. So from ‘badsite.ru’, the additional sites ‘badsite.ga’, ‘badsite.ml’ or ‘badsite.tk’ could be created. This allows instances of a website to persist online after the original has been taken down while keeping the website recognisable and easy to find.

- **219 dedicated commercial second-level domains were identified to have hopped domain at least once in 2021.**
- **A total of 63 unique TLDs were identified as being abused in domain hopping in 2021.**



- **202 second-level domains were found to have hopped once;**
- **13 hopped twice;**
- **two hopped three times;**
- **two hopped four times in a bid to remain online and active in the 12-month monitoring period.**

We first work with partners to ensure that the site is removed from the internet. Every subsequent hop, however, then requires a new action by our analysts to re-enforce the previous take down(s) by actioning the site again on the new TLD.

- **22 countries were identified as hosting domain hopping sites.**

When tracking hosting country, we noted that some sites often changed TLD but remained hosted in the original host country; other sites showed a preference to change hosting country after each TLD domain change, sometimes returning to the originally identified hosting country after a period of hosting elsewhere under a different TLD.

What can we do about this?

Domains are allocated and managed by internet registries and registrars. Our ongoing work in this area will enable us to identify domains exploiting the legitimate TLD marketplace. We continue to work with Members to not only identify and remove criminal sites but offer new preventative measures to guard against domains hopping to unsuspecting TLDs. We hope to involve more registrars and registries in the fight against this exploitative practice in 2022.

Trends & data > Site types

As in previous years, image hosts continue to be frequently abused by offenders distributing child sexual abuse imagery. These sites provide “storage” for images which either appear on dedicated websites or are shared within forums. These forums and commercial websites can display many thousands of abusive images. When 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.

In 2021, we saw a significant increase in the number of image stores being used to share child sexual abuse imagery, moving into our Top 3 for the first time. These sites are similar to image hosts but designed to index and store related images in vast quantities. They are also not as easily accessible to the public as an image host site.

Site type	Number of records	% of total number
Image host	184732	73%
Cyberlocker	24913	10%
Image Store	14621	6%
Forum	10710	4%
Banner	8086	3%
Website	2746	1%
Video channel	2431	1%
Social network	1104	under 1%
Search	948	under 1%
Blog	614	under 1%

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.

Paid for vs free hosting services

- **241,500 URLs (96%) were hosted on a free-to-use service where no payment was required to create an account or upload the content.**

In the remaining 4% 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.

Trends & Data > Geographical hosting

Where are webpages being hosted?

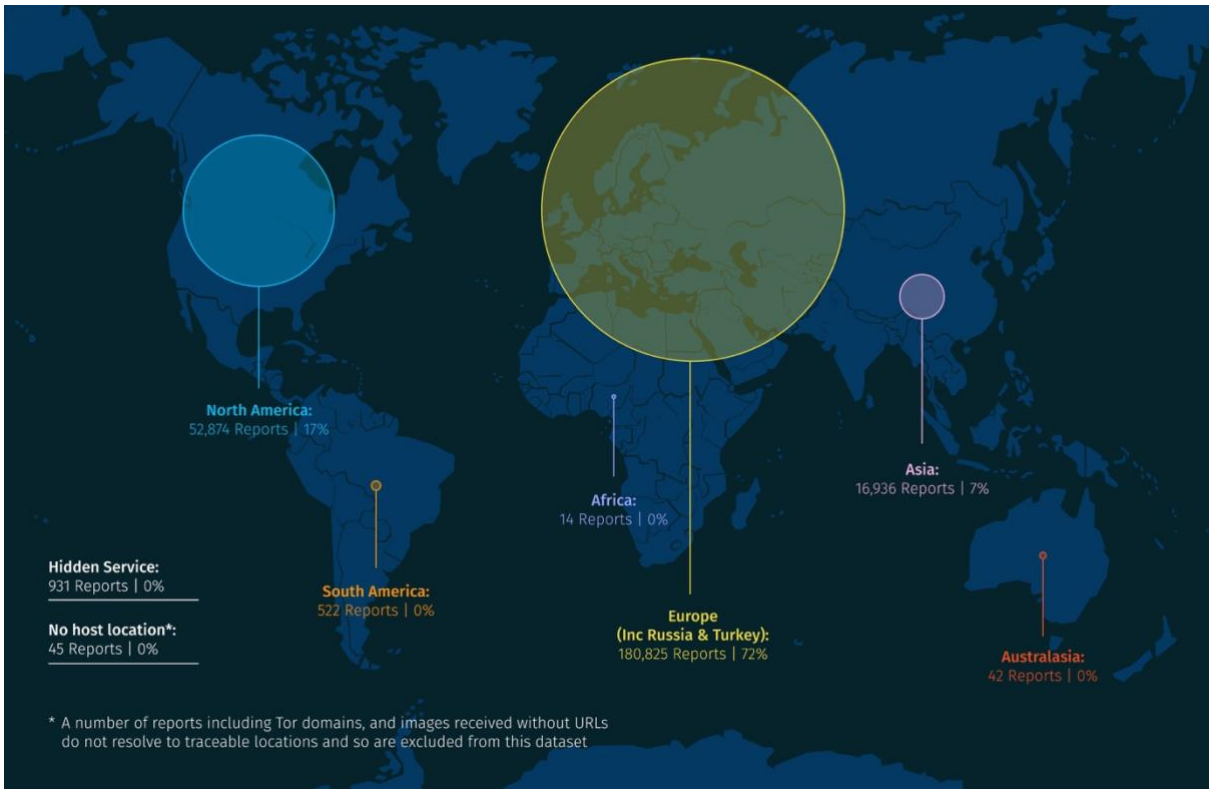
Find out about the UK hosting situation here.

When we've assessed that an image or video fails UK law, our aim is to get it removed from the internet as fast as possible.

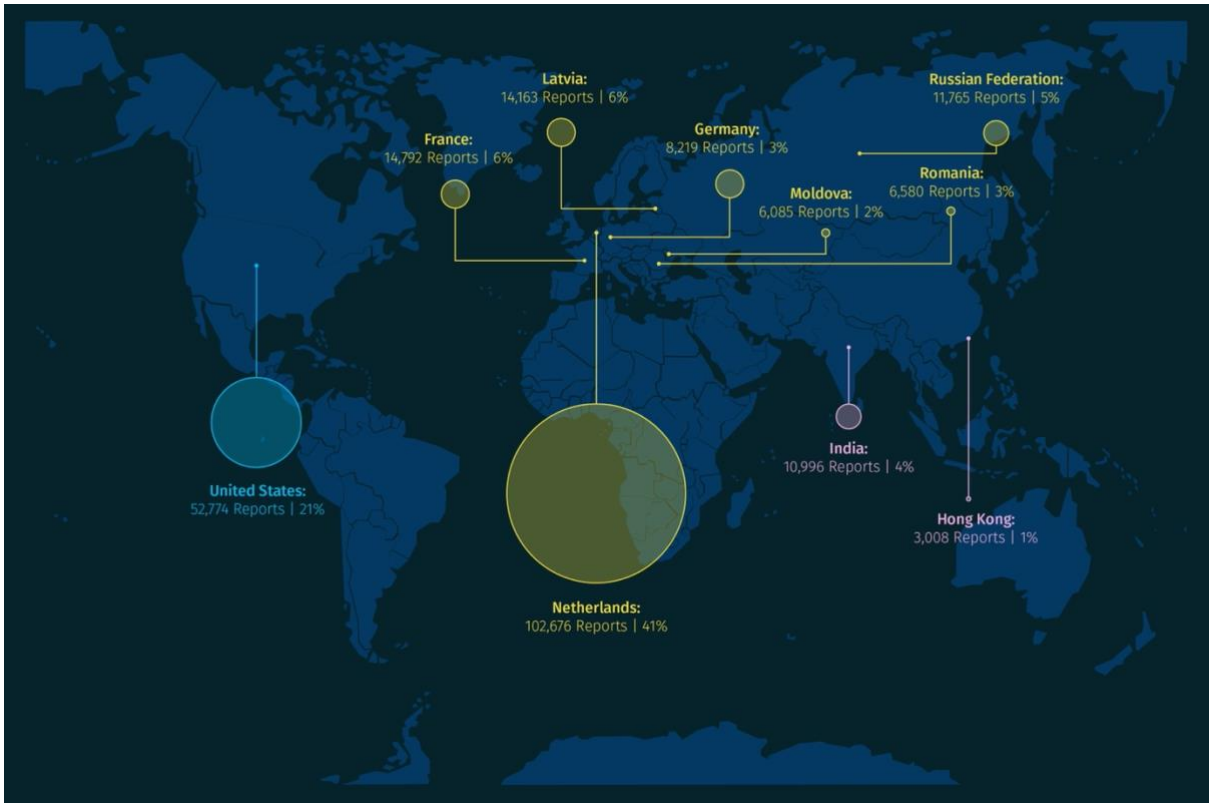
To do this, we perform a trace on the content to identify the physical server that the content is hosted on. This tells us which partners in which country we need to work with. When the content is removed from the physical server – its source – then we can be sure that the image has been removed from any websites or forums, or image boards etc, that could be linking to it.

