

Child sexual abuse online - detection, removal and reporting

Fields marked with * are mandatory.

Introduction

The fight against child sexual abuse is a priority for the EU.

The European Commission published in July 2020 the [EU Strategy for a more effective fight against child sexual abuse](#). The Strategy sets out a comprehensive response to the growing threat of child sexual abuse both offline and online, by improving prevention, investigation, and assistance to victims. It includes eight initiatives for the 2020-2025 period to put in place a strong legal framework, strengthen the law enforcement response, and facilitate a coordinated approach across the many actors involved in protecting and supporting children.

In particular, the Commission committed in the Strategy to:

- propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities; and
- start working towards the possible creation of a European centre to prevent and counter child sexual abuse, based on a thorough study and impact assessment. The centre would provide holistic support to Member States in the fight against child sexual abuse, online and offline, ensuring coordination to maximise the efficient use of resources and avoiding duplication of efforts.

Purpose

The purpose of the present open public consultation is to gather evidence from citizens and stakeholders to inform the preparation of the above initiatives and it is part of the data collection activities that the related [inception impact assessment](#) announced in December 2020.

Structure

Following a first set of questions to identify the type of respondent, the consultation has two sections, one for each of the initiatives in the Strategy that it covers:

1. Legislation to tackle child sexual abuse online effectively:

- Issue: what is the current situation and where are the gaps?
- Legislative solution: what should it include to tackle the above gaps effectively?

2. Possible European centre to prevent and counter child sexual abuse:

- Issue: what is the current situation and where are the gaps?

- Possible European centre: what features could it have to help tackle the above gaps effectively?

Terminology:

The consultation uses the following terminology:

- 'Child sexual abuse material' ('CSAM'), refers to material defined as 'child pornography' in Article 2(c) of [Directive 2011/93/EU](#). The consultation uses 'child sexual abuse material' instead of 'child pornography', in accordance with the [Luxembourg Guidelines](#).
- 'Grooming' refers to the solicitation of children for sexual purposes.
- 'Child sexual abuse online' includes both 'child sexual abuse material' and 'grooming'.

'Public authorities' refers to e.g. regional, national or international government entity, including law enforcement.

Privacy

All replies as well as position papers will be published online. Please read the privacy statement on how personal data and contributions will be processed.

The estimated time for completion is 30 minutes. Thank you for your contribution.

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Irish
- Italian
- Latvian
- Lithuanian

- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* First name

Michael

* Surname

TUNKS

* Email (this won't be published)

mike@iwf.org.uk

* Organisation name

255 character(s) maximum

Internet Watch Foundation (IWF)

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

144739515066-23

* Country of origin

Please add your country of origin, or that of your organisation.

- | | | | |
|---|--|--|--|
| <input type="radio"/> Afghanistan | <input type="radio"/> Djibouti | <input type="radio"/> Libya | <input type="radio"/> Saint Martin |
| <input type="radio"/> Åland Islands | <input type="radio"/> Dominica | <input type="radio"/> Liechtenstein | <input type="radio"/> Saint Pierre and Miquelon |
| <input type="radio"/> Albania | <input type="radio"/> Dominican Republic | <input type="radio"/> Lithuania | <input type="radio"/> Saint Vincent and the Grenadines |
| <input type="radio"/> Algeria | <input type="radio"/> Ecuador | <input type="radio"/> Luxembourg | <input type="radio"/> Samoa |
| <input type="radio"/> American Samoa | <input type="radio"/> Egypt | <input type="radio"/> Macau | <input type="radio"/> San Marino |
| <input type="radio"/> Andorra | <input type="radio"/> El Salvador | <input type="radio"/> Madagascar | <input type="radio"/> São Tomé and Príncipe |
| <input type="radio"/> Angola | <input type="radio"/> Equatorial Guinea | <input type="radio"/> Malawi | <input type="radio"/> Saudi Arabia |
| <input type="radio"/> Anguilla | <input type="radio"/> Eritrea | <input type="radio"/> Malaysia | <input type="radio"/> Senegal |
| <input type="radio"/> Antarctica | <input type="radio"/> Estonia | <input type="radio"/> Maldives | <input type="radio"/> Serbia |
| <input type="radio"/> Antigua and Barbuda | <input type="radio"/> Eswatini | <input type="radio"/> Mali | <input type="radio"/> Seychelles |
| <input type="radio"/> Argentina | <input type="radio"/> Ethiopia | <input type="radio"/> Malta | <input type="radio"/> Sierra Leone |
| <input type="radio"/> Armenia | <input type="radio"/> Falkland Islands | <input type="radio"/> Marshall Islands | <input type="radio"/> Singapore |
| <input type="radio"/> Aruba | <input type="radio"/> Faroe Islands | <input type="radio"/> Martinique | <input type="radio"/> Sint Maarten |
| <input type="radio"/> Australia | <input type="radio"/> Fiji | <input type="radio"/> Mauritania | <input type="radio"/> Slovakia |
| <input type="radio"/> Austria | <input type="radio"/> Finland | <input type="radio"/> Mauritius | <input type="radio"/> Slovenia |

- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau

- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara

- Cyprus
- Latvia
- Saint Barthélemy
- Yemen
- Czechia
- Lebanon
- Saint Helena Ascension and Tristan da Cunha
- Zambia
- Democratic Republic of the Congo
- Lesotho
- Saint Kitts and Nevis
- Zimbabwe
- Denmark
- Liberia
- Saint Lucia

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, ‘business association, ‘consumer association’, ‘EU citizen’) country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

Public

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

I agree with the [personal data protection provisions](#)

1. Legislation to tackle child sexual abuse online effectively

a. Issue: what is the current situation and where are the gaps?

