Council of the European Union

Brussels, 13 May 2022
(OR. en)

9068/22
ADD 1

Interinstitutional File:
2022/0155(COD)

JAI 641
ENFOPOL 256
CRIMORG 69
IXIM 119
DATAPROTECT 149
CYBER 170
COPEN 182
FREMP 98
TELECOM 216
COMPET 332
MI 388
CONSOM 117
DIGIT 97
CODEC 690
IA 71

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	12 May 2022
To:	General Secretariat of the Council
No. Cion doc.:	SWD(2022) 209 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse

Delegations will find attached document SWD(2022) 209 final.

Encl.: SWD(2022) 209 final

EUROPEAN
COMMISSION

Brussels, 11.5.2022
SWD(2022) 209 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

{COM(2022) 209 final} - {SEC(2022) 209 final} - {SWD(2022) 210 final}

Contents

Term/Acronym	*Definition*
AI	Artificial Intelligence
API	Application Programming Interfaces
Classifiers	A form of artificial intelligence, an algorithm that sorts data into labelled classes or categories
CSA	Child Sexual Abuse
CSA online	CSA content refers to text-based exchanges, photos, videos and other material illegal under EU law (CSA Directive). In this document it refers to the three main types of abuse: known CSAM, new CSAM and grooming
CSA Directive	Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography
CSAM	Child Sexual Abuse Material, e.g. images and videos
CSEA	Child Sexual Exploitation and Abuse
Darkweb	Websites not indexed by conventional search engines, making use of masked IP addresses, which are only accessible with a special web browser
DSA	Digital Services Act Proposal for a Regulation on a Single Market for Digital Services and amending Directive 2000/31/EC, COM(2020) 825 final
E2EE	End-to-end Encryption
EECC	Directive 2018/1972/EU of 11 December 2018 establishing the European Electronic Communications Code
E-evidence	Electronic evidence: electronically stored data such as subscriber information, metadata or content data
Encryption	Process of changing electronic information or signals into a secret code or cipher
Grooming	Offenders building trust and a relationship with a child in an effort to gain access to the minor for sexual exploitation or abuse. Also known as solicitation
Hash	A unique digital code created by a mathematical algorithm ("hashing") that becomes this file's signature, or its hash value
Hotline	Child sexual abuse hotlines deal with questions about or reports of child sexual abuse. They can report content to law enforcement, take action for CSAM to be removed from the internet and act as interest groups
IP address	Internet Protocol address: a unique identifier allowing a device to send and receive packets of information; a basis for connecting to the Internet

ISCO	International Standard Classification of Occupations
Malware	Any type of software designed to disrupt the normal functioning of a computer, server, or computer network
NCMEC	National Centre for Missing and Exploited Children (US private, non-profit organisation) to which online service providers are required to report under US law instances of potential child sexual abuse that they find in their networks
OTTs	Over-the-Top communications services enable direct interpersonal and interactive exchange of information via electronic communications (i.e. the Internet), without connecting to the public telephone network
P2P	Peer-to-peer sharing describes networks in which each computer can act as a server, allowing files to be shared directly without the need for a central server
PhotoDNA	The most widely used tool based on hashing technology, available free of charge, based on a licensing agreement tailored to avoid abuse and use for any other purpose than the detection of CSA
Safety-by-design	The embedding of the rights and safety of users into the design and functionality of online products and services from the outset
SDGs	Sustainable Development Goals, a set of 17 interlinked goals established by the UN in 2015 as "a blueprint to achieve a better and more sustainable future for all people and the world by 2030"
SMEs	Enterprises that do not exceed a staff headcount of 250 people, a turnover of EUR 50M and an annual balance sheet total of EUR 43M
Trusted flagger program	A program under which an organisation designates certain persons or organisations whose reports of online CSA are trusted to meet sufficiently high standards, and may be treated differently, for example by being given higher priority for review
URL	Uniform Resource Locator, i.e. the address of an internet object (e.g. an image, a video, or an entire website)

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Children face a number of risks in their daily lives, both online and offline, from which they cannot fully protect themselves. One of these risks is that of being sexually abused during childhood. The initiative assessed here aims to complement the existing EU framework by defining the responsibilities of certain online service providers to protect children against sexual abuse. In the absence of harmonised rules at EU level, providers of social media platforms, gaming services, and other hosting and online communications services find themselves faced with divergent rules across the internal market. The proliferation of rules is increasing, with recent legislative changes in the Netherlands and Germany, and at the same time there is evidence that current efforts at national level are insufficient to successfully address the underlying problem.

Children have the fundamental right to such protection and care as is necessary for their well-being, and their best interests must be a primary consideration in all actions relating to them[1]. Consequently, the fight against child sexual abuse (CSA) is **a priority for the EU**[2]. In the July 2020 EU strategy for a more effective fight against child sexual abuse, the Commission set out **eight concrete actions,** implementing and developing the right legal framework and catalysing multi-stakeholder efforts in relation to **prevention** and **investigation** of these crimes and **assistance to victims and survivors.**

The legislative proposal that this impact assessment accompanies responds to the commitment undertaken in the strategy to propose the **necessary legislation to tackle child sexual abuse effectively**, **online and offline**[3]. In particular, this initiative:

1. sets out **obligations to detect, report and remove child sexual abuse online** to bring more clarity and certainty to the work of both law enforcement and relevant actors in the private sector to tackle online abuse[4]; and
2. establishes an **EU Centre to prevent and counter child sexual abuse** to provide comprehensive support for the implementation of the proposed Regulation by service providers and to Member States, in the fight against child sexual abuse[5].

The commitment and this initiative respond to the **calls for action** from the **Council, the European Parliament**, and the **European Economic and Social Committee**[6], and

---

1 EU Charter of Fundamental Rights, Art. 24(1) and (2).

2 EU strategy for a more effective fight against child sexual abuse, COM (2020) 607, 24 July 2020, p.2.

3 *Ibid*, p. 6.

4 *Ibid*, p. 5.

5 *Ibid*, p. 12. This initiative is the outcome of the commitment in the strategy to start working towards the possible creation of an EU Centre to prevent and counter child sexual abuse.

6 European Parliament resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child (2019/2876(RSP)); Council conclusions on combatting the sexual abuse of children of 8 October 2019, No. 12862/19; European Economic and Social Committee, Combatting child sexual abuse online, TEN/721 COM (2020) 568 final 2020/0259 COD, 29 October 2020.

globally in multiple forums[7], including by online service providers[8] and in the media[9], as it has become evident that current measures are falling short of effectively protecting the right of children to live free from sexual violence. This initiative is therefore **expected,** as the need to better prevent and combat child sexual abuse through additional legislation was **already clear** during the preparation of the 2020 strategy, and also during the inter-institutional negotiations of the Interim Regulation (see below).

The initiative aims to build on and complement the **existing policy instruments** in the fight against CSA, which can be grouped into legislation, coordination and funding[10].

1. Legislation

The existing legal framework consists of measures in the areas of criminal law, protection of privacy and personal data, and the internal market, regulating online and telecommunications services and content moderation. It includes:

- **horizontal instruments** in the area of data protection and online privacy (e.g. GDPR[11] and e-Privacy Directive[12] and its proposed revision[13]), and of the single market for digital services (e.g. e-Commerce Directive[14] and the proposed Digital Services Act[15]),
- **sector-specific** legislation, such as the Child Sexual Abuse Directive[16], the Europol Regulation[17] and its proposed revision[18], the Interim Regulation

---

7 E.g. at the December 2019 summit of the WePROTECT Global Alliance to End Child Sexual Exploitation Online , or by the "Five Eyes" (US, UK, Canada, Australia and New Zealand) in July 2019.

8 See for example a call for clear legal frameworks to deal with harmful content by Facebook, Referring Former President Trump's Suspension From Facebook to the Oversight Board, blog post by Nick Clegg, VP of Global Affairs, 21 January 2021.

9 See, for example, the series of New York Times articles published from September 2019 to February 2020, which exposed to the public, the depth and complexity of the problem.

10 Annex 5 contains additional information on relevant legislation and policy.

11 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation'), *OJ L* 119, 4.5.2016.

12 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications'), *OJ L* 201, 31.7.2002.

13 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

14 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000.

15 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC of 15 December 2020, COM/2020/825 final.

16 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *OJ L* 335, 17.12.2011.

17 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

18 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by

derogating from the application of certain rights and obligations under the ePrivacy Directive[19], and the Victims' Rights Directive[20].

Horizontal instruments

The General Data Protection Regulation (GDPR)

- **What it does**: the GDPR sets out rules on the processing of personal data relating to individuals, specifying the fundamental right to protection of personal data.
- How CSA-related **responsibilities** are distributed between **EU and Member States:** as a horizontal instrument, the GDPR does not contain CSA-specific provisions, but it applies to all activities of processing personal data, including those related to CSA, except for those carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, which are covered by Directive 2016/680/EU[21]. Member States are notably responsible for **enforcement** through their data protection authorities, and the European Data Protection Board (EDPB) is tasked with the consistent application of the GDPR.
- How the proposed legislation **builds on and interacts** with the GDPR: the proposed legislation builds on the GDPR, including its Article 6 which allows, e.g., processing of personal data to comply with a legal obligation (Art. 6(1)(c)), or when processing is necessary for the purpose of legitimate interest (Art. 6(1)(f)).

The ePrivacy Directive and its proposed revision

- **What it does**: the ePrivacy Directive and the proposed Regulation for its revision harmonise national rules to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality of communications, with respect to the **processing of personal data** in electronic communications services. These ePrivacy rules particularise and complement the GDPR.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: as horizontal instruments, the ePrivacy Directive and the proposed successor Regulation do not contain CSA-specific provisions; they apply to any processing of specified data categories in electronic communications. Member States are responsible for **enforcement** through their competent national authorities.

Europol in support of criminal investigations, and Europol's role on research and innovation of 9 December 2020, COM/2020/796 final.

19 Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, OJ L 274, 30.7.2021, p. 41–51

20 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, *OJ L* 315, 14.11.2012.

21 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

- How the proposed legislation **builds on and interacts** with the ePrivacy Directive and its proposed revision: the proposed legislation would limit the scope of certain rights and obligations which are currently in the ePrivacy Directive, notably those on the confidentiality of communications and related data in order to enable companies to identify child sexual abuse taking place on their systems after the issuance of a detection order, subject to strict safeguards.

The eCommerce Directive

- **What it does**: the eCommerce Directive sets out a framework for the provision of information society services in the internal market. One of its key principles is a conditional liability exemption framework for providers of specific categories of information society services. In principle, providers may not be held liable for information (including illegal content) that they host (store), cache (temporarily store) or transmit during the provision of their services, subject to the conditions laid down in the Directive. For example, this means that providers of hosting services may not be held liable for information they host, unless they gain actual knowledge or awareness of the illegality and fail to act expeditiously. The Directive also prohibits Member States from imposing general obligations to monitor their services or to actively seek facts or circumstances indicating illegal activity. The eCommerce Directive does **not establish a legal basis** for any **processing of personal data**.
- How CSA-related **responsibilities** are distributed between **EU and Member States:** as a horizontal instrument, the eCommerce Directive does not contain CSA-specific provisions. It governs activities of relevant service providers. Member States are responsible for **enforcement** through their national authorities.
- How the proposed legislation **builds on and interacts** with the eCommerce Directive: the proposed legislation imposes narrowly targeted obligations to detect, report and remove child sexual abuse online, based on specific indicators and requirements to ensure compatibility with the eCommerce Directive (see box 9).

The Digital Services Act proposal

- **What it does**: the Digital Services Act (DSA) proposal, if adopted as proposed, and building upon the eCommerce Directive's framework, would provide a **horizontal standard for content moderation** by providers of **intermediary services**. It would remove a number of disincentives for providers' voluntary efforts to detect, remove or disable access to illegal content (including child sexual abuse material, CSAM) and would create obligations for them to provide information on their content moderation efforts when requested by national authorities. The DSA would also create additional due diligence obligations tailored to specific categories of providers of intermediary services (e.g. hosting services, online platforms, very large online platforms) as well as transparency reporting obligations. For instance, it would require hosting services to put in place notice and action mechanisms enabling any user or entity to notify them of the presence of suspected illegal content. Furthermore, the DSA would oblige very large online platforms to implement risk mitigation measures on their services. The DSA would also establish rules on its implementation and enforcement, including as regards the cooperation of and coordination between

the competent authorities. The DSA would **not establish a legal basis** for any **processing of personal data**.

- How CSA-related **responsibilities** are distributed between **EU and Member States:** as a horizontal instrument covering all types of illegal content, the DSA does not contain CSA-specific provisions. The DSA would create a framework at EU level for the notification of materials noticed by users to companies, with obligations for companies to respond to orders issued by public authorities in Member States, as well as additional due diligence requirements for very large platforms. For the very large platforms, a stronger role for the Commission in the enforcement process is also being considered during the ongoing inter-institutional negotiations at the time of writing.
- How the proposed legislation **builds on and interacts** with the DSA as proposed: the proposed legislation complements the DSA notably by specifying mandatory removal of CSAM when ordered and a comprehensive reporting obligation tailored to the specificities of CSA online, which often takes place hidden from public view and demands specific follow-up where identified. These specificities require a different approach from the horizontal one of the DSA. Finally, as the DSA aims to maintain some of the main principles of the eCommerce Directive, including the prohibition of general monitoring obligation and the unavailability of the liability exemption for hosting services if failing to act after obtaining actual knowledge or aware of the illegality of the content, the considerations above made for the eCommerce Directive also apply to the DSA.

The Victims' Rights Directive

- **What it does:** the Victims' Rights Directive establishes minimum standards on the rights of, support for and protection of victims of crime and ensures that they are recognised and treated with respect. They must also be granted access to justice.
- How CSA-related **responsibilities** are distributed between the **EU and Member States**: as a horizontal instrument, the Victims' Rights Directive, applicable to all victims of crime, does not contain CSA-specific provisions. The EU adopted specific rules for victims of child sexual abuse and sexual exploitation under the Child Sexual Abuse Directive (see below), to respond more directly to the specific needs of those victims.
- How the proposed legislation **builds on and interacts** with the Victims' Rights Directive: whilst the proposed legislation focuses on strengthening the functioning of the internal market by setting common rules aimed at preventing and combating the misuse of online services for CSA-related purposes, it could also help support and facilitate the work of Member States on assistance to victims of CSA, notably through the creation of the EU Centre to prevent and counter CSA, which would facilitate research and the exchange of best practices among Member States. The proposed legislation does not create new obligations for Member States in this respect.

Sector-specific legislation

The Child Sexual Abuse Directive

- **What it does**: the **Child Sexual Abuse (CSA) Directive's** main objective is to harmonise minimum criminal law rules at EU level concerning the definitions of child sexual abuse and exploitation offences and corresponding sanctions and to require the establishment of prevention measures in this area. It also requires Member States to ensure the provision of assistance and support to victims before, during and after the conclusion of criminal proceedings. In terms of websites disseminating CSAM, the Directive requires Member States to take necessary measures to ensure the prompt removal of webpages hosted in their territory and to endeavour to obtain the removal of such pages hosted outside their territory. It also enables Member States to take voluntary measures to block access to web pages containing or disseminating CSAM within their territory, while providing safeguards (restriction is limited to what is necessary and proportionate; users are informed of the reason for the restriction and of the possibility of judicial redress). The Child Sexual Abuse Directive does not establish a legal basis for any processing of personal data.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: the Directive defines a minimum set of standards at EU level to define and sanction these crimes, prevent them and assist victims. Member States are required to comply with these minimum rules and may go beyond them if they consider it necessary. Similarly, the Directive defines the responsibilities of Member States but leaves to national authorities to comply with those responsibilities in the way that suits best the national specificities (e.g. on prevention programmes).
- How the proposed legislation **builds on and interacts** with the Child Sexual Abuse Directive: the former is intended to reinforce and complement the latter without creating unnecessary overlaps. Whereas the Directive focuses on defining the roles and responsibilities of Member States' authorities in the fight against CSA using the tools of criminal law, the proposed legislation focuses, from an internal market angle, on defining the roles and responsibilities of private companies offering their services in the Single Market, notably concerning the detection, reporting and removal of CSA online. Nonetheless, the proposed legislation could help **support and facilitate** the efforts by Member States to meet the obligations defined in the CSA Directive relating to prevention and assistance to victims, notably through the creation of the EU Centre to prevent and combat CSA.

  The proposed initiative cannot address remaining implementation issues with the Directive. A study has been launched to prepare the evaluation of the CSA Directive and at the moment there are ongoing infringement procedures against 21 Member States. The majority of the challenges Member States face in the implementation concern offline prevention measures (in particular prevention programmes for offenders and for people who fear that they might offend) and criminal law definitions. Exchanges between the Commission and Member States are ongoing to ensure that they swiftly address these remaining issues. The Commission has also organised dedicated expert workshops with Member States to facilitate the exchange of lessons learned and of best practices in national experiences in the implementation of the CSA Directive. That said, the present

legislative initiative could indirectly have a positive effect on the implementation of the Directive, in particular through the EU Centre as an expert hub and facilitator of exchanges of knowledge and best practices.

The "Interim Regulation"

- **What** it does: voluntary detection of CSAM and grooming in certain online communication services like instant messenger and email has been made subject, as of 21 December 2020, to comply with the ePrivacy Directive's rules on confidentiality of communications, due to changes in the definitions of the European Electronic Communications Code becoming effective and those services consequently fell under the ePrivacy Directive. To address this issue, the Commission proposed a **temporary** derogation from the application of certain rights and obligations under the **ePrivacy Directive**, for the sole purpose of detecting and reporting CSA and removing CSAM. The Interim Regulation[22], which entered into force on 2 August 2021, enables those services to continue such practices on a voluntary basis, provided those practices are lawful and, in particular, meet a range of conditions. The Regulation ceases to apply **three years after its entry into force**. The Interim Regulation does not establish a legal basis for any processing of personal data.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: the Commission is responsible for making a list of names and organisations acting in the public interest against CSA to which providers report CSA online, for requesting the European Data Protection Board (EDPB) to issue guidelines for the purpose of assisting the supervisory authorities in assessing whether processing falling within the scope of the Regulation complies with the GDPR, and for preparing a report on the implementation of the Regulation. Member States are notably responsible for enforcing the Regulation and for statistics related to the detection, reporting and follow up of the CSA reports.
- How the proposed legislation **builds on and interacts** with the Interim Regulation: the proposed legislation replaces the Interim Regulation, and uses it as a reference to present a long-term framework that maintains some of its elements and covers a wider range of services, including private communications.

The Europol Regulation and its proposed revision

- **What it does**: the **Europol Regulation** sets out the mandate of the European Union's law enforcement agency, which is to support and strengthen action by competent authorities of the Member States and their mutual cooperation including in preventing and combating serious forms of crime, such as sexual abuse and sexual exploitation. Among other tasks, Europol's current mandate allows the agency to collect, store, process, analyse and exchange information, including criminal intelligence; to notify the Member States of any information and connections between criminal offences concerning them and to coordinate, organise and implement investigative and operational actions to support and

[22] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

strengthen actions by the competent authorities of the Member States. The proposed revision of Europol's mandate would notably allow it to receive data from private parties directly, subject to certain conditions.

- How CSA-related **responsibilities** are distributed between **EU and Member States**. Europol can support Member States' actions in preventing and combating CSA crimes. In particular, Europol receives reports from online service providers via the US National Centre for Missing and Exploited Children (NCMEC) for 19 Member States[23], completes these reports with its own information (if any) and forwards them to the Member States' authorities.
- How the proposed legislation **builds on and interacts** with the Europol Regulation and its proposed revision. The proposed legislation creates an EU Centre to prevent and counter CSA, which will work closely with Europol. The Centre will receive the reports from online service providers, check that they are likely to be actionable, i.e. they are not manifestly unfounded and can thus in principle be acted upon, and forward them to Europol so that it can enrich the reports with additional criminal intelligence, as well as to national law enforcement agencies. This would ensure that Europol and national law enforcement resources are focused on key investigative tasks such as swiftly rescuing victims from ongoing abuse, rather than on e.g. filtering out the reports that are not relevant. The revised Europol mandate would complement the proposed legislation in particular on the ability for Europol to receive and process reports from the EU Centre originating from online service providers.

2. Coordination

The existing legal framework is complemented by practical efforts at EU level to step up the fight against CSA in all areas: investigations, prevention, and assistance to victims.

EU level cooperation in investigations

- **What it does**: **Europol** provides EU level coordination for investigation of cross-border cases. In addition, the **EU policy cycle (EMPACT)**[24] serves to coordinate the operational priorities of Member States' law enforcement authorities in the area of combating CSA, to organise joint operations and strategic approaches to specific phenomena from a law enforcement perspective. Europol also helps coordinate investigations involving law enforcement agencies in third countries and in the Member States.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: Europol supports operational action by law enforcement agencies in Member States at their request. Europol does not have executive powers (i.e. it is not a "European FBI").
- How the proposed legislation **builds on and interacts** with existing EU level cooperation in investigations: the proposed legislation aims to support the existing cooperation in investigations by ensuring that the reports from online service providers that reach Europol and national law enforcement agencies are actionable and relevant. The EU Centre would not have any operational capability

[23] The rest of Member States have chosen to receive the information directly from NCMEC due to e.g. their national data retention regimes, which require extremely swift action.

[24] More information can be found here.

on investigations, but would support them indirectly by **facilitating** the process of detection, reporting and removal of CSA online by service providers.

EU level cooperation in prevention

- **What it does**: at the moment, EU level cooperation in prevention of CSA is fragmented and limited to ad hoc expert meetings organised by the Commission to support Member States in the implementation of the CSA Directive, initiatives on awareness raising under EMPACT and Europol. The 2020 CSA Strategy aimed to boost EU level efforts on prevention by making it one of its pillars. Specifically, the Strategy included the **EU Centre** to prevent and counter CSA, which will also carry out certain tasks relating to prevention. The Strategy also announced the launch of a **prevention network** of practitioners and researchers to support the EU Member States in putting in place usable, rigorously evaluated and effective prevention measures to decrease prevalence of child sexual abuse in the EU. The network will aim to give structure and regularity to exchanges of knowledge and best practices between Member States.
- How CSA-related **responsibilities** are distributed between **EU and Member States.** The CSA Directive requires Member States to implement provisions while leaving it to them to determine exactly what these measures or programmes are. The degree to which the requirements of the Directive are fulfilled vary among the Member States (see section 2.2.3.).
- How the proposed legislation **builds on and interacts** with existing EU level cooperation in prevention. The proposed legislation will establish the EU Centre, which will be the driving force of the work relating to preventing and combating CSA at EU level. Whilst the Centre would principally focus on its tasks set out in the envisaged legislation connected to the common rules for online service providers to combat CSA online, the Centre could also contribute to and facilitate Member States' work relating to prevention, for instance through the involvement of multiple stakeholders and the sharing of best practices and lessons learned across Member States. The proposed legislation will not create new obligations for Member States on prevention.

EU level cooperation in assistance to victims

- **What it does**: EU level cooperation in assistance to victims takes place currently through the Victims' Rights Platform[25], which deals with **horizontal** issues relevant for victims' rights. The platform brings together representatives of EU level networks, agencies, bodies and civil society organisations relevant for the implementation of the EU Strategy on victims' rights.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: the platform facilitates the implementation of the EU strategy on victims' rights, which details key actions for the European Commission and for Member States. Also, the CSA Directive requires Member States to implement provisions related to assistance to victims, while leaving it to them to determine exactly what these measures are. The degree to which the requirements of the Directive are fulfilled varies among the Member States (see section 2.2.3.).

[25] More information is available here.

- How the proposed legislation **builds on and interacts** with existing EU level cooperation in assistance to victims: apart from its main tasks in the process of combating CSA online, the EU Centre could also facilitate and support Member States action in assistance to victims of CSA, specifically by serving as a hub of expertise to support evidence-based policy development, help develop research on assistance to victims, including victims' needs and the effectiveness of short-term and long-term assistance programmes. The Centre will also support victims, at their request, in having their images and videos taken down by assisting them in exchanges with the relevant online service providers. The EU Centre could participate in the Victims' Rights Platform to contribute to the discussion of horizontal issues concerning victims and to the implementation of the EU strategy on victims' rights. The proposed legislation will not create new obligations for Member States on assistance to victims.

Multi-stakeholder cooperation at EU and global level

- **What it does**: at **EU level**, the Commission facilitates multi-stakeholder cooperation between service providers and national authorities in the fight against CSA online through the **EU Internet Forum**[26], which brings together online service providers and ministers of interior of all Member States.
  At **global level**, the Commission continues to contribute to **increasing voluntary standards** for the protection of children against sexual abuse by promoting multi-stakeholder cooperation, through the **WeProtect Global Alliance to End Child Sexual Exploitation Online** (WPGA)[27].
- How CSA-related **responsibilities** are distributed between **EU and Member States**: at EU level, the Commission organises the EU Internet Forum, in which Member States participate at ministerial level (once a year), and at various levels in the technical discussions. Depending on the initiative, Member States and/or the Commission may be responsible for the execution.
  At global level, the Commission participates in the policy board of the WPGA, as one of its founding members. Member States are WPGA members and notably participate in its biannual global summit (the next one will take place in Brussels in June 2022 and will be co-hosted by the Commission and the French Presidency of the Council of the EU).
- How the proposed legislation **builds on and interacts** with existing multi-stakeholder cooperation at EU and global level: the proposed legislation builds on the experience of the EU Internet Forum and the WPGA and aims to boost multi-stakeholder cooperation in the EU and globally in the fight against CSA, through the EU Centre. The Centre will be an independent **facilitator** that will bring together all the relevant actors in the EU and beyond in any aspect of the fight against CSA, including investigations, prevention and assistance to victims, to ultimately facilitate and support Member States' action in those areas. The Centre will have a more operational focus than the EU Internet Forum and the WPGA,

[26] More information is available here.

[27] The We Protect Global Alliance to End Child Sexual Exploitation Online is a not-for-profit organisation resulting from the merger between UK-led We Protect and the Global Alliance Against Child Sexual Abuse Online launched by the Commission in 2012. Its aim is to raise standards and to foster a stronger and more coherent response around the globe and across stakeholder groups. It includes 98 countries, 45 companies and 65 civil society organisations and international institutions.

which are centred on policy and are not designed to play a role in facilitating day-to-day efforts on the ground.

3. Funding

- **What it does**: the 2020 strategy includes a commitment to continue providing funding for fighting child sexual abuse, e.g. to support the development of national capacities to keep up with technological developments. The Commission has organised regular calls for project proposals to fight the online and offline aspects of child sexual abuse, with a total value of 61 million euro in the last 10 years (funded under Horizon2020 and Internal Security Fund[28]). Notable examples of EU-funded projects include:
  - The **INHOPE network of hotlines**, where users can report child sexual abuse materials they encounter online (formerly funded through the Connecting Europe Facility programme, and currently under the DIGITAL Europe programme). The content is analysed, and if assessed as illegal, hotlines notify the relevant online service providers requesting the swift removal of the content, and report the case to the relevant law enforcement agency for victim identification purposes. National hotlines are an important element of implementation of Article 25 of the CSA Directive, as a majority of Member States has chosen to implement most of this article through the hotlines. As of January 2022, the INHOPE network consists of 46 hotlines in 42 countries (including all Member States except Slovakia);
  - The **International Child Sexual Exploitation** (ICSE) database at Interpol, which is an important tool enabling law enforcement to identify victims globally. The database has helped identify 23,564 victims worldwide at the time of writing[29].

  The Commission has also financially supported the adoption of the *Barnahus* model of child-friendly, multidisciplinary protection of child victims during criminal proceedings, which includes limiting the number of interviews of child victims and conducting them by trained experts, as a standard in the EU.
- How CSA-related **responsibilities** are distributed between **EU and Member States**: the Commission manages the funding instruments mentioned above. That said, part of the Internal Security Fund is managed by Member States under the supervision of the Commission, and Member States also contribute own funding to the efforts, to a varying extent.
- How the proposed legislation **builds on and interacts** with existing funding mechanisms: the creation of the EU Centre requires dedicated EU funding, and no changes will be made to existing funding mechanisms. However, increased coordination and cooperation in prevention efforts facilitated by the EU Centre may also result in more targeted and higher-quality proposals during future funding rounds.

---

[28] The latest open call for proposals of 16M EUR to prevent, assist victims, and combat child sexual abuse was launched on 16 December 2021, with a deadline for submission of proposals until 24 February 2022.

[29] Interpol, International Child Sexual Exploitation database, accessed in January 2022.

Relevant Sustainable Development Goals (SDGs)

The most relevant SDGs for this initiative are 5.2., eliminate all forms of violence against women and girls, and 16.2., end abuse, exploitation, trafficking and all forms of violence against children.

Other SDGs of particular relevance are those that address risk factors of CSA, such as SDG 1 on poverty (e.g. children forced by their parents to be sexually abused online), SDG 3 on health (e.g. given the short and long-term negative health consequences of CSA on children), SDG 4 on education (e.g. prevention campaigns to raise awareness of CSA online risks), and SDG 9 on industry, innovation and infrastructure (e.g. as the initiative aims to support service providers efforts to fight against CSA online, including through the EU Centre).

2. PROBLEM DEFINITION

Table 1 shows the intervention logic (problem, drivers, objectives and options) that will be described and analysed in the impact assessment:

Table 1: problem, problem drivers, objectives and options (intervention logic)

Problem	Problem drivers	General objective	Specific objectives	Options				
				Non-legislative	Legislative			
				A	B	C	D	E
Some child sexual abuse crimes are **not adequately addressed** in the EU due to challenges in their **detection, reporting and action** by relevant services providers, as well as **insufficient prevention** and **assistance to victims.** Diverging national responses negatively affect the **Internal Market**	1. **Voluntary action** by online service providers to detect online child sexual abuse **has proven insufficient** 2. **Inefficiencies** in **public-private cooperation** between online service providers, civil society organisations and public authorities hamper an effective fight against child sexual abuse 3. Member States' efforts to **prevent** child sexual abuse and to **assist victims** are **limited**, **divergent** and **lack coordination** and are of **unclear effectiveness**	Improve the functioning of the Internal Market by introducing **clear, uniform and balanced EU rules** to **prevent** and **combat** child sexual abuse	1. Ensure the effective **detection, removal and reporting** of online child sexual abuse where they are **currently missing** 2. Improve **legal certainty, transparency and accountability** and ensure **protection of fundamental rights** 3. Reduce the **proliferation and effects** of child sexual abuse through harmonisation of rules and **increased coordination** of efforts	**Practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims**, and establishing an **EU Centre** on **prevention and assistance to victims**	Option A + legislation 1) specifying the conditions for **voluntary detection**, 2) requiring **mandatory reporting** and **removal** of online child sexual abuse, 3) expanding the **EU Centre** to also support **detection, reporting and removal**	Option B + **mandatory detection** of **known** child sexual abuse material	Option C + **mandatory detection** of **new** child sexual abuse material	Option D + **mandatory detection** of '**grooming**' (solicitation of children)

2.1. What is the problem?

2.1.1. Definition and magnitude

The problem that this initiative tackles is that providers of certain online services offered in the EU face divergent rules at national level when it comes to their responsibility for preventing and combating child sexual abuse on their services. At the same time, the existing responses at national level to some child sexual abuse[30] crimes are proving insufficient. Challenges persist in **detection, reporting and action** by relevant service providers, as well as **insufficient prevention, assistance to victims and cooperation**. The divergence of national responses to the problem creates **legal fragmentation** which negatively affects the **Internal Market.**

Prevalence

At least **one in five** children falls victim to sexual violence during childhood[31]. A global study of childhood experiences in 2021 found that than **one in three** respondents (34%) had been asked to do something sexually explicit online during their childhood, and **more than half** (54%) had experience a form of child sexual abuse online[32]. A recent survey in Spain concluded that **two out five** Spanish adults suffered sexual abuse when they were children[33].

The majority of victims are girls, who are **more than twice** as likely to be abused than boys[34].

Vulnerable children are more likely to fall victims of CSA online. In a recent survey about childhood experiences:

- 59% of respondents who identified as **transgender and non-binary** experienced online sexual harm, compared to 47% of cisgender respondents;
- 65% of respondents who identified as **LGBQ+** experienced online sexual harm, compared to 46% non-LGBQ+ people;
- 57% of **disabled respondents** experienced online sexual harm, compared to 48% of non-disabled respondents.

---

30 This document refers to child sexual abuse for simplicity but it should be understood as covering also child sexual exploitation and child sexual abuse material.

31 One in Five Campaign, Council of Europe, 2010-2015.

32 Economist Impact survey of more than 5,000 18 to 20 year olds in 54 countries, published in the 2021 Global Threat Assessment, WeProtect Global Alliance, 2021. The forms of child sexual abuse online surveyed (referred as "online harms") include 1) Being sent sexually-explicit content from an adult or someone they did not know before they were 18; 2) Being asked to keep part of their sexually-explicit online relationship with an adult / or someone they did not know before a secret; 3) Having sexually-explicit images of them shared without consent (by a peer, adult, or someone they did not know before); and 4) Being asked to do something sexually-explicit online they were uncomfortable with (by a peer, adult, or someone they did not know before).

33 M. Ferragut, M. Ortiz-Tallo, M. J Blanca. Prevalence of Child Sexual Abuse in Spain: A Representative Sample Study. Journal of Interpersonal Violence, 21 September 2021.

34 Collin-Vézina, D., et al., Lessons learned from child sexual abuse research: Prevalence, outcomes, and preventive strategies, 18 July 2012, p. 6. See also M. Stoltenborgh, M.H. van IJzendoorn, E.M.Euser, M.J. Bakermans-Kranenburg, A global perspective on child sexual abuse: Meta-analysis of prevalence around the world, 2011, pp. 79-101.

"Offline" and online CSA

The sexual abuse of children can take multiple forms, **both offline** (e.g. engaging in sexual activities with a child or exploiting a child for prostitution) and **online** (e.g. forcing a child to engage in sexual activities via live streaming, or viewing or distributing online child sexual abuse images and videos).

The **offline** and **online** aspects of the crimes have become increasingly intertwined, and most CSA cases today contain **an online component**[35]. For example, an offender may abuse a child offline, record the abuse, and share it online. Or the offender may establish a first contact with children online and then lure them to meet offline and sexually abuse them[36]. It is therefore not possible to separate categorically between online and offline.

That said, this initiative focuses on the online aspects of the crime with relation to **detection, reporting and removal** efforts, in particular by the providers of the services used. This is because the internet has become the main medium for sharing CSAM, as well as for contacting children with the aim of abusing them. The internet facilitates the creation of communities in which offenders share materials and experiences. The volume of CSAM shared online has grown exponentially in the last years, while sharing of such material offline, e.g. via mail services, remains at a very low level and was not signalled as a common issue encountered by law enforcement in CSA investigations during stakeholder consultations.

The Member States have sought to address this growing phenomenon through rules at the national level, reinforcing existing legislation or adopting new rules to improve the detection and follow-up on online child sexual abuse. This has inadvertently created a fragmentation of the internal market which negatively impacts the provision of certain online services, while at the same time failing to stem the proliferation of this particularly harmful content. Therefore, this initiative addresses the **detection, reporting and removal** in the **online** sphere, which enables and fuels **offline and online abuse**, as well as on **prevention and assistance to victims**, where the **online and offline** aspects are also closely related.

Interlinkages between detection, reporting and action, prevention, and assistance to victims

In addition to the online-offline interlinkages, all the different areas of the problem are also **closely related**: **detection, reporting and action** (i.e. follow up to the reports, including removal by service providers and action by law enforcement)**, prevention, and assistance to victims**. In general, for public authorities to be able to act and assist the victim, the crime has to be detected and reported, which in turn may prevent future crimes from happening (e.g. if the offender is arrested and the victim is rescued). This also applies to detecting grooming and to stopping the circulation of CSAM (known and new), which are both criminal behaviours. In addition, the continued circulation of CSAM has a particularly harmful societal impact: the distribution of CSAM is a form of re-victimisation that occurs every time the images and videos are seen. The knowledge that the images and videos are being distributed is a continuous source of distress for victims. In addition, viewing of CSAM can lead to hands-on abuse as it supports potential offenders in normalising and rationalising their behaviour; recent surveys even indicate that this may often be the case[37]. When CSAM is detected by service providers and investigated by law enforcement, it frequently leads to stopping

[35] Two thirds of law enforcement authorities surveyed indicate that over 70% of child sexual abuse cases have an online component (see the targeted survey of law enforcement authorities, Annex 2).

[36] ECPAT, Summary Paper on Child Sexual Exploitation, November 2020, p. 6.

[37] Protect Children, CSAM Users in the Dark Web: Protecting Children Through Prevention, 2021.

ongoing or future abuse of child victims by the offenders caught distributing CSAM and/or grooming the child (see box 1 below).

Box 1: importance of detection, reporting and action in prevention and assistance to victims

The distribution of CSAM is closely linked to its **production**, and therefore physical sexual abuse of children. The detection and reporting of CSAM is therefore a key **prevention tool** and an important way **to assist victims** by also preventing re-victimisation.

The detection of CSA online frequently leads to **stopping ongoing or future physical sexual abuse**. This is clearly the case for new CSAM and grooming, which often reveals ongoing and/or imminent physical sexual abuse. But it is also the case for known CSAM, as viewing it often leads to hands-on abuse. In an anonymous online survey in the Darkweb, 37% of individuals who viewed CSAM had sought direct contact with a child **after viewing the material**[38]**.** Also, half of the offenders sentenced in the US in 2019 for CSAM related offences (non-production) engaged in aggravating sexual conduct prior to, or concurrently with, the CSAM charge[39]. The detection of CSAM also stops its **distribution**, which **fuels demand for more and new material** and therefore **new abuses**. Offenders not only exchange CSAM bilaterally but are typically required to contribute with new material to join online communities trading it. 44% of offenders convicted in the US for CSAM-related offences (non-production) participated in an online community, 77% required sentencing enhancements for possession of 600 or more images[40]. The material demanded has become more and more extreme. In the same 2019 US data, 52% of cases included images or videos of infants or toddlers and 84% of cases required sentencing enhancements for images depicting sadistic or masochistic conduct or abuse of an infant or toddler.

Detection, reporting and action

The proportion of cases where CSA is **discovered in a timely manner** and prevented or stopped **is very limited**. Oftentimes, children do not manage to seek help themselves, and those in their 'circle of trust' (i.e. family and other close contacts), in charge to provide protection and care, are often the abusers[41]. **One in three victims will never tell anyone** and at least **four in five** CSA cases are not reported to public authorities[42]. There are indications that the **COVID-19** crisis has exacerbated the problem[43], especially for children who live with their abusers[44].

In this context, **online service providers** and in particular 'online intermediaries'[45] such as messaging services, online forums, and online platforms (such as video-sharing and media-sharing platforms, social networks, etc.) have acquired an **important role**.

---

38 Protect Children, CSAM Users in the Dark Web: Protecting Children Through Prevention, 2021.

39 United States Sentencing Commission, Federal Sentencing of Child Pornography (non-production offences), June 2021.

40 *Ibid*.

41 Gewirtz-Meydan, A., Finkelhor, D., Sexual Abuse and Assault in a Large National Sample of Children and Adolescents, 16 September 2019.

42 *Ibid.* See also M. Ferragut, M. Ortiz-Tallo, M. J Blanca. Prevalence of Child Sexual Abuse in Spain: A Representative Sample Study. Journal of Interpersonal Violence, 21 September 2021, which found that only 27.5 % of Spanish adult victims of CSA have told someone about their experience while still a child.

43 Europol report on online child sexual abuse during the pandemic, 19 June 2020.

44 Unicef et al. COVID-19 and its implications for protecting children online, April 2020.

45 See also the Impact Assessment accompanying the Proposal on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, SWD(2020) 348 final, December 2020, p.7 (para 15).

First, online intermediaries are often the only ones to have any **possibility to detect** the ongoing abuse. Frequently, the abuse is **only discovered** thanks to the efforts of **online service providers** to detect CSAM on their services, and to protect children from being approached by predators online. The key role of these reports is evidenced by the fact that in some Member States, up to **80%** of investigations are launched due to reports from service providers[46]. This is particularly the case in electronic (private individual or group) communications, which offenders frequently use to exchange CSAM and approach children, where the service provider is **the only one** that can detect the abuse. It is reflected in recent statistics showing that the vast majority of reports (more than 80% in 2020, up from 69% in 2019) originate in interpersonal communication services (e.g. messenger applications and email)[47], and surveys. In a recent one, two-thirds of respondents who received sexually explicit material online as children from an adult they knew or someone they did not know, received it through a **private messaging service** (68%), most commonly on their own personal mobile device (62%)[48].

Secondly, the **internet** has also given offenders a new way of **approaching children**. They contact children on social media, gaming platforms and chats and **lure them** into producing compromising images of themselves or into offline meetings. In addition, children are **spending more time online than ever before**[49], increasing the risk of coming into contact with **online predators**[50].

Third, offenders frequently record the sexual abuse for repeat viewing and sharing. Where CSAM is shared online, the harm is **perpetuated**. The exponential development of the digital world has facilitated the global sharing of materials and the creation of networks of offenders via online intermediaries. The images and videos of CSA **continue to circulate** long after the abuse itself, and survivors often find themselves powerless to ensure removal of online content depicting their abuse[51]. In some cases, offenders continue to traumatise victims long after the abuse has taken place by creating fake accounts with the actual names of the victims. These accounts typically do not contain illegal content but they attract offenders familiar with the CSAM depicting those victims, who discuss the past abuse and the current personal information of the victims (e.g. where they live, work or family situation)[52].

It is estimated that, at any given moment, across the world there are more than **750 000 individuals online** exchanging CSAM, streaming live abuse of children, extorting children to produce sexual material or grooming children for future sexual abuse[53].

The problem and problem drivers considered in the impact assessment apply to the three main types of abuse: known CSAM, new CSAM and grooming, also referred to as a whole as **CSA online**.

---

46 Targeted survey of law enforcement authorities (see annex 2, section 1).

47 NCMEC, 2019 and 2020 data.

48 Economist Impact, WeProtect Global Alliance Global Threat Assessment, 2021.

49 Europol, European Union serious and organised crime threat assessment, 12 April 2021.

50 UNSW Sydney, The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing, May 2021.

51 NCMEC, Captured on Film, 2019.

52 WeProtect Global Alliance, Global Threat Assessment 2021.

53 U.N. General Assembly, Human Rights Council, Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, 13 July 2009.

Box 2: current system to detect and report CSA online in the EU

The CSA detection efforts of online service providers fall into three categories: first, the detection of **'known' CSAM**, that is, images and videos that have been reported or detected before and that have already been verified as constituting CSAM; secondly, the detection of **'new' CSAM**, i.e. images and videos that have not previously been detected and verified; and third, the detection of **'grooming'** (also referred to as solicitation of children), where offenders trick or threaten children into sharing compromising images or meeting them offline for the purposes of sexual abuse[54].

Currently, EU legislation allows certain online communication services like instant messenger and email to continue **voluntary measures** to detect and report child sexual abuse online, provided that their activities are lawful and, in particular, meet a set of specific conditions[55]. In general, the measures that providers take vary widely and proactive detection of CSA online is still a rarity among service providers active in the EU.

The vast majority of CSA reports from service providers reaches law enforcement authorities in the EU through the US National Centre for Missing and Exploited Children (**NCMEC**)[56], which is therefore of **key importance** for the fight against CSA in the EU. While US law does not oblige providers **to detect** CSA online in their services, it does oblige service providers **to report** it to NCMEC where they become aware of the abuse. NCMEC determines the relevant jurisdiction(s) from where materials were uploaded. Where the report relates to an EU Member State, the report is