"I would also like to share with you that pretty much all of the reports that you have contributed with so far has played vital roles in a number of investigations as well as a number of convictions relating to CSAM and CSE. It has played a key role in getting search warrants approved in many of the cases. A number of these search warrants and investigations has also led to the discovery of more aggravated crimes against children including hands on sexual offences. We are very thankful for your support in these cases". - **Swedish Police Authority**

Number of reports by continent



Number of reports by country



In 2021 we found a smaller proportion of child sexual abuse URLs being hosted in the Netherlands than in previous recent years (41% or 102,676 URLs vs 77% or 117, 544 URLs in 2020).

At the same time, a higher proportion was traced to the United States (21% or 52,774 URLs vs 5% or 8,257 URLs in 2020). It's important to note, however, the numbers of individual reports, and not just the proportions.

What can we do about removing this content?

We are committed to playing our part globally in the removal of content.

We constantly innovate to achieve this. We've set up 49 Reporting Portals around the world as part of our work in partnership with the Global Fund to End Violence Against Children. This has enabled us to develop vital links with other NGOs, governments and police services globally to remove this content.

In the EU we work closely with Europol and Interpol and the Lanzarote Committee of the Council of Europe. Europol have produced a number of threat assessments which have referenced many similar trends we have identified including a rise in self-generated content.

As a key organisation within the INHOPE network (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. IWF Reporting Portals are included under the INHOPE umbrella.

Additionally, we "chase up" our partners if this criminal imagery is not removed quickly.

View trends and data for the UK.

Trends & Data > Commercial content

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 252,194 webpages we confirmed as containing child sexual abuse imagery in 2021, 28,390 (11%) were commercial in nature. This is an increase on 2020, when we took action against 12,899 (8%) commercial webpages.

What can we do about it?

We monitor and research any new trends we have observed. Sharing this intelligence with our sister hotlines and law enforcement agencies means that websites can be removed and distributors can be investigated.

Any payment information displayed on these commercial websites is captured and shared with our partners in the financial industry. This helps to prevent misuse of their services and disrupt further distribution of the criminal imagery.

Trends & Data > Dark web reports

What are 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 using normal methods.

- **In 2021 we identified 931 new hidden services, up from 734 in 2020. This is an increase of 27%.**

What can we do about this?

We work with the National Crime Agency (NCA) Child Exploitation and Online Protection (CEOP) Command to share 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.

Trends & Data > Commercial dark web reports

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

Of the 931 newly-identified hidden services distributing child sexual abuse imagery in 2021, 661 were assessed as being commercial. Due to the anonymous nature of hidden services, these commercial websites only accept payment in virtual currencies.

What can we do about this?

Our Virtual Currency Alerts help our Members in the virtual payments sector to identify payments which are associated with child sexual abuse imagery. We continue to monitor trends in these payments and share this intelligence with our partners.

Trends & Data > Commercial disguised websites

What are commercial 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 concealing the distribution of criminal imagery has increased in 2021.

- **In 2021, we uncovered 26,272 websites using a "digital pathway" to hide child sexual abuse imagery. This is 115 times every working day.**
- **It represents an increase of 541% on the 4,100 disguised websites identified in 2020**

The huge increase in these types of sites is due to a new trend. In 2021, our analysts spotted some image host sites requiring a 'digital pathway' for the first time - meaning a particular route had to be taken to access a single image of child sexual abuse. These images would have appeared as blank webpages without following the necessary pathway. By identifying this new trend, we were able to uncover and take action on thousands of concealed images in a day.

Disguised websites have also continued to exploit 'top-level domain hopping' to avoid detection and remain online.

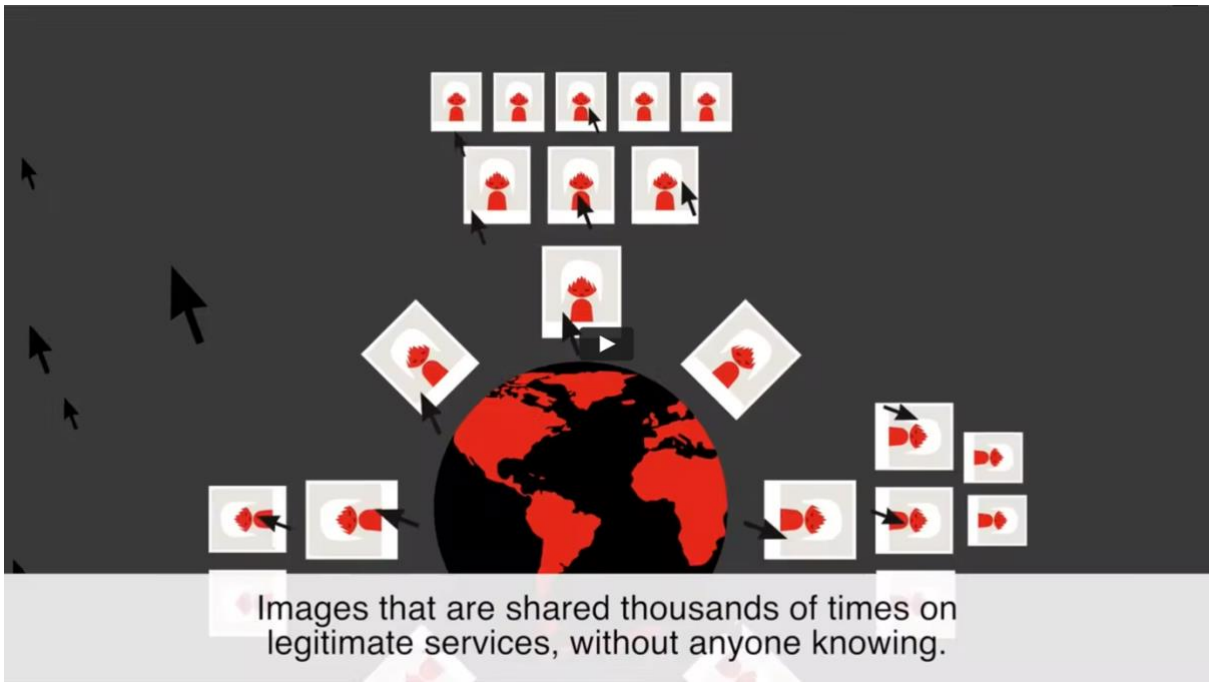
What can we do about this?

We actively monitor the techniques used by these websites in order to uncover the criminal material in order to get it removed. We also share intelligence with our partners to enable them to do the same.