1. In your experience, what types of child sexual abuse online and related activities are most concerning and should be tackled in priority?

- Distribution of **known** child sexual abuse material by uploading it to the open web (e.g. by posting it in social media or other websites, uploading it to image lockers, etc)
- Distribution of **known** child sexual abuse material via messaging applications and e-mails
- Distribution of **known** child sexual abuse material via darknets
- Distribution **known** of child sexual abuse material in peer-to-peer networks
- Distribution of **new** child sexual abuse material by uploading it to the open web (e.g. by posting it in social media or other websites, uploading it to image lockers, etc).
- Distribution of **new** child sexual abuse material via messaging applications and e-mails
- Distribution of **new** child sexual abuse material via darknets
- Distribution of **new** child sexual abuse material in peer-to-peer networks
- Online grooming of children
- Children distributing self-generated material
- Other

Please specify:

500 character(s) maximum

Dealing with both grooming and live streaming remain technically very challenging. Currently it is very difficult to act on a live stream as the technology isn't well developed enough and it is only the companies which would have the power to act in this area.

2. Why do you consider the above activities most concerning? Please explain, also taking into account the current measures in place that you are aware of to tackle the above activities.

2000 character(s) maximum

The current global pandemic seems to have exacerbated the threat to children online. The IWF has once again had a record year, processing 299,000 reports of suspected child sexual abuse imagery and confirming over 153,000. This includes a period of 6 weeks during 2020, when IWF was operating at a reduced capacity whilst we initially responded to the pandemic. In 2020, we also saw a huge rise in self-generated indecent images of children, up 77% on the previous year, with a total 68,000 reports actioned by the hotline containing self-generated child sexual abuse.

We know that this situation is in part because children and those who seek to groom and exploit them are both spending increasing amounts of time online creating a perfect storm of events. It is now estimated in the UK that 300,000 people pose a threat to children either through online or contact offending. Estimates make the UK the third highest consumer of live-streamed child sexual abuse and Europol has noted similar increases in the downloading of CSAM in Spain and Denmark with huge investigations being conducted into 30,000 people in Germany and a huge investigation in Italy by Europol in July 2020.

The IWF has removed record numbers of image and videos hosted mainly on image hosting boards and cyberlockers located mainly within the EU and the Netherlands. Whilst there has been some progress made in this area with legislation being introduced in the Netherlands which seeks to name and shame those companies hosting content there and there have been some operational success stories the numbers continue to grow. The IWF is monitoring and responding to the opportunities created by both the Digital Services Act proposal, this new CSEA strategy and the UK's Online Harms legislation which present further opportunities to act through the Know Your Business Customer principle and by designating hotlines as trusted flaggers.

Please specify:

500 character(s) maximum

The Internet Watch Foundation's 2019 Annual report found 89% of the URLs we removed in 2019, were hosted in Europe, 71% in the Netherlands. 84% of this content was found on image hosting boards and 6% on cyberlockers. In 2020, we have also seen a rise in self-generated indecent images of Children. Up 77% on 2019 and we remain concerned about the potential links between the creation of this imagery and grooming and exploitation of young girls aged 11-13 who are most likely to appear in images.

3. Considering the current gaps in the fight against child sexual abuse online that in your view exist, which of the following outcomes should the new legislation aim to achieve in priority with regard to child sexual material and online grooming?

- Reduce the amount of **known** child sexual abuse material uploaded in the open web
- Reduce the amount of **known** child sexual abuse material distributed via messaging applications and emails
- Reduce the amount of **known** child sexual abuse material distributed via darknets
- Reduce the amount of **known** child sexual abuse material distributed via peer-to-peer networks

- Reduce the amount of **new** child sexual abuse material uploaded in the open web
- Reduce the amount of **new** child sexual abuse material distributed via messaging applications and emails
- Reduce the amount of **new** child sexual abuse material distributed via darknets
- Reduce the amount of **new** child sexual abuse material distributed via peer-to-peer networks
- Reduce the amount of sexual material self-generated by children distributed online
- Enable a swift takedown of child sexual abuse material after reporting
- Ensure that child sexual abuse material stays down (i.e. that it is not redistributed online)
- Reduce the number of instances of online grooming of children
- Other

Please specify:

500 character(s) maximum

IWF provides tools and services assist many companies to disrupt CSAM. In just 1 month We identified 8.8m attempts to access known CSAM through companies deploying these vitally important services.

Detection of new imagery is challenging. Strengthening reporting mechanisms, improved awareness of the law, investing in new technology and tackling the threat posed by encryption are priorities.

Peer to peer and dark web should be dealt with through alternative legal frameworks.

