

IWF response to the House of Lords Communications Committee Inquiry: The Internet: to regulate or not?

1. About the IWF:

- 1.1. The Internet Watch Foundation was founded in 1996 as a result of the Metropolitan Police notifying the Internet Service Providers Association (ISPA) that some newsgroup content being carried by Internet Service Providers (ISPs) were indecent images of children. The police believed that this may have constituted a publication offence under the Children Act (1978) of England and Wales, by the ISPs.
- 1.2. Following discussions with the then Department of Trade and Industry (DTI), the Home Office and the Metropolitan Police, some ISPs and the Safety Net Foundation (formed by the Dawe Charitable trust) an R3 Safety Net Agreement regarding rating, reporting and responsibility was created by ISPA, the London Internet Exchange (LINX) and the Safety Net Foundation. A key outcome of this agreement was the formation of the Internet Watch Foundation (IWF).
- 1.3. The IWF was established to fulfil an independent role in receiving, assessing and tracing public complaints about child sexual abuse content on the internet and to support the development of website rating systems.
- 1.4. Since our inception in 1996, we have operated a “hotline” function for the public to report potentially criminal content and we have been issuing “take-down notices” to UK ISPs in partnership with the Police so that they can have this content removed.
- 1.5. When the IWF formed, we had five funding members and our organisation has grown significantly over the past two decades. We now have 136 funding members, the most we have ever had, and employ 38 people with just over half of them analysing content we receive from public reports and proactive searching.
- 1.6. We receive 10-15% of our funding directly from the European Union and its Safer Internet Programme. We are one of the three charitable partners which make up the [UK Safer Internet Centre](#). Our EU funding equates to 50% of our analyst salaries and we are currently having to consider future arrangements for funding after our current funding arrangement ceases post Brexit.
- 1.7. We currently receive no financial support from UK Government.

2. Scale of the challenge:

- 2.1. When the IWF was formed in 1996, the UK was responsible for hosting 18% of the world's Child Sexual Abuse Material (CSAM). Our latest annual report figures (2017) show that hosting of this content in the UK remains under 1%. The success in reducing UK hosting of CSAM is as a direct result of our self-regulatory model and partnership approach with the internet industry, law enforcement and Government.
- 2.2. In the last three years we have seen a growth in content being hosted in Europe, particularly in the Netherlands. Three years ago (2014) 57% of the world's CSAM was hosted in North America and 41% in Europe. Today (2017), Europe hosts 65% of the world's CSAM and North America 32%.
- 2.2. In 2017, our analysts processed 132, 636 reports of suspected child sexual abuse. Of these, 80,318 (61%) were confirmed as CSAM. Of those reports, 50% came from the public and 50% were proactively sourced by our analysts. 43% of children appearing in these reports were between the ages of 11 and 15 and 86% were girls. We also found that the younger the victim, the higher the level of abuse they suffer with 63% of images of abuse for the age range 0-2 being classified as Category A (the highest level of abuse).

- 2.3 In partnership, with the independent think-tank Demos, the IWF in January this year [launched a report](#) which highlights the scale of the challenge with dealing with this content online. In 1990, the Home Office estimated there were just 7,000 child sexual abuse images, videos and tracings in circulation and today we know that police seizures regularly involve millions of illegal images being found on an offender's computer.
- 2.3 Estimates to assess the problem range widely, the number people arrested for "obscene publications" violations increased by 134% in 2014/15 to 7,324. In total 54,000 child sexual abuse offences (contact abuse and CSAI) were recorded in the year 2015/16 according to the Office of National Statistics.
- 2.4 [CEOP estimates that 50,000 individuals have viewed illegal CSAI online](#), although the [NSPCC places estimates much higher at 590,000](#), which means there is a wide variation in determining what the scale of the challenge is and it is difficult for us to predict just how much content there is online and how many offences can be identified.
- 2.5 There is no doubt that the internet has been a huge force for social good. We are better connected, better informed and more entertained than ever before, but with the evolution of new technology and the benefit that this brings, there are challenges to address with the internet ecosystem and particularly the sewerage that it creates.
- 2.6 One of the big problems, is that the internet has significantly changed offender behaviour. The huge volume of material and the global, borderless nature of the internet have challenged the very norms that societies are founded on. For law enforcement, they rely on borders and different jurisdictions to define their operations and with so much internet enabled crime it is becoming increasingly difficult to bring offenders to justice for all sorts of crimes where the victim is in one country, the offender in another and a crime is facilitated by a website hosted in a third jurisdiction. Under which legal process do you have the trial and who is responsible for bringing someone to justice in that scenario?
3. **Our experience: Working with Industry:**