Trends & Data > Hash metadata analysis

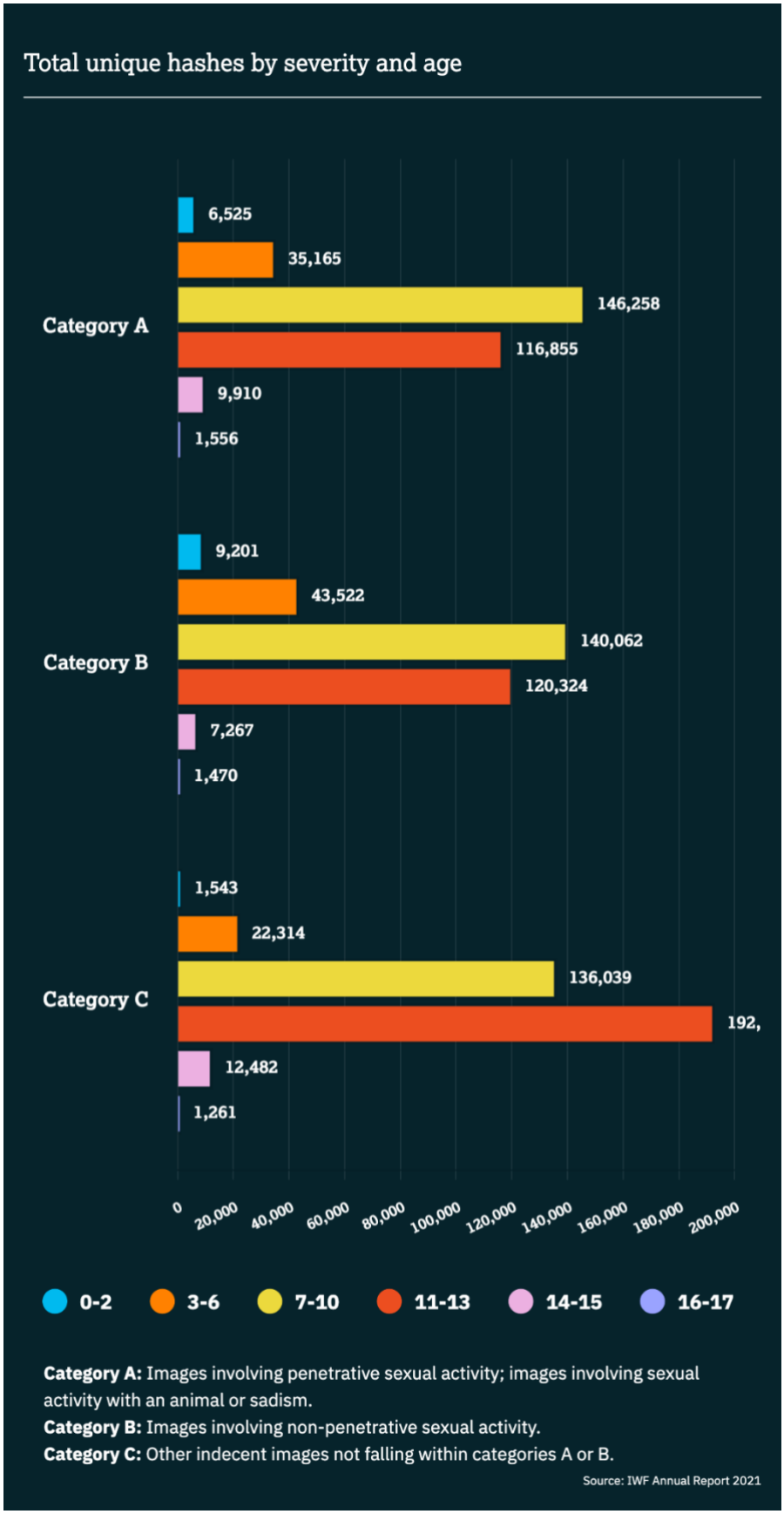
What is a hash?

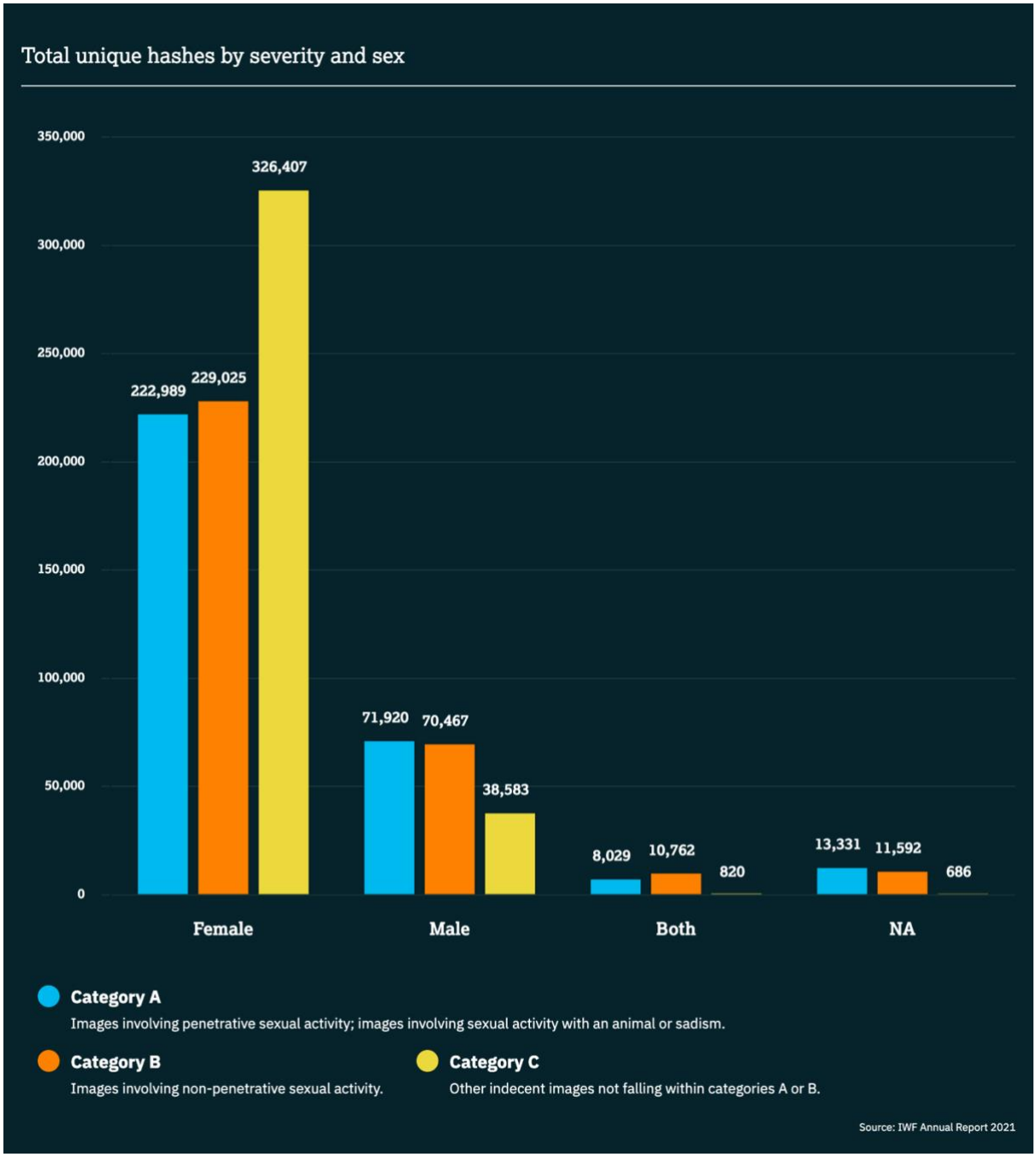
A hash is a unique digital fingerprint, or label that identifies a picture of confirmed child sexual abuse. Our hashes are created in various formats (think of them like different languages) including PhotoDNA, SHA1, SHA256 and MD5.



By using our Hash List, tech companies can stop criminals from uploading, downloading, viewing, sharing or hosting known images and videos showing child sexual abuse.

- **By the end of 2021, we had created 1,004,611 unique hashes to share with technology companies.**


Total unique hashes by severity and age
Category A
6,525
35,165
146,258
116,855
9,910
1,556
Category B
9,201
43,522
140,062
120,324
7,267
1,470
Category C
1,543
22,314
136,039
192,
12,482
1,261
0
20,000
40,000
60,000
80,000
100,000
120,000
140,000
160,000
180,000
200,000
0-2
3-6
7-10
11-13
14-15
16-17
Category A: Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.
Category B: Images involving non-penetrative sexual activity.
Category C: Other indecent images not falling within categories A or B.
Source: IWF Annual Report 2021


Total unique hashes by severity and sex
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
326,407
222,989
229,025
71,920
70,467
38,583
8,029
10,762
820
13,331
11,592
686
Female
Male
Both
NA
Category A
Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.
Category B
Images involving non-penetrative sexual activity.
Category C
Other indecent images not falling within categories A or B.
Source: IWF Annual Report 2021

Trends & Data > Hash meta data analysis > IntelliGrade hashes metadata analysis

What is IntelliGrade?