4. Considering the current gaps in the fight against child sexual abuse online that in your view exist, which of the following outcomes should the new legislation aim to achieve in priority with regard to tackling child sexual abuse in general, including prevention and victim support aspects?

- Provide legal certainty for all stakeholders involved in the fight against child sexual abuse online (e.g. service providers, law enforcement and child protection organisations)
- Enable a swift start and development of investigations
- Improve transparency and accountability of the measures to fight against child sexual abuse online
- Ensure that the legislation is future proof, i.e. that it remains effective despite future technological developments

- Ensure a victim-centric approach in investigations, taking the best interests of the child as a primary consideration
- Improve prevention of child sexual abuse
- Improve assistance to victims of child sexual abuse
- Other

Please specify:

500 character(s) maximum

We have called for a regulation to replace the current CSAM directive to help solve some of the transposition issues with the current directive. We also believe that prevention will be vital in addressing self-generated imagery. We have also seen the challenges with the current temporary derogation and during the e-privacy file. It is vitally important that the EU does not enshrine technology solutions in law, legislation must remain flexible to new technological solutions.

5. In which of the following ways do you cooperate **with law enforcement authorities** in the fight against child sexual abuse online?

- Forwarding reports of child sexual abuse online received from the public
- Forwarding reports of child sexual abuse online received from service providers
- Providing technology for the detection of child sexual abuse online
- Providing hash lists for the detection of child sexual abuse material
- None
- Other

Please specify:

500 character(s) maximum

We are the only non-law enforcement agency with access to the National Child Abuse Image Database (CAID) in the UK. We are one of three trusted votes required for the classification of imagery in that system and are currently undertaking a project to assess 2 million images from the database to pass onto industry. We provide law enforcement with images that we have found proactively which contribute to CAID. Reporting facilities operate in 46 countries and tech firms deploy our services globally

6. Are there any areas of improvement in the cooperation between civil society organisations and law enforcement authorities in the fight against child sexual abuse online?

- Yes
- No
- No opinion

If yes, what are the areas of improvement?

1000 character(s) maximum

Law Enforcement is often responsible for holding large amounts of imagery and data. It would be helpful if this imagery and data could be shared with civil society organisations, where appropriate, to better understand how we could assist with the prevention and detection of child sexual abuse images and videos.

If the European Commission continues as planned with the development of the new Centre it must recognise that for the fight against child sexual abuse to be effective it will need to ensure that law enforcement can work together with the internet industry globally. The IWF brings 25 years' worth of experience of working with law enforcement and our 150+ industry members in the global deployment of technical tools and services. We believe that as an NGO we can effectively bridge the gap between law enforcement and industry and this partnership could and should be strengthened further, with global hash sharing and interaction between lists a real priority.

7. In which of the following ways do you cooperate **with service providers** in the fight against child sexual abuse online?

- Sending notice-and-takedown requests to service providers
- Receiving reports of child sexual abuse online from service providers
- Providing technology for the detection of child sexual abuse online
- Providing hash lists for the detection of child sexual abuse material
- Advising service providers on policies to fight child sexual abuse online
- Other

Please specify:

500 character(s) maximum

The IWF provides a secure and anonymous reporting function to members of the public, which is available on our website. It is also possible for the industry, law enforcement and others to report into the IWF, although this is not where we receive the bulk of our reports. We also provide industry with hashes, our URL blocking list and several other key services which help keep their platforms free from CSAM. We are also members of several of the trust and safety boards of companies.

8. Are there any areas of improvement in the cooperation between civil society organisations and service providers in the fight against child sexual abuse online?

- Yes
- No
- No opinion

If yes, what are the areas of improvement?

2000 character(s) maximum

The IWF is uniquely placed to comment on the relationship between civil society and industry. For 25 years we have successfully levied funding out of the industry to improve our collective response to child sexual abuse online. The funding the industry gives the IWF is crucial in ensuring that the data sets we provide remain high quality, up to date and effective in the fight against child sexual abuse online. This funding enables us to proactively crawl the internet and invest in the latest tools and services to improve the collective response. We provide a secure and safe space for the industry to come together and discuss the latest challenges in fighting child sexual abuse online and we have increasingly assisted by acting as a broker between the industry and government in the UK on these issues. We would also be very willing to adopt a similar role in the EU if this would assist the Commission.

There is always scope to improve the relationship between NGOs and the industry. We believe that one of the areas we could particularly assist industry in, is training their moderators to recognise child sexual abuse more effectively. We also believe we have some of the strongest welfare standards in the industry and we could also assist companies in designing effective processes for safeguarding the health and welfare of their staff.

In the UK, we believe we have a new role to play in assisting the new regulator with codes of practice, transparency requirements and conducting investigations on behalf of the regulator. In the same way we are proposing to assist the regulator, through the development of a new regulatory arm, we could assist the industry further by also assisting them in developing robust policies and processes to achieve effective regulatory compliance and in improving their response to this issue. The IWF has recently updated its MoU with the CPS and NPCC in the UK with the purpose of providing these services potentially in the future.