Our Members



- 3.1 The IWF has over twenty years of dealing with these issues and has developed a strong working relationship with the internet industry, law enforcement and Government, both in the EU and UK of effectively dealing with the spread of child sexual abuse material online.
- 3.2 We believe that our model of self-regulation has been particularly effective, because at a time where the political environment has been uncertain, dominated by issues such as the 2008 financial crisis, fixing the economy and Brexit, these issues have not affected our collaborative approach with the internet industry. Our industry members fund our work and when they sign up to the IWF we ask that they do all that they can to stop the spread of this illegal material online.
- 3.3 Many of our big fee-paying members go above and beyond just paying the IWF membership. Google for example gave us £250,000 per year for four years to expand our team of Internet Content Analysts by seven people. Facebook and Twitter regularly pay for our staff to attend their internet safety events, with our Deputy CEO recently attending an event in Dublin and our Hotline Manager due to attend an event in San Francisco this summer.
- 3.4 They also lend us technical expertise as well as financial support. Microsoft, Cisco and Google have all sent us engineers to spend a week with us.
- 3.5 We have also worked directly with the industry to develop products and services to directly stop the spread of Child Sexual Abuse Material online. Our founder member BT worked closely with us to develop a URL blocking list as part of their “cleanfeed” innovation, which currently has on average 6,000 illegal URLs containing child sexual abuse on it and is reviewed daily by our analysts.
- 3.6 Microsoft developed PhotoDNA which enables them and us to create a unique Hash, (a unique fingerprint formed by a series of unique letters and numbers for each image), which then prevents this image being reuploaded to the internet once it has been defined as illegal. As the majority of images we deal with are duplicates, this helps prevent revictimisation of children in the images and also prevents ordinary members of the public stumbling across this content online. We are now working closely with them to develop PhotoDNA for Video which will enable us to act on specific video clips that we know contain child sexual abuse. At the time of writing this submission, we have over 300,000 unique illegal images of child sexual abuse on our Image Hash list. This is deployed daily by a number of major companies including Facebook and Google to stop the uploading of any duplicates on their platforms and is also used by the IWF in our proactive programme.
- 3.7 Over the past three years, Microsoft has also provided £15,000 annually in research grants to the IWF and this has enabled us to be an authoritative voice on the current trends, patterns and research in this area, with the latest piece of research based called “Trends in Online Sexual Exploitation: Examining the Distribution of Captured Live Streamed Child Sexual Abuse” due to be released in May 2018.

4. Our experience: Working with Government and the need for legal certainty

- 4.1 Whilst we clearly gain a lot of expertise, support and assistance from the internet industry, it is important to recognise the role that Government plays in our partnership approach to dealing with this content. We work closely with a number of Government Departments including the Home Office, Department of Digital, Culture, Media and Sport, Cabinet Office and Number 10 Downing Street in order to play our part in making the UK “the safest place to go online.” We also work with Parliamentarians in Westminster, the European Parliament in Brussels and in the devolved administrations as we also recognise the importance of advocating our work at a local level. We currently have 75 political champions a number of whom hold senior Cabinet and Shadow Cabinet positions.

- 4.2 One of the many lessons we have learned over our twenty plus-years of operation is that there is a need for legal certainty when removing content online and Government and politicians have a crucial role to play in defining what is and isn't illegal.
- 4.3 For Child Sexual Abuse Material, there is a clear legal framework, which is broadly accepted globally which has made it possible for us to be so effective at what we do.
- 4.4 In the UK, the Protection of Children Act (1978) makes it an offence to take, make, possess, show, distribute or advertise indecent images of children. The Criminal Justice and Immigration Act (2008) went further and built upon the Protection of Children Act, by extending the definition of a photograph to include tracings, derivatives and pseudo images whether made by electronic or other means and the Coroners and Justice Act (2009), went even further by defining Non-Photographic Images of children (manga and hentai for example) and made these illegal in the UK, the only country in the world to do so.
- 4.5 The IWFs remit is based on these laws, to remove Child Sexual Abuse Imagery wherever it occurs and to remove Non-Photographic Imagery (NPI) Child Sexual Abuse Imagery hosted in the UK.
- 4.6 We can assess content severity levels due to guidelines produced by the Sentencing Council. Their 2014 guidelines, mean that our analysts can define illegal child sexual abuse material following a three-step categorisation process as set out below, these are the same guidelines used by law enforcement and the judiciary use in bringing offenders to justice:

Category	Description
A	Image involves sexual penetrative activity; images involve sexual activity with an animal or sadism
B	Images involve sexual, non-penetrative sexual activity
C	Other indecent images not falling under Category A or B
Not illegal	The image is not deemed to be illegal.