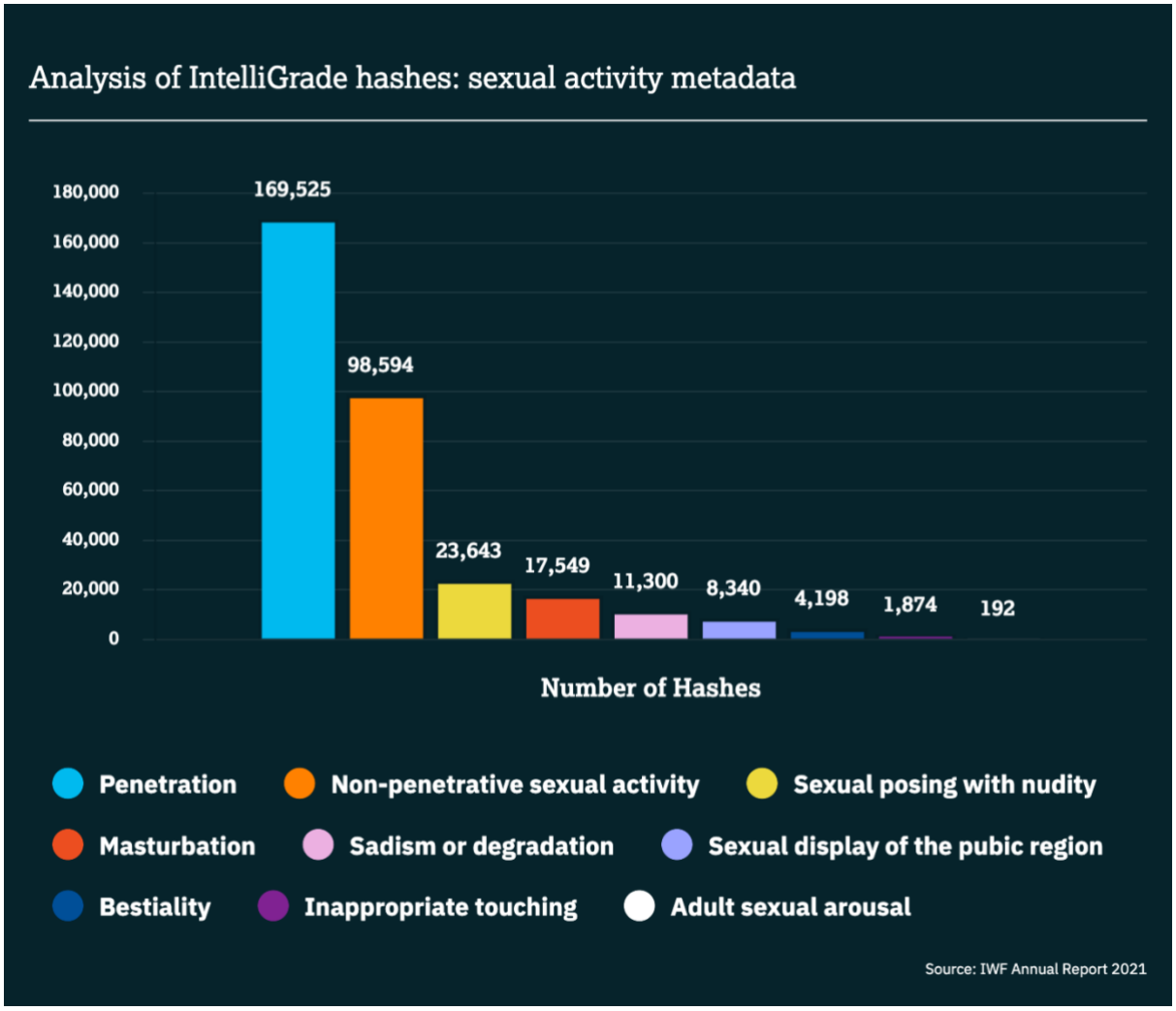
In 2021 we launched IntelliGrade. IntelliGrade is a powerful tool that enables our analysts to accurately grade child sexual abuse images and videos, while automatically generating unique hashes (digital fingerprints) which are used to identify and eliminate these images wherever they appear.

What makes IntelliGrade different from other technology, is that it allows us to enrich these hashes with **additional contextual metadata**.

A key benefit of this enrichment process is that hashes generated by IntelliGrade are compatible with child sexual abuse laws and classifications in the UK, US, Canada, Australia, New Zealand and the Interpol Baseline standard.

This means we can provide a dataset of hashes of child sexual abuse imagery which is compatible with multiple legal jurisdictions around the world. And just like the hashes that we've been creating since 2016, the IntelliGrade hashes are also created in various formats including PhotoDNA, SHA1, SHA256 and MD5.

- **At the end of 2021, the total number of unique IntelliGrade hashes was 335,215.**


Analysis of IntelliGrade hashes: sexual activity metadata
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
169,525
98,594
23,643
17,549
11,300
8,340
4,198
1,874
192
Number of Hashes
Penetration
Non-penetrative sexual activity
Sexual posing with nudity
Masturbation
Sadism or degradation
Sexual display of the pubic region
Bestiality
Inappropriate touching
Adult sexual arousal
Source: IWF Annual Report 2021

Trends & Data > Hash meta data analysis > IWF Taskforce

In 2021 IWF's new Taskforce started work. It's a team of highly skilled Image Assessors trained to the same high standards as our analysts. They are assessing and hashing (creating unique digital fingerprints) two million Category A and B child sexual abuse images. We are able to do this work thanks to a grant from Thorn.

These images come from the UK Government's Child Abuse Image Database (CAID). Once we've assessed and hashed them, we're able to share them back with UK law enforcement, and also with technology companies and other hotlines to prevent the distribution and upload of this material.

What makes our work unique, is that our Taskforce uses IntelliGrade to do their work. IntelliGrade allows us to enrich these hashes with **additional contextual metadata**. This offers us new ways in which we can support the global effort to eliminate online child sexual abuse content.

- **In 2021 the IWF Taskforce assessed 335,215 unique images of child sexual abuse. Each one was hashed and enriched with relevant metadata.**

Our Taskforce comprises six Image Assessors and one Quality Assurance Officer. They are restricted to working just four hours a day with mandatory breaks each hour due to the intensive nature of the work.

Welfare is our top priority and you can read more about how we look after our people here.

You can read about a day in the life of an image assessor on our website to learn more about the incredible team that does this work, and how they remain resilient and supportive of each other.

What our Image Assessors say:

"It's rewarding to be working as part of a team of people from varied backgrounds to help eliminate child sexual abuse material from the internet. Knowing that what you have achieved during the day will go towards preventing children being victimised over and over again is very satisfying."

"Every time I click my mouse, I know I'm making a difference. You can't say that for many other jobs."

"As someone now working as an Image Assessor, I found that the number of images of abuse are far beyond what I ever imagined, and I feel the work we do is crucial in giving children back their childhoods. This has given me a sense of pride that I am part of such an amazing team of people with the same goal of making the internet a safer place."

Trends & Data > UK Data > UK hosted child sexual abuse imagery

UK hosting volume

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 2021 this figure was just 0.15%.**
- **In 2021, 381 URLs displaying child sexual abuse imagery were hosted in the UK, an increase of 112% from 180 URLs in 2020.**

In 31 cases the criminal content had already been removed by the time we received authorisation from the police to instigate its removal or it had moved hosting country already, leaving us with 350 URLs to take action on.