9. In your opinion, do current efforts to tackle child sexual abuse online strike an appropriate balance between the rights of victims and the rights of all users (e.g. privacy of communications)?

at most 1 choice(s)

- Yes, the balance is about right
- No, current efforts place too much emphasis on victims' rights and not enough emphasis on the rights of all users
- No, current efforts place too much emphasis on the rights of all users and not enough emphasis on victims' rights
- No opinion

Comments

1000 character(s) maximum

We believe that this is an incredibly complex question, in which the options set out above do not do the question justice. There is always a balance to be struck between privacy of users and the safety of children. The current position the European Commission finds itself in on the temporary derogation from the Electronic Communications Code is skewed heavily in the favour of privacy rights of all users rather than victims. The temporary derogation simply wants to ensure the status quo continues, that companies can carry out all the activities they have previously undertaken to ensure child safety and welfare.

The responses to this question must avoid as falling on one side or another. Instead, the question should be seeking to find solutions that both protect the privacy of users, whilst ensuring the protection of children. Often these debates become too polarising, and this significantly hinders progress.

10. Do you have any other comments in relation to the current situation and challenges in your actions to fight against child sexual abuse online?

2000 character(s) maximum

b. Legislative solution: what should it include to tackle the above gaps effectively?

Scope

1. If online service providers were to be subject to a legal obligation to detect, remove and report child sexual abuse online in their services, providers of which of the following services should be subject to that legal obligation?

- Instant messaging
- Text-based chat (other than instant messaging)
- Webmail
- Voice chat
- Video chat
- Video streaming
- Audio streaming
- Web hosting
- Image hosting
- Social media
- Online gaming
- Cloud infrastructure
- Message boards
- No service provider should be subject to such legal obligation
- Other

Please specify:

500 character(s) maximum

Any changes to the CSAM directive must also be aligned with the proposed changes in the EU's Digital Services Act. The e-commerce liability regime has been the foundation for how hotlines have been able to notify and get illegal content removed from the internet. It is critically important that any changes are aligned.

We believe the EU should be adopting consistent frameworks and ensuring as broader scope as possible by utilizing frameworks used in the NISD, ECS, EECC or ISS Re: e-privacy.

2. If legislation were to explicitly allow online service providers to take voluntary measures to detect, remove and report child sexual abuse online in their services, providers of which of the following services should be included?

- Instant messaging
- Text-based chat (other than instant messaging)
- Webmail
- Voice chat
- Video chat
- Video streaming
- Audio streaming
- Web hosting
- Image hosting
- Social media
- Online gaming
- Cloud infrastructure
- Message boards
- No service provider should be legally enabled to take such voluntary measures
- Other

Please specify:

500 character(s) maximum

3. If legislation was to either allow or oblige relevant online service providers to detect, remove and report child sexual abuse online in their services, should the legislation apply to service providers that offer services within the EU, even when the providers themselves are located outside the EU?

Yes

No

Comments

1000 character(s) maximum

Mandatory reporting must complement other global reporting structures. For example, US companies already report into the NCMEC and that process should continue for US companies. To ask them to also report to an EU Centre would create unnecessary duplication.

We support the introduction of obligating the detection and removal of CSAM, however, mandatory reporting for EU companies we believe currently needs further consideration. There are different member state laws to consider on what is defined as illegal content currently, the volume of reports from a single service provider could easily overwhelm the mandatory reporting function and technically this could be extremely costly to implement. The Commission should carry out a full cost benefit analysis of such a proposal.

The EU must ensure that all these proposals improve our understanding of the problem and complement other already well-established systems and processes, not simply add more reports or duplicate current efforts.

4. Which types of child sexual abuse online should the possible legislation cover and how?

	Mandatory detection and removal	Mandatory reporting	Voluntary detection and removal	Voluntary reporting	No need to cover this in the legislation
Known child sexual abuse material (i.e. material previously confirmed as constituting child sexual abuse)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
New (unknown) child sexual abuse material	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online grooming	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Live-streaming of child sexual abuse	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Comments

2000 character(s) maximum

All forms of Child Sexual Abuse should be prevented from circulating on the internet wherever possible. Companies can utilise technical tools such as hashes to prevent its upload in the first place and where imagery is awaiting removal URL blocking is a good way of effectively disabling public access.

Mandatory reporting, however, is particularly important in cases of online grooming and live streaming. This is because there could be an immediate risk to a child's welfare and in the case of live streaming, it is very difficult to detect after the event as live streams leave very little digital footprint for investigators to follow, unless footage from the live stream has been "capped".

Our views on known child sexual abuse material are that it should be prevented from being uploaded in the first place using hash lists. There are effective mechanisms in place through hotlines on a voluntary basis for dealing with known child sexual abuse material, with content being removed as quickly as 10 minutes from being notified. The IWF finds that where we have pre-existing relationships with companies through our membership, that this is particularly effective.

With the detection of new CSAM material it is vitally important that hotlines work with law enforcement to identify new children in that imagery so that they can be potentially safeguarded, and offenders brought to justice. There have been numerous examples in recent years, where work carried out by IWF analysts have led directly to the rescue of children.

The priority must always be the safety and welfare of children. It is vitally important that any system which encourages mandatory reporting improves our response to keeping them safe. Focusing on those cases which cause the highest harm and those most at risk from immediate threats to life or danger have to be prioritised over previously detected imagery, where a child may have already been safeguarded.