- 4.7 It is important to recognise that the IWF also has no powers by statute. Our operations are governed by a [Memorandum of Understanding between the National Police Chiefs' Council \(NPCC\), the Crown Prosecution Service \(CPS\) and the IWF](#) and is linked to Section 46 of the 2003 Sexual Offences Act.
- 4.8 The industry is responsible for acting on illegal content online because of the Directive 2000/31/EC of the European Parliament and Council of 8th June 2000 on certain legal aspects of information society services electronic commerce, in the internal market ('Directive on Electronic Commerce').
- 4.9 The E-Commerce directive under section 40, creates "a duty to act, under certain circumstances, with a view to stopping or preventing illegal activities" it continues: "this directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States."
- 4.10 For the IWF this enables us to issue "Notice and Take Down" reports to the UK Internet Industry once our analysts have assessed an image as being illegal.
- 4.11 We have some of the fastest removal times anywhere in the world and our latest Annual Report statistics show that 53% of content was removed within two hours of a notice and takedown being issued.
- 4.12 Sections 17, 18 and 19 of the E-Commerce Directive relates to mere-conduits, caching and hosting are also of relevance to the IWFs activities and are essential to our collaborative approach with the internet industry. We would be keen to see these sections retained in their current state, if the Government considers reforming the Directive (particularly once Britain

leaves the European Union) as has been hinted and recommended recently by [Lord Bew's Intimidation in Public Life: A review by the Committee of Standards in Public Life.](#)

- 4.13 It is our belief that content that is deemed to be harmful and which should be removed from the internet should be defined in law and not subject to discretionary, subjective interpretation. We strongly believe, based on our experience, that this process should be independent of Government and free from political interference.
- 4.14 We also believe that the process for removing content from companies should also be independent of individual companies themselves. If left to individual companies, commercial imperatives can too easily shape decisions, and, in any case, smaller companies cannot afford the reviewing mechanisms that larger companies can. There is a myth that the tech industry is a-wash with money and the brightest and the best brains, with the ability to solve all the world's problems and whilst that may be true of some of the larger players, there is a need to recognise that much of the tech industry in the UK is made up of small start-ups that do not have access to the sorts of resources Government think they do.
- 4.15 It is our opinion that an independent process with company membership needs to be established, governed by a majority of independent board members, drawn from relevant stakeholders on the particular type of content that is being regulated.

5. Our Experience: Working with Law Enforcement:

- 5.1 The IWF has worked closely with law enforcement ever since its inception in 1996. Whilst we do not get involved in the investigative process, we complement law enforcement by offering a secure and anonymous place for the public to report and are currently one of the only hotlines in the world permitted to proactively search for this material online. In the UK, we work closely with National Crime Agency (NCA) Child Exploitation Online Protection (CEOP) team and our CEO sits on their Command Strategic Governance Group. Our Deputy CEO is a member of their Command Prevent Board. We also work closely with the Government (Home Office, RICU Team) in running an educational awareness programme that target 18-24-year old men who we know are most likely to stumble across this content online, to know the law and how to report if they do stumble across CSAM online.
- 5.2 We work closely with NCA CEOP and our CEO sits on their Command Strategic Governance Group and our Deputy CEO is a member of their Command Prevent Board.
- 5.2 What is clear to us is that the volume of material being unearthed by ourselves and law enforcement is presenting significant challenges to them. The IWF has graded 500,000 images for law enforcement to assist their development of the Child Abuse Image Database (CAID) and we are the first non-law enforcement agency to have access to this database, further highlighting our trusted position with Government and Law Enforcement, but much more needs to be done.
- 5.3 We would like to be able to use CAID data to supply hashes to the UK based internet industry in the form of hashes to ensure that even more illegal images than just the IWF data sets are able to be given to industry to prevent them being reuploaded to the internet and further reducing revictimisation. We have already piloted this approach with six companies with the agreement of the Home Office and are currently in discussions with the Department about how this can be further expanded.
- 5.4 We also believe that if we are going to ever come close to eradicating the spread of child sexual abuse imagery on line then this requires law enforcement to be properly resourced, both financially, technically and have people with the right skills in order to respond to highly sophisticated methods used by offenders producing and consuming this material. Issues such as end to end encryption, live streaming of abuse and expansion in the use of "hidden services" (websites hosted within proxy servers- otherwise known as the dark web), makes it almost impossible for law enforcement to produce an evidence trail for as it leaves little or no digital footprint for law enforcement to investigate or use as evidence in court.