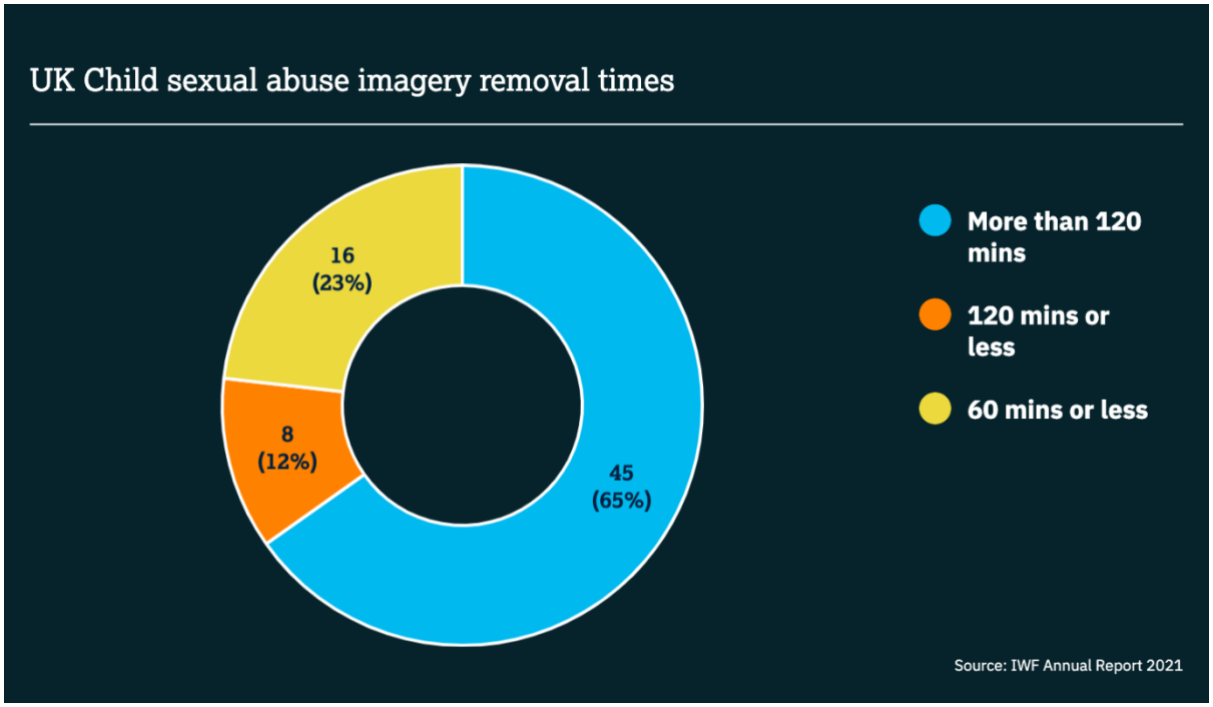
69 takedown notices relating to the 350 URLs were sent to UK hosting companies (we might send one notice for several webpages).

UK child sexual abuse content removal in minutes

We have to act quickly. The longer an image stays live, the more opportunity there is for offenders to view and share it, and more harm is caused to the victims.

In partnership with the online industry, we push to secure the rapid removal of this content. The 'takedown' clock ticks from the moment we issue a takedown notice to the hosting company, to the time the content is removed.

Fastest removal: 3 minutes



- **25 companies' services in the UK were abused to host child sexual abuse images or videos during 2021.**

We issue takedown notices to UK companies, whether they're in IWF membership or not.

- **24 companies who were abused were not IWF Members.**
- **1 company was an IWF Member.**

What can we do about this?

We use a minimum of 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.

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.

Trends & Data > UK Data > Non-photographic reports

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

We received 1,689 reports of suspected non-photographic child sexual abuse imagery from external sources (a reduction of 436% from 2020). However, after our assessment, none of these were confirmed as UK-hosted content.

In 2021 we enabled people to have more freedom to tell us what they were reporting to us. This has enabled us to more quickly triage the reports that come into our hotline. By doing this, we have been able to increase the amount of time that our analysts can spend proactively searching for child sexual abuse imagery, and decrease the time they were spending on off-remit reports. This has contributed to reduction in the number of suspected non-photographic child sexual abuse reports we have received.

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. If we find this content hosted in the UK, we issue a notice to the hosting provider who removes it. This hasn't happened in the UK since 2016.

However, this type of content does exist online and if UK-hosted, would fail UK laws.

Technology companies want the flexibility of being able to block and filter it 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.

Technology and services > Technology amplifying impact

“We use technology to take the shocking child sexual abuse images and videos that our Hotline Analysts assess and create detailed, trusted datasets that are used by our Members to detect and remove that content across the internet,” Dan Sexton, Chief Technology Officer.

Technology has enormous potential to enhance and massively amplify the impact the IWF has in the fight to eliminate child sexual abuse material online.

The tech team have developed state of the art tools to support the Hotline’s work, and are constantly looking for ways to improve efficiency, accuracy, and impact, while also generating valuable high-quality data for our services, like our hash and URL lists.

We use technology to take the shocking child sexual abuse images and videos that our Hotline Analysts assess and create detailed, trusted datasets that are used by our members to detect and remove that content across the internet.

With the scale of the problem growing exponentially, using technology to automate, augment and expand our efforts to eliminate child sexual abuse material online is becoming increasingly important.

The internet is constantly expanding and changing, and it is crucial that we continually improve and innovate, enabling the IWF’s critically important work to scale and have a global impact. The tech team is dedicated to leveraging cutting-edge technology to develop new ways of supporting our Hotline Analysts and industry partners to detect and remove child sexual abuse material from the internet.

You can find out about some of our key services such as our URL List, Hash List, Non-Photographic imagery list and Report Remove.


01:22

Technology and services > IWF reThink Chatbot

We have built an interactive chatbot in collaboration with The Lucy Faithfull Foundation.

This project is funded by the End Violence Fund, as part of their campaign to keep children safe online by investing in solutions to tackle child online sexual exploitation and abuse.

With the help of practitioners and psychologists from The Lucy Faithfull Foundation, we have designed a conversation flow to guide an internet user exhibiting offending behaviours to services offered by the Stop It Now! helpline. The chatbot can also signpost users to self-harm and mental health agencies which could help them address other issues as well.

With the Lucy Faithfull Foundation, we conducted focus groups with offenders who have undergone treatment and counselling.

When the chatbot is deployed it will enhance efforts to curb the demand for criminal images on the internet.

We want people to rethink their inappropriate online behaviours, reduce the demand for child sexual abuse material, and stop online child sexual abuse from taking place in the first place.

The chatbot will be tested as a pilot in 2022 while an independent evaluation by academics and experts in the field from the University of Tasmania takes place.

"If [the chatbot] existed 12 or18 months ago, I 100% would not be in the position I am now. If this goes live it will definitely save some people being in the same position as me." A focus group participant undergoing treatment with Lucy Faithfull Foundation.

Technology and services > AI & Machine Learning

Artificial intelligence and machine learning have gone from science fiction theory to a commonplace feature in the technology we use in our day to day lives.

Machine learning systems process large data sets to create models that can be used to assess data and make decisions with much greater speed than a human ever could. At IWF we have been researching the effectiveness of AI classifiers to analyse images and identify suspected child sexual abuse material.

While AI classifiers do not yet have the level of accuracy required to perform automated image assessments to the standard that we need, they have huge potential to support triage functions, detect suspected new and unknown content, and assist with victim identification.

How can we use AI to support our work?

Our software team has been prototyping AI models which can be used to identify known victims of child sexual abuse using powerful facial recognition technology, ensuring that images of those victims can be correctly flagged to us and removed from the internet.

In addition to working to integrate machine learning technology into our own image assessment and web crawling tools, we are looking into how we can support technology partners to train and assess AI models to enable them to more accurately detect new content containing child sexual abuse.

Human assessment is, and will always be, critical to maintaining the IWF's high level of accuracy and trusted status. But there is huge potential for AI and machine learning to support the work of our expert analysts, uncover new information about the images we process, and help our partners to improve the accuracy and effectiveness of technology used to detect new child sexual abuse content.

Technology and services > Intelligent Crawler

We created an intelligent web crawler. It's loaded with over a million quality assured hashes of known child sexual abuse material, each one having gone through a human assessment by our expert analysts. The web crawler enables automated detection at scale with an extremely high level of accuracy.