5. Some of the current tools that service providers use to voluntarily detect, report and remove child sexual abuse online do not work on encrypted environments. If online service providers were to be subject to a legal obligation to detect, remove and report child sexual abuse online in their services, should this obligation apply regardless of whether these services use encryption?

- Yes
- No

Comments

2000 character(s) maximum

The IWF is extremely concerned about the impact of end-to-end encryption to detect child sexual abuse. We are not against the introduction of end-to-end encryption, but we believe that if companies want to introduce this on their services that they should first ensure equivalency with the current protections in place to safeguard children. If this cannot be achieved, then companies should not be encrypting their services. The IWF has been vocal about the impacts of encryption through our recent campaigning on DNS over HTTPS.

We also believe that it is vitally important that the EU reaches a conclusion on the temporary derogation as soon as possible. If it cannot be agreed for PhotoDNA to continue to be used on email and messaging services, encryption will be the least of our collective concerns. The reduction of reports to NCMEC (down 51%) gives some idea of the challenges that encrypting these services would have for law enforcement and others in the fight against child sexual abuse.

The European Commission should be working with partners globally to challenge the internet industry to design solutions to ensuring companies can continue to detect CSAM in encrypted channels. Currently there are no technical solutions to this problem, so therefore we believe a solution should be found before services encrypt.

6. If yes, what should be the form of such legal obligation?

- Relevant online service providers who offer encrypted services should be obliged to maintain a technical capability to proactively detect, remove and report child sexual abuse online in their services
- Other

Safeguards

7. To be able to detect, remove and report child sexual abuse online, service providers need to carry out a series of actions.

To what extent do you agree that the following actions are proportionate, when subject to all the necessary safeguards?

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
To check whether images or videos uploaded online (e.g. to a social media platform, or a file hosting service) are copies of known child sexual abuse material	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To assess whether images or videos uploaded online (e.g. to a social media platform, or a file hosting service) constitute new (previously unknown) child sexual abuse material	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To check whether images or videos sent in a private communication are copies of known child sexual abuse material	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To assess whether the images or videos sent in a private communication constitute new child sexual abuse material	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To assess whether the contents of a text-based communication constitute grooming	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To assess, based on data other than content data (e.g. metadata), whether the user may be abusing the online service for the purpose of child sexual abuse	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. The actions to detect, remove and report child sexual abuse online may require safeguards to ensure the respect of fundamental rights of all users, prevent abuses, and ensure proportionality.

To what extent do you agree that the legislation should put in place safeguards to ensure the following:

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
The tools used to detect, report and remove child sexual abuse online reduce the error rate to the maximum extent possible	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The tools used to detect, report and remove child sexual abuse online are the least privacy intrusive	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The tools used to detect, report and remove child sexual abuse online comply with the data minimisation principle and rely on anonymised data, where this is possible	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The tools used to detect, report and remove child sexual abuse online comply with the purpose limitation principle , and use the data exclusively for the purpose of detecting, reporting and removing child sexual abuse online	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The tools used to detect, report and remove child sexual abuse online comply with the storage limitation principle , and delete personal data as soon as the purpose is fulfilled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The online service provider conducts a data protection impact assessment and consults the supervisory authority , if necessary	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Online service providers are subject to the oversight of a supervisory body to assess their compliance with legal requirements	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reports containing new material or grooming are systematically subject to human review before the reports are sent to law enforcement or organisations acting in the public interest against child sexual abuse	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
All reports (including those containing only previously known child sexual abuse material) are systematically subject to human review before the reports are sent to law enforcement or organisations acting in the public interest against child sexual abuse	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A clear complaint mechanism is available to users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Effective remedies should be available to users that have been erroneously affected by the actions of the service provider to detect, report and remove child sexual abuse online	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Providers should make clear in the Terms and Conditions that they are taking measures to detect, report and remove child sexual abuse online	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify):

2000 character(s) maximum

We felt it important to justify the reason why we do not agree with the data minimisation principle. We fully understand and recognise the importance of the protection of fundamental rights and people's right to privacy. We are not against people having the right to a private life, however, when it comes to children, they also have the right to a childhood free from sexual exploitation and abuse. They also have the right to play and explore the online digital world safely. Victims of child sexual abuse also have a right to privacy. They have the right not to have images of their abuse spread and circulated online.

We feel it is important to stress the accuracy of detection technologies which has been central to the arguments around the current temporary derogation from the e-privacy directive. The detection of child sexual abuse images and videos is highly accurate, particularly when it comes to the use of PhotoDNA which has an exceptionally low false positive rate. It has a 1 in 100,000,000 false positive rate and this technology is widely deployed by over 50 technology companies globally. It provides vitally important insight that allows organisations like the IWF to rescue victims of abuse in partnership with law enforcement and bring offenders who are exchanging these images to justice. It is vitally important that companies have the ability to retain any information they may have about victims or offenders when making reports to mandatory reporting bodies or law enforcement, so that this information can be used in the investigative process in bringing potential offenders to justice.