6. Specific Questions posed by the inquiry:

6.1 Is there a need to introduce specific regulation for the internet? Is it desirable or possible?

- 6.1.1 We believe that the IWF's model works because there is a legal framework in place which defines what is illegal and what isn't illegal. This means that there is a clear standard for the IWF to enforce against in respect of Child Sexual Abuse Material (CSAM) online. There is also a legal framework in place which means that providers are liable for the content that they host through the e-commerce directive, which requires them to take action against illegal content once it is made aware to them and we believe that our model could be an example that could be replicated for other forms of internet harms.
- 6.1.2 We believe that the IWF model of self-regulation is unique and works, evidence by our impact over the last twenty-years and shows what can be achieved when there is legal certainty, an independent assessment process, transparency over what has been removed and a rigorous review process to ensure accountability over the decisions made.
- 6.1.3 It is our view that self-regulation does work where there is legal certainty over what is and isn't illegal. We do appreciate, however, that even though laws can define a legal framework, there are other challenges to overcome such as freedom of expression, which can be hugely subjective, difficult to define in law and technically difficult to enforce against.
- 6.1.4 The global, borderless nature of the internet does present unique challenges and cultural differences across different jurisdictions, which does make internet regulation particularly challenging where there is not international consensus on what is defined as illegal content.
- 6.1.5 Our work in removing CSAM online, however, is globally renowned, respected and experiences good levels of co-operation. Internationally, we play an active part in the WEPROTECT Global Alliance with our CEO sitting on its International Advisory Board and the UN's International Telecommunications Union (ITU) Child Online Protection (COP) Steering Group. We work closely with Europol and Interpol and by actively participating in Europol's EC3 meetings, related to European Cybercrime.
- 6.1.6 As a founding member of the [INHOPE](#) Association of hotlines (51 hotlines in 45 countries), we work with other hotlines to remove content hosted in other countries where a hotline exists. In the absence of a hotline in a country found to be hosting content, thanks to the legal support provided by law enforcement and a global acceptance of CSAM as being illegal, we can speed up the removal process for this content by working directly with law enforcement in a country where a hotline does not exist.
- 6.1.7 We are also currently implementing a three-year programme, funded by the Global Fund to End Violence against Children to establish 30 international reporting portals in the most underdeveloped countries in the world, to ensure that they have a place to report as internet penetration in those countries continues to grow. We currently have 13 reporting portals in British Overseas Territories and 8 other portals established in India, Belize, Namibia, Uganda, Tanzania, Mozambique, Mauritius and Malawi.
- 6.1.8 There are currently no bright ideas of how to introduce effective internet regulation without damaging the delicate infrastructure and eco-system which has made the internet such a valuable tool in the first place. Internet companies also do not see regulations as a credible threat as legislators often lack the technical "literacy" to understand what can be achieved in engineering terms, and, in turn what the useful role for regulation might be. Given the critical importance of internet based services and products to the UK economy the danger of unintended consequences particularly to smaller firms or start-ups (vital to the UK economy), of poor legislation needs to be very carefully considered.

6.2 What should the legal liability of online platforms be for the content that they host?

- 6.2.1 The IWF's model is based on trust and confidence of the internet industry in the assessment that is made by our analysts. In a time of political uncertainty, the IWF has made great strides forward in tackling illegal child sexual abuse material online, under the current regulations.
- 6.2.2 The e-commerce directive as outlined under the section which calls for legal certainty is particularly important to the IWF's activities and function. Without making platforms liable for the content that they host, it would be very difficult for the IWF to enforce "notice and take down" procedures, block access to illegal content and ultimately remove this from the internet, which will create more work for an already stretched law enforcement in the longer term. Any changes to this directive will create uncertainty and could have an impact on the spread of child sexual abuse material online.
- 6.2.3 We believe that the current legal framework for liability already exists and does not require any further changes of amendments for companies to cooperate with the removal of illegal content online.

6.3 How effective, fair and transparent are online platforms in moderating the content that they host? What process should be implemented for individuals who wish to reverse decisions to moderate content? Who should be responsible for reviewing this?