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.

In 2021, we've been using our web crawler to provide an additional service to our Members in the domain registry sector. Now we can automatically scan new sites for known child sexual abuse images after they have been registered and inform our Members if anything is detected.

In 2021 it crawled almost 14 million webpages, and over 66 million images. By comparing each image our crawler finds to the hashes of known child sexual abuse material, it means we can find duplicate child sexual abuse images hidden across the internet.

"Computer vision and machine learning in general are useful tools, and we seek to leverage them where possible to reduce the amount of manual effort our analysts need to put in to prioritise and classify images. Technology is ever-improving but currently lacks the level of granularity and precision we need for our work. At the IWF the final decision is always based on a human assessment with computer vision being used as a complementary tool."

Chris Wilson, IWF Head of Software

Technology and services > IntelliGrade

IntelliGrade is a powerful new tool that enables our analysts to accurately grade child sexual abuse images and videos, while automatically generating unique hashes (digital fingerprints) which are used to identify and eliminate these images wherever they appear.

What makes IntelliGrade different from other technology, is that it allows us to enrich these hashes with additional contextual metadata.

A key benefit of this enrichment process is that hashes generated by IntelliGrade are compatible with child sexual abuse laws and classifications in the UK, US, Canada, Australia, New Zealand, and the Interpol Baseline standard.

This means we can provide a dataset of hashes of child sexual abuse imagery which is compatible with multiple legal jurisdictions around the world.

This gives reassurance to some of the world's biggest – and smallest – tech companies so that they can better protect their customers, and better protect children whose abuse images are shared online.

And it gives peace of mind to those survivors of child sexual abuse that we can now fight back, together.

“Harmonising child sexual abuse laws around the world would be a major step in enabling all of us to better fight back against those who share child sexual abuse imagery online. But we can’t wait for a day that might never happen. IntelliGrade does that for us. At IWF, we’re enriching the hashes (digital fingerprints) of millions of child sexual abuse images to create one, harmonised, world-compatible dataset.”

Chris Hughes, IWF Hotline Director

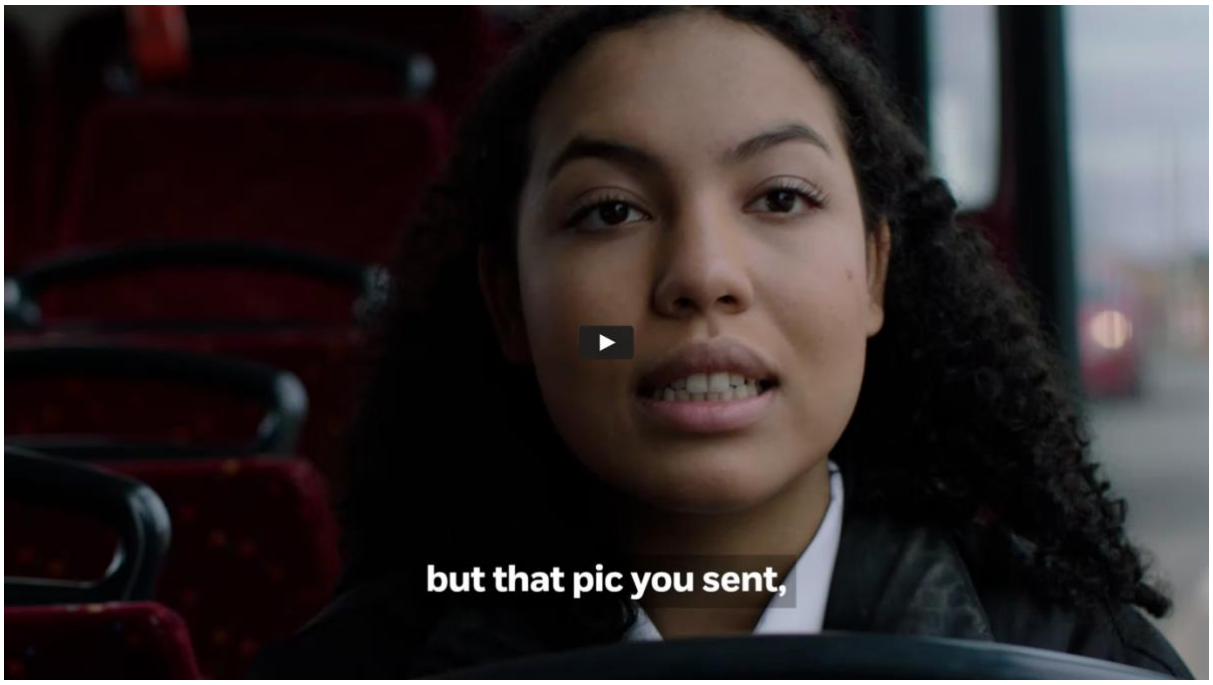
Technology and services > Report Remove

In partnership with

To support young people to remove sexual images of themselves online, together with the NSPCC we developed Report Remove in partnership with age verification app, Yoti.

In 2021, the IWF processed 110 reports which came to us from Report Remove.

It was launched in June after several years of development.



By teaming up with the NSPCC's Childline service, it ensures that the young person is safeguarded throughout the process.

Meta has been a long-term partner of IWF to help tackle child sexual abuse imagery online. Additionally, Meta collaborated with IWF to support the technical development and piloting of Report Remove.

Here's how it works:

1. Young people aged 13+ are first directed to Yoti to verify their age using ID.
2. They are prompted to create a Childline account, which allows them to be safeguarded and supported throughout the process.
3. Young people are then taken to a dedicated IWF portal where they can securely upload images, videos or URLs (website addresses).

4. IWF analysts assess the reported content and take action if it meets the threshold of illegality*. The content is given a unique digital fingerprint (a hash) which is then shared with internet companies to help prevent the imagery from being uploaded or redistributed online.
5. The outcome will be conveyed to Childline who will then contact the young person via their Childline account to keep them updated and offer further support.

This solution provides a child-centred approach to image removal which can be done entirely online.

The young person does not need to tell anyone who they are (their ID is not linked to their report), they can make the report at anytime, and further information and support is always available from the Childline website.

Each hash is tagged as originating from 'Report Remove'. This ensures that law enforcement bodies are aware that this is a self-referred image, to reduce the risk of children receiving a visit from police unnecessarily. As the Report Remove tool develops, we hope it may be possible to gain further information on self-generated images to see how this process and the laws surrounding it could be improved to better protect children.

Technology and services > IWF URL List

What is the IWF URL list?

We provide a list of webpages containing 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 repeated victimisation of the children in the images. We update the list twice a day, removing and adding URLs.

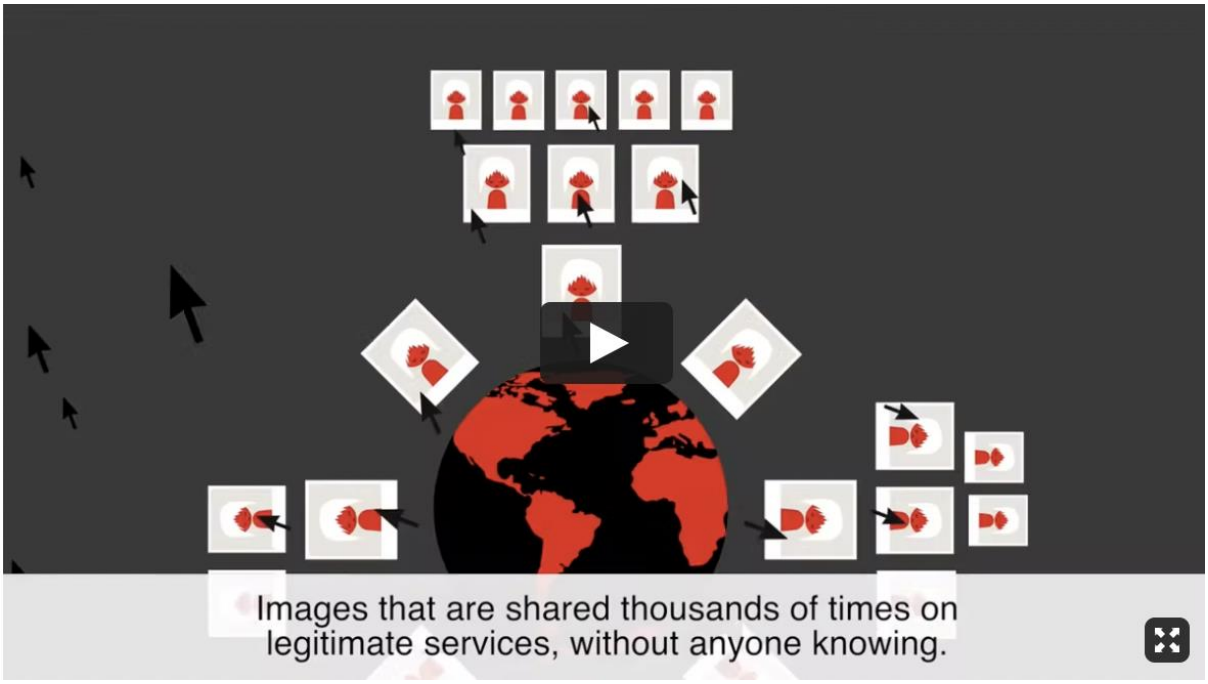
During 2021:

- **The list was sent across all seven continents.**
- **A total of 203,234 unique URLs were included on the list (a 38% increase on 147,232 in 2020).**
- **On average, 1,001 new URLs were added each day (591 in 2020).**
- **The list contained an average of 5,526 URLs per day (5,747 in 2020).**

Why is the URL List important?

When the URL List is deployed by a technology company, it prevents people from stumbling across known – and available – 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.

Technology and services > Hash List



What is the 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.

Why is this Hash List important?

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.

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.

You can read the analysis of our hash data here.

Technology and services > Non-Photographic Imagery List

What is our NPI List?

Our Non-Photographic Image (NPI) URL List is comparable to our standard URL List but features webpages (URLs) showing images and videos of Non-Photographic child sexual abuse. These could include cartoons, drawings, computer-generated imagery (CGI) and other Non-Photographic representations of child sexual abuse.

The URLs provided in the IWF NPI List are those deemed at the time of assessment by our analysts to breach UK legislation.

Whilst Non-Photographic child sexual abuse imagery is criminal only within the UK, some of our Members chose to use this list voluntarily to ensure that this material does not appear on their platforms and services.

- **In 2021, 234 unique URLs of non-photographic child sexual abuse imagery were included on the list. 13 IWF Members subscribe to this service.**

New content is added to the list daily and our analysts manually assess every webpage on the list.

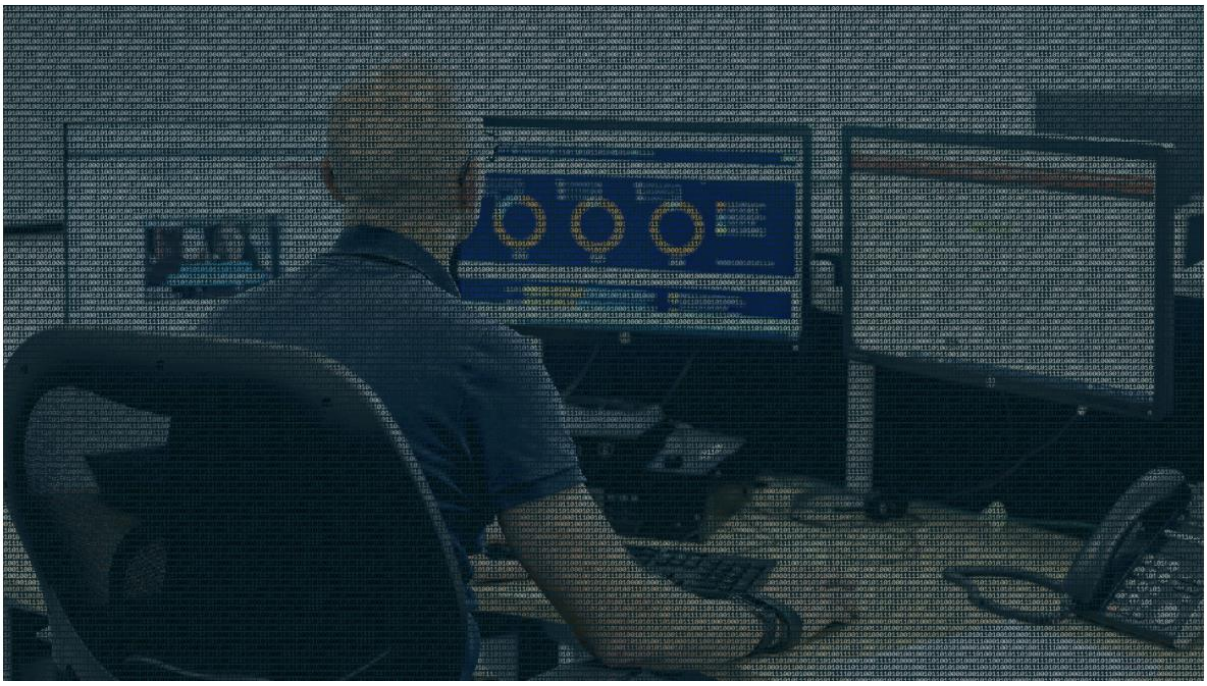
Working with others > Our Members

In 2021 we were funded by more than 170 global companies, and the European Union.

A wide range of industry sectors are attracted to work with us. During the year we welcomed 27 new Members from nine countries, including our first industry presence in Finland and the Philippines.

Whilst IWF membership is highly relevant to the more traditional tech industry sectors of hosting, domain registries and telecommunications companies, the benefits and services we offer are now having broader appeal among hoteliers and hospitality, digital forensics, VPNs, banking and alternative network providers.

Working with others > Corporate, in-kind support and grants



We would like to thank all those who have supported our work in 2021.

Support comes in many ways; some of our Members provide additional funding or in-kind support over and above their membership fees; we have corporate supporters who provide us with in-kind support as well as fundraise for our charity, and we receive grants and donations from organisations to carry out specific pieces of work which meet our charitable objectives.

You can read more about where our funding comes from in our Trustees' Report which is produced annually.

Working with others > .XYZ: taking a zero-tolerance approach

When the IWF warned US-based domain registry company XYZ that sites registered with their top level domains (TLDs) were being abused as locations for sharing child sexual abuse material (CSAM), the company was swift to take action.

Between 11 October and 7 November, the IWF took action against 12,233 reports which were related to 75 domains registered with XYZ. XYZ's response was emphatic and, within hours of being notified of the issues, they had suspended the offending domains.

Jocelyn Hanc, Vice President of Operations at XYZ, said "having a fast response to suspending domains being abused to host "evil and heinous" child sexual abuse content is a matter of principle for the company.

"We have a zero-tolerance policy for CSAM because it is the right thing to do. The creation of CSAM content is an evil and heinous act, and we will do our part to stop its consumption. XYZ's entire Anti-Abuse program is based on the same philosophy – that it is the right thing to do."

Ms Hanc said the company "heavily invests" in its anti-abuse processes, but warned that "bad actors" can still "easily re-connect with any other top-level domain in a matter of minutes" even after having their .xyz domain suspended.

She said: "We report the usage to our registrar partners so they can review and ban the customer account. Ultimately our actions cannot stop the bad actor from continuing to abuse on other platforms."

According to Ms Hanc, the XYZ Anti-Abuse Team operates the company's proprietary Anti-Abuse system daily to review and take action on confirmed user submitted reports, internal research, and data from cybersecurity partners. When they receive a report of child sexual abuse material, they escalate the report to the IWF for review.

The Anti-Abuse Team also receives notifications of child sexual abuse material from the IWF and takes action as necessary. Ms Hanc said these reports are treated as a priority. She said close cooperation between registries, registrars, and groups like the IWF is essential in stopping criminals "in their tracks".