It is also important to recognise that changes in GDPR, have meant that data protection regulators in the UK and in Spain and elsewhere in Europe has deemed hashes to be pseudonymized personal data. It is vitally important that hashes can continue to be used to detect and prevent the upload of known CSAM imagery and that any data minimisation principles do not apply to them

Sanctions

9. To what extent do you agree with the following statements, in the context of possible future legislation allowing/obliging relevant online service providers to detect, report and remove child sexual abuse online in their services:

	Fully agree	Partially agree	Partially disagree	Fully disagree	No opinion
Companies should be subject to financial sanctions if they fail meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Companies should be subject to criminal sanctions if they fail meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Companies that erroneously detect, remove or report child sexual abuse online in good faith should not be subject to the relevant sanctions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

There should be no sanctions for failure to meet the legal obligations (including safeguards) related to the detection, reporting and removal of child sexual abuse online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
---	-----------------------	-----------------------	-----------------------	-----------------------	----------------------------------

Other (please specify):

2000 character(s) maximum

More work needs to be carried out on the liability of senior manager and financial sanctions for companies. The question is very broad in its outline and identifying who is responsible is a complex question depending on the position of a company in the internet infrastructure stack. For example, an ISP enables access to the internet, but if the user is using a VPN or an encrypted service such as an App or web browser, then the ISP would not be able to see the content and prevent a user accessing known illegal child sexual abuse material through a block list. A question though would remain, that they are responsible for providing the connection, but would argue that they couldn't be held liable for content on other platforms or services. In the argument of DNS over HTTPS, the fact that a user could change their trusted recursive resolver (TRR) to that of their ISP, could also again raise questions of where the responsibility lies.

The EU needs to consider how they could force executives of companies based overseas to act in compliance with EU law? This is further complicated by cloud hosting providers who for example are responsible for a site administered in Malaysia, is hosting in Uzbekistan, and receiving services from a potentially corrupt provider.

Finally, even though greater clarity is needed on scope, responsibility, and the international aspect of these crimes, the IWF would certainly welcomes further measures to focus the minds of the executives of image hosting boards and cyberlockers, particularly in the Netherlands who are in large part, responsible for almost 90% of the content we removed in the last year. We welcome the steps by the Dutch Minister, Ferdinand Grapperhaus, to introduce new legislation to address these issues, it is vitally important that this new legislation encourages effective co-operation with those bad actors who have been responsible for hosting most of this content. The new CSAM strategy and DSA should complement this effort.

Transparency and accountability

10. Transparency reports could refer to periodic reports by service providers on the measures they take to detect, report and remove child sexual abuse online. These transparency reports should be:

	Yes	No	No opinion
Obligatory to ensure transparency and accountability	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Voluntary : an obligation would incur an additional burden on the online service providers, especially when they are small and medium enterprises	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Evaluated by an independent entity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Standardised , to provide uniform quantitative and qualitative information to improve the understanding of the effectiveness of the technologies used as well as the scale of child sexual abuse online	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Other (please specify):

500 character(s) maximum

Companies are making steps to improve the transparency and accountability of their operations. The DSA and CSAM strategy present opportunities to ensure greater levels of transparency on CSAM. Each platform operates in a different way and that these differences must be considered when transparency reports are published. Many have different terms and conditions about what is acceptable on their platforms and many also count child nudity reports in with CSAM. Contextual information is important

11. **Transparency reports** should include the following information:

- Number of reports of instances of child sexual abuse online reported by type of service
- Number of child sexual abuse material images and videos reported by type of service
- Time required to take down child sexual abuse material after it has been flagged to/by the service provider
- Types of data processed to detect, report and remove child sexual abuse online
- Legal basis for the processing to detect, report and remove child sexual abuse online
- Whether data are shared with any third party and on which legal basis
- Number of complaints made by users through the available mechanisms and the outcome of those proceedings
- Number and ratio of false positives (an online event is mistakenly flagged as child sexual abuse online) of the different technologies used
- Measures applied to remove online child sexual abuse material in line with the online service provider's policy (e.g. number of accounts blocked)
- Policies on retention of data processed for the detecting, reporting and removal of child sexual abuse online and data protection safeguards applied
- Other

Performance indicators

12. Which indicators should be monitored to measure the success of the possible legislation?

- Number of reports of child sexual abuse online reported by company and type of service

- Number of child sexual abuse material images and videos reported by company and type of service
- Time required to take down child sexual abuse material after it has been flagged to/by the service provider
- Number of children identified and rescued as a result of a report, by company and type of service
- Number of perpetrators investigated and prosecuted as a result of a report, by company and type of service
- Number of related user complaints as a result of a report, by company and type of service
- Other

Please specify:

1000 character(s) maximum

IWF has recently contributed to a paper produced by the UK Government on Transparency. A number of recommendations were made as a result of that working group which we feel could be of use to the European Commission: <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/government-transparency-report#conclusion-and-next-steps>

Whilst the numbers of reports (focused on very heavily in the above section) is important, it is perhaps, even more so, to include context around these numbers. Often headlines can report high numbers or low numbers, and these can be used to either say a company is a wash with CSAM or it is not finding enough. Having the appropriate contextualization around the data is extremely important. Each company operates in a different way and therefore the Commission should ensure that any transparency mechanisms make this clear. Comparing what is removed on one platform, with another is not particularly helpful if they report in different way.

2) Possible European centre to prevent and counter child sexual abuse

a. Issue: what is the current situation and where are the gaps?