- 6.3.1 There is no doubt that online platforms need to be much more transparent in how much content that they are removing from their platforms. However, we also believe that any independent bodies that are also recommending to platforms content that should be removed are equally as transparent.
- 6.3.2 We support proposals contained within the Government's recent Internet Safety Strategy to introduce a transparency report and a voluntary code of practice which ensures that companies maintain processes and deal with notifications swiftly and efficiently and give clear explanations to the public about action taken against content. We believe that this approach should be voluntary, rather than statutory, as there have already been efforts by companies such as Google, to be much more transparent in the amount of content that they remove online and with both Facebook and Google announcing that they are making significant investment in personnel and technology to focus specifically on this. It is also clear, from our experiences that self-regulation can work, if the Government is clear on expectations of companies, but should not underestimate the complexities of the challenge as set out in the introduction to this response.
- 6.3.3 The IWF believes that users should have the right to appeal the legality of content that is removed from the internet, but that this should be a part of a range of measures to ensure compliance with the law. There have been examples of internet users reporting content to companies of information that is true but embarrassing in the way that wealthy and powerful people use UK defamation laws to protect their interests. We believe that companies and bodies responsible for the removal of content should ensure that those responsible for making decisions about the removal of content are trained to a high standard and supported both psychologically and managerially. We also believe that their decisions should be quality assured through a rigorous internal process and externally audited. Ultimately, any challenge to the legality of content should be subject to judicial review.
- 6.3.4 The IWF would be happy to co-host a series of roundtable events which debate and consider the right response to the form of content being regulated, based on our extensive knowledge and experience of working with industry, law enforcement and Government.

- 6.3.5 At the IWF, we gradually expose our analysts to the types of content that they will be reviewing and it can take six months to properly induct them before they are fully exposed to the most severe forms of content.
- 6.3.6 We ensure that they have mandatory counselling monthly, and are subject to a mandatory psychological assessment with an experienced professional to ensure that they are still able to cope with the process. We also ensure that for certain tasks such as hashing that regular breaks are taken to ensure that we are looking after their welfare effectively.

6.4 What role should users play in establishing and maintaining online community standards for behaviour?

- 6.4.1 The IWF is one of three charities (including SWGfL and Childnet International) who make up the UK Safer Internet Centre. There is a wealth of resources on the UK Safer Internet Centre webpage which provides advice and support to children, their parents and those professionals working with children and young people.
- 6.4.2 For children there are interactive games and quizzes, films and advice about staying safe online, with latest blog postings giving advice on [how to spot advertising on Instagram](#) and [how to control your privacy settings on the platform](#).
- 6.4.3 For Parents, there is advice about [safety tools on social media networks and other platforms](#), [a parent's guide to technology](#) and advice about [how to have a conversation with your child about safe internet usage](#).
- 6.4.4 The website also provides Teachers with [teaching resources](#) , [curriculum planning](#) and [appropriate filtering and monitoring](#).
- 6.4.5 All three charities that make up UKSIC believe that users play an important part in maintaining standards of behaviour online and that is why we run the [UK's Safer Internet Day](#) to encourage greater responsibility of children, parents and carers and those working with children and young people.
- 6.4.6 The day has been running in the UK for the last past eight years and the 2018 theme was specifically focussed on promoting more respectful behaviour online with the slogan: "Create, Connect and Share Respect a better internet starts with you." This day reached 45% of children aged 8-17 in the UK and 30% of parents and was supported by over 1700 organisations. We also believe that there is a need to educate children about the nature of the online world and how it works and operates.
- 6.4.7 The current political narrative in general places a lot of blame at the doors of the large tech companies for "needing to do more" to remove illegal and harmful content online. However, there are examples of flawed legislation which will have a negative impact on the availability of information, the freedom of expression online and many other of the internet's benefits if Britain decides to introduce greater regulation through proposing legislation by that focusses all their attention on "tech companies needing to do more."
- 6.4.8 One example of flawed legislation is the NetzDG law in Germany which requires companies to remove illegal content online or face large fines of up to 50 million euros. This is seeing companies removing more content than they should, some of it even legal, to avoid being heavily fined. Now politicians in Germany are calling on reform to the law to ensure that users also play their part in making the internet a safer place.

6.5 What measures should online platforms adopt to ensure online safety and protect the rights and freedom of expression and freedom of information online?