She said: “We have a zero-tolerance policy for child sexual abuse imagery and materials. Our first thought is to act quickly to disconnect the content from the internet. That is what happens when XYZ suspends any domain for violations of our Anti-Abuse policies.

“That being said, shutting down the domain is the least effective method of stopping a criminal. The domain is merely the vessel used to orchestrate the crime and once it has been suspended, the criminal simply finds another vessel to facilitate the abuse. This is why XYZ strongly believes that the registry, registrar, and cybersecurity organizations should work together altruistically.

“The registry has no direct contact with the registrant, and can only suspend the domain and notify the registrar. If all parties act in harmony - the registry receiving information from experts in cybersecurity and notifying registrars of suspensions, we can help stop criminals in their tracks.”

Ms Hanc said most TLDs are unrestricted and do not require pre-qualifications for registration of a domain name.

“CSAM is hosted on a server, not on a domain,” she said. “The only entity that could easily monitor the files is a hosting provider. The bad actor can connect that content to any domain they control - and then change that connection to any other domain in a manner of minutes.

“The domain is just a convenient address or handle to give to others to access the IP. Content can even be accessed at an IP itself without a domain. This is why we report suspensions to the registrars, so they can be aware of their customer’s intentions.”

Ms Hanc said XYZ is “very public” about their stance on abusive use. She said she hopes this sends a message that abusers know they will not get far using a .xyz domain.

You can find out more about being an IWF Member on our website.

Working with others > Our Reporting Portals

We provide IWF Reporting Portals to countries which do not already have a way of reporting this online criminal content. Working with local governments, police, industry, funders and charities, we give people a place to report, linked directly to our analysts in the UK.

Today we have 49 of these Reporting Portals 50 including the UK - giving more than 2.6bn people a safe place to report – anonymously – suspected online pictures and videos of children being sexually abused. Six were launched in 2021 and the first – the Mauritius Portal – was launched in 2013.

Reporting Portals are customised webpages. When reports are confirmed as illegal by our expert analysts in our UK Hotline, we work to have the images and videos removed from the internet.

Setting up a reporting portal is a low-cost, fast and effective way to fight against child sexual abuse.

You can find out more about our Reporting Portals on our website.

Key facts from 2021

- Number of people globally with access to a portal: **2,597,000,000**
- Number of roundtables held: **5**: Kenya, Morocco, Tunisia, Argentina, Sri Lanka
- Number of portals launched in 2021: **6:** Kenya, Morocco, Guatemala, Tunisia, Argentina, and ICMEC-IWF Reporting Portal for countries that don't have a reporting mechanism yet.
- Languages featured: **17:** Arabic, English, French, Hindi, Indonesian, Kazakh, Lingala, Malaysian Bahasa, Mongolian, Nepali, Pashto, Portuguese, Spanish, Swahili, Ukrainian, Urdu, Wolof.
- Number of continents covered: **4:** Africa, Asia, Europe, South America.
- Number in INHOPE network: **49**
    - Akrotiri and Dhekelia
    - Angola
    - Anguilla
    - Argentina
    - Ascension Islands
    - Belize
    - Bermuda
    - British Virgin Islands

- Burundi
- Cayman Islands
- Comoros
- Cote d'Ivoire
- The Democratic Republic of Congo
- El Salvador
- Falkland Islands
- The Gambia
- Ghana
- Gibraltar
- Guatemala
- Haiti
- India
- Indonesia
- Kenya
- Liberia
- Madagascar
- Malawi
- Malaysia
- Mali
- Mauritius
- Mongolia
- Montserrat
- Morocco
- Mozambique
- Namibia
- Nepal
- Pakistan
- Pitcairn
- St Helena
- Senegal

- Sierra Leone
- Tanzania
- Tristan Da Cunha
- Tunisia
- Turks and Caicos
- Uganda
- Ukraine
- Zambia
- Zimbabwe
- ICMEC-IWF Reporting Portal (across countries)

Working with others > Our Learning Awareness Programme in Zambia and Uganda

We launched a campaign to help boost child welfare and internet safety in Uganda and Zambia.

Funded by the UK Home Office's Conflict, Stability and Security Fund and supported by Meta and MTN, the pilot campaign, **Help Children Be Children,** focused on raising awareness on online child sexual abuse and on the importance of reporting.

To create and deliver this campaign, we worked with our portal partners in Zambia, ZICTA, and Uganda, NITA, as well as with nationally-based organisations such as Sauti116 and Lifeline Childline Zambia.

The campaign comprised three main elements:

- An awareness and marketing campaign;
- A capacity-building component for law enforcement and policy-makers, and
- An online module developed to train helpline staff.

Working through Africa-based advertising agency TBWA, we created impactful visual designs and microsites for the portals: **www.stopit.ug** in Uganda and **www.stopit.ac.zm** in Zambia, leading to more than **45,000 microsite views** and a **rise in reports through the portals**.

Our partner, the International Centre for Missing and Exploited Children (ICMEC) delivered a roundtable and law enforcement training to more than **500 key stakeholders** discussing the issue of child sexual abuse and how to combat it.

Our partner, Child Helpline International (CHI) created an insightful online module delivered to helpline staff in both countries that **strengthened their efforts to prevent child abuse** and **enhanced their knowledge on the reporting tools** available to tackle this problem.

IWF Members MTN and Meta were key supporters of the campaign and their efforts have greatly contributed to its success.

Due to the success of the pilot, they are supporting a second phase launching in 2022.

Working with others > UK Safer Internet Centre

The UK Safer Internet Centre is a unique partnership of three world-leading charities – Childnet International, IWF and SWGfL. A bridge between Government, industry, law enforcement and society, we are the engine of the online protection landscape in the UK, dealing with both prevention and response.

We work together to identify threats and harms online and then create and deliver critical advice, resources, and interventions that help keep children and young people safe. All resources are available in our newly launched website.

We have four main functions:

1. **Hotline:** an anonymous and safe place for members of the public to report suspected child sexual abuse images and videos online, wherever they are found in the world.
2. **Helpline:** to support professionals working with children and young people on online safety issues.
3. **Platform:** for people to report harmful content online which is not related to child sexual abuse material.
4. **Awareness Centre:** to provide advice and support to children and young people, parents and carers, schools and the children's workforce and to coordinate Safer Internet Day across UK.

Here's a report on our achievements

Links and resources:

- The Professionals Online Safety Helpline (POSH) – To support professionals working with children and young people in the UK.
- Online Safety Training - Online safety training for staff, children and parents, delivered by experts from SWGfL both face-to-face or online.
- Project Evolve – Free digital education toolkit to prepare learners for the digital world.
- 360 Degree Safe – An online safety self-review tool for schools.
- STAR SEND Toolkit - Teaching toolkit to equip, enable and empower educators with the relevant knowledge to support young people with special educational needs and disability (SEND).

Safer Internet Day

We run UK Safer Internet Day (SID), an annual event to promote the safe and positive use of digital technology for children and young people. Our reach is unparalleled by any other organisation working in this space and over the years, Safer Internet Day has become a landmark event in the online safety calendar worldwide.

Safer Internet Day 2021 reached more young people than ever before, with 51% of UK children aged 8-17 hearing about the day, alongside 38% of UK parents and carers.

The educational resources created for the day were downloaded over 1.5 million times and the event had a media reach of 126 million people. 99% of teachers say Safer Internet Day plays a significant role in their school's online safety provision.

For SID in February 2021, we ran a virtual event with politicians where children from St. Patrick's College, Dungannon, were able to discuss their views on this year's theme: "An internet we can trust exploring reliability in the online world." The event was chaired by Dr. Lisa Cameron MP, a Vice Chair of the APPG on Social Media and included contributions from the Shadow Digital Minister, Chi Onwurah MP and Will Gardner, CEO of Childnet International. Over 30 MPs and Peers also supported Safer Internet Day by tweeting their support online.

The UKSIC also worked with young people to develop a Young People's Charter for Safer Internet Day 2021 on how government and online stakeholders can help create a more trustworthy internet.

Glossary

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: Images involving penetrative sexual activity; images involving sexual activity with an animal or sadism.

B: Images involving non-penetrative sexual activity.

C: Other indecent images not falling within categories A or B.

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.