1. Do you see a need for additional coordination and support at EU level in the fight against child sexual abuse online and/or offline to maximize the efficient use of resources and avoid duplication of efforts?

- Yes
- No
- No opinion

Comments

1000 character(s) maximum

There is a gap in unification and standardization of efforts on EU level (and internationally). There is a need for coordination of data sharing (hashes and intelligence) without duplicating efforts and creating yet another institution, but adding a real value to the fight against online CSAM. Consistency and compatibility with international efforts to tackle CSAM should always be ensured.

There is a need at European level to work closer with industry and provide clear detection and reporting mechanisms and regulations. There is a need for a unified and harmonized classification of CSAM across Europe. Technology tools used by all actors in the field (LEA, hotlines, industry) which enable smooth data exchange can maximize efforts to prevent and detect online CSAM and duplication of efforts across the board. If such centre is going to be established it should maintain links with the stakeholders acting at national level to reflect the diversity of the national situation.

2. Please specify the challenges in the fight against child sexual abuse that could benefit from additional coordination and support at EU level

- Law enforcement: lack of an EU approach (i.e. based on EU rules and/or mechanisms) to detect child sexual abuse online and in particular lack of a single **EU database** to detect known child sexual abuse material
- Law enforcement: lack of EU approach to **determine relevant jurisdiction (s)** of the instances of child sexual abuse online and to **facilitate investigations**
- Law enforcement: lack of an EU approach in the functioning of **hotlines** to report child sexual abuse online
- Law enforcement: lack of control mechanism at EU level to ensure **accountability and transparency** (e.g. in cases of erroneous takedown or abuse in the search tools to report legitimate content, including misuse of the tools for purposes other than the fight against child sexual abuse)
- Prevention: insufficient **research** into what motivates individuals to become offenders
- Prevention: lack of **evaluation** of effectiveness of prevention programmes
- Prevention: insufficient **communication and exchange of best practices** between practitioners (e.g. public authorities in charge of prevention programmes, health professionals, NGOs) and researchers
- Assistance to victims: insufficient **research** on the effects of child sexual abuse on victims
- Assistance to victims: lack of **evaluation** of effectiveness of programmes to assist victims

- Assistance to victims: insufficient **communication and exchange of best practices** between practitioners (e.g. public authorities, health professionals, NGOs) and researchers
- Other

b. Possible European centre: what features could it have to help tackle the above gaps effectively?

Roles

Law enforcement support

1. Should the centre be established, which of the following functions would be relevant to support law enforcement action in the fight against child sexual abuse in the EU?

	Very relevant	Relevant	Somewhat relevant	Not relevant	No opinion
Receive reports in relation to child sexual abuse, ensure the relevance of such reports, determine jurisdiction(s), and forward them to law enforcement for action	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Maintain a single EU database of known child sexual abuse material to facilitate its detection in companies' systems	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Coordinate and facilitate the takedown of child sexual abuse material identified through hotlines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Monitor the take down of child sexual abuse material by different stakeholders	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Comments (including other possible functions to support law enforcement action, if any):

1000 character(s) maximum

There are already suitable mechanisms in place for receiving reports of Child Sexual Abuse Material and in co-ordinating the swift and effective take down and removal of content. The ICCAM database hosted by INHOPE allows the transfer of cases between hotlines in each jurisdiction in the EU and those hotlines have relationships with their national law enforcement. In the case of the IWF we also prevent this content from being reuploaded through the provision of hash datasets. More can be done to ensure hash data sets can interact with each other more effectively and take into account international collaborations. The IWF knows well the benefits of joining up the activities with hotlines and law enforcement through its work with the CAID database. There is clearly also some relevance in monitoring the compliance of companies with NTDs in a swift and efficient manner and also in holding companies to account for the systems and process they have in place for dealing with reports of CSAM.

2. What other roles, if any, could the possible centre, play in relation to the EU co-funded network of INHOPE hotlines in the Member States?

([INHOPE](#) is an international association of Internet hotlines co-funded by the European Commission. It focuses on the removal of illegal content, specifically child sexual abuse material online)

1000 character(s) maximum

Hotlines have an extremely important role to play in the detection, removal and prevention of child sexual abuse imagery online. Over 25 years we have built up a wealth of knowledge, expertise and experience in dealing with CSAM online. We believe that our work and experiences should be built on, further enhanced and that there is great scope within the Commission's proposals to do this.

The LIBE Committee made a number of recommendations in their 2017 report which remain highly relevant to this consultation. We outlined our support for their proposals in our submission on the roadmap.

We believe that we have led the way in Europe on proactive searching and working collaboratively with the internet industry. We currently have plans in place to enable hash data sets that currently assess to different standards globally to communicate more effectively with one another and are investing in web crawlers and image classifiers that will further improve our response.

3. Should the centre be established, which of the following functions would be relevant to ensure transparency and accountability regarding actions of service providers to detect, report and remove child sexual abuse online in their services?