- 6.5.1 The UK Safer Internet Centre, again contains a number of resources which encourage people to express themselves online and to ensure that they do so respectfully. The UK Safer Internet Centre has produced a number of [Social Media Guides](#) relevant to all of the major platforms about online safety features and how to use their platforms responsibly.

- 6.5.2 The UK Safer Internet Centre, also provides a “one stop shop” to sign post those needing help to the right relevant organisations that can assist them with their specific concerns (hate speech, removal of suspected CSAM etc.) through [the need help?](#) Section of the website.
- 6.5.3 There are also a number of proposals contained within the [Government’s Internet Safety Strategy green paper](#), which include giving children and adults a greater understanding about their online safety. The Childnet Digital Leaders programme, supported by Facebook, puts young people at the heart of a whole schools’ approach and ensures internet safety learning is fun and effective.
- 6.5.4 Google has an “Internet legends programme” to educate primary school children in the UK to empower children and act responsibly online. The programme was designed in partnership with Parentzone, Childnet and the Oxford Internet Institute.
- 6.5.5 It is initiatives like these that educate children and young people about responsibility online which play a vital role in ensuring that children are aware of what is and isn’t acceptable online and the importance of their role in playing a responsible part of the internet eco-system.

6.6 What information should platforms provide to users about their personal data?

- 6.6.1 It is not for the IWF to comment on what platforms should provide to their users about their personal data. However, the GDPR legislation sets out provisions on informed consent that are consistent with international human rights norms.

6.7 In what ways should online platforms be more transparent about their business practice- for example their use of algorithms?

- 6.7.1 How public companies should be about the algorithms they use is a complex question as it goes right to the heart of the business model of the internet.
- 6.7.2 The sheer volumes of content now available online means that algorithms are now a vital tool used in identify harmful and illegal content online. However, if they come across potentially questionable material online, we believe that it is important that human analysts have the final say on any recommendation to have any content removed.

6.8 What is the impact of the dominance of a small number of online platforms in certain international markets?

- 6.8.1 Many of the smaller platforms do not have the capacity and resources to review illegal content and remove it, they are simply trying to make themselves commercially viable in the first instance. It is therefore important that all companies no matter their size can rid their platforms of illegal content online and that proposals such as designing in safety by design, proposed in the internet safety strategy are implemented.
- 6.8.2 The IWF operates a tiered approach to membership which sees the largest firms paying £79,000 per year for membership and the smaller platforms paying £1,060 based on the size and sector in which the firm operates. This means that we will work with all members and give them access to the services that they need in order to improve online safety for their users.
- 6.8.3 Clearly, the dominance of some companies does create challenges for the IWF. We have seen a number of mergers and acquisitions of companies which does have an impact on our ability to leverage more funding from the internet industry as there are less companies to contribute to membership fees if they have been brought out.

6.9 What effect will leaving the European Union have on the regulation of the Internet?

- 6.9.1 For the IWF there are several risks presented through Britain leaving the European Union. We will lose 10-15% of our funding as a result of no longer being eligible as a member state

for funding. Our current funding period runs until December 2018 and we are currently applying for a further round of funding which should secure funding until 2021, however, after that we will have to find alternative revenue streams. This could significantly impact on our ability to remove illegal CSAM online as the funding equates to 50% of our analyst's salaries.

- 6.9.2 With the UK enshrining all current EU legislation into UK law, there is the potential for the UK Government to make changes to existing EU legislation. One of our big concerns is that any reform to the e-commerce directive could change the nature of our relationship with the internet industry and make enforcement of notice and take down and blocking challenging, particularly if the liability framework for companies contained within this directive is altered.
- 6.9.3 Our recent annual report also states that over the past three years we have seen a gradual shift in the hosting of illegal child sexual abuse material from the U.S. and Canada to Europe with now 65% of content being hosted in the EU. We are concerned that the UK is a world-leader in eradicating this imagery online and that without our active involvement in Europe this could have a significant impact on the safeguarding of children in both Europe and the UK moving forward.
- 6.9.4 Finally, the IWF recently supported, along with a number of other civil society organisations, an amendment to the EU Bill (Withdrawal) at Committee and Report stage in the House of Lords, which asked that the Government lay before Parliament a strategy to deal with cross-border law enforcement issues post-Brexit. Our concern is that Britain could potentially lose expertise from agencies such as Europol and Eurojust which will make pursuing cross-border crimes potentially much more problematic post-Brexit. It is also possible that it will be harder to pursue criminals across borders without UK involvement in the European Arrest Warrant for example.