	Very relevant	Relevant	Somewhat relevant	Not relevant	No opinion
Ensure that the tools employed are not misused for purposes other than the fight against child sexual abuse	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure that the tools employed are sufficiently accurate	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure that online service providers implement robust technical and procedural safeguards	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Draft model codes of conduct for service providers' measures to detect, report and remove child sexual abuse online	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sanction service providers whose measures to detect, report and remove child sexual abuse online, including associated technical and procedural safeguards, do not meet legal requirements	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Receive complaints from users who feel that their content was mistakenly removed by a service provider	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Publish aggregated statistics regarding the number and types of reports of child sexual abuse online received	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Comments (including other possible functions to ensure transparency and accountability, if any):

1000 character(s) maximum

4. Please share any good practices or any other reflections with regard to the support to law enforcement investigations that the possible centre could provide.

1000 character(s) maximum

Prevention

5. Should the centre be established, which of the following functions would be relevant to **support prevention efforts** in the fight against child sexual abuse in the EU?

	Very relevant	Relevant	Somewhat relevant	Not relevant	No opinion
Support Member States in putting in place usable, rigorously evaluated and effective multi-disciplinary prevention measures to decrease the prevalence of child sexual abuse in the EU	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Serve as a hub for connecting, developing and disseminating research and expertise, facilitating the communication and exchange of best practices between practitioners and researchers	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Help develop state-of-the-art research and knowledge, including better prevention-related data	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide input to policy makers at national and EU level on prevention gaps and possible solutions to address them	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Comments (including other possible functions to support prevention efforts, if any):

1000 character(s) maximum

6. What key stakeholders in the area of prevention should the possible centre cooperate with to stimulate the exchange of best practices and research?

1000 character(s) maximum

7. What role could the possible centre play to improve the cooperation with industry on prevention?

1000 character(s) maximum

8. What practical actions could the possible centre take to raise awareness on prevention issues?

1000 character(s) maximum

Assistance to victims

9. Should the centre be established, which of the following functions would be relevant to **support efforts to assist victims** of child sexual abuse in the EU?

	Very relevant	Relevant	Somewhat relevant	Not relevant	No opinion
--	---------------	----------	-------------------	--------------	------------

Support implementation of EU law in relation to assistance to child victims of sexual abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support the exchange of best practices on protection measures for victims	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Carry out research and serve as a hub of expertise on assistance to victims of child sexual abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support evidence-based policy on assistance and support to victims	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Support victims in removing their images and videos to safeguard their privacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ensure that the perspective of victims is taken into account in policymaking at EU and national level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Comments (including other possible functions to support efforts to assist victims of child sexual abuse, if any):

1000 character(s) maximum

10. Who are the potential key stakeholders in the area of victim support the possible centre should cooperate with to facilitate the exchange of best practices and research?

1000 character(s) maximum

11. What key actions could the possible centre undertake to ensure that the perspective of child victims is taken into account in policymaking at EU and national level?

1000 character(s) maximum

12. What practical actions could the possible centre take to raise awareness of children's rights and of child victims' needs?

1000 character(s) maximum

13. What good practices can you point out with regard to the potential centre's support for assistance to victims?

1000 character(s) maximum

Governance and type of organisation

14. Which stakeholders should be involved in the governance of the possible centre?

1000 character(s) maximum

Depending on the nature of the relationships and the functions of the Centre it would seem sensible to bring together representatives from all of the relevant organisations suggested in this consultation to talk through the next steps, we would suggest that this could be led by the European Commissioner for Home Affairs, the Executive Director of Europol and involve other key organisations and networks from INHOPE, INSANE, IWF, NCMEC, Thorn and other organisations working in the child trafficking, child rights and protection spheres. This Centre will also require the co-operation and collaboration of the industry if it is to be effective and they should also be involved in shaping the discussions about how they wish to engage and work with a new centre.

15. What would be the most appropriate type of organisation for the possible centre?

- EU body
- Public-private partnership
- Not for profit organisation
- Other

16. How should the possible centre be funded? (please select as many options as appropriate)

- Direct funding from the Union budget
- Mandatory levies on industry
- Voluntary contributions from industry
- Voluntary contributions from not-for-profit organisations
- Other

17. Are you aware of any organisations which you believe could serve as suitable models/references or which could provide best practices/lessons learned for the possible centre? Please specify.

1000 character(s) maximum

The European Commission needs to think carefully about how the Centre will be funded. This will largely be driven by the decisions the Commission makes about the functions of the new Centre. The Commission will need to ensure that the funding does not impact on current effective initiatives for tackling child sexual abuse and exploitation and that the fund mechanisms for those current effective mechanisms are not negatively impacted either through a levy from the industry or through pressures in the EU budget.

The Commission needs to carefully consider that if it introduces mandatory reporting for example, who will pay for a potentially very expensive system to process reports on an ongoing basis. Many of the large American technology firms, we imagine, are likely to be against a levy as they already report into NCMEC and are likely to seek assurances that this complements existing structures.

18. Other comments:

2000 character(s) maximum

We remain at the disposal of the European Commission to help shape the plans for the new Centre. We would particularly welcome the opportunity to discuss some of our technical projects which we think could be extremely useful to the aims and ambitions of the European Commission. Please do not hesitate to contact us, if this would be of interest.

If you would like to submit a document completing your answers to this consultation you can do that here.

Please upload your file

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Contact

[Contact Form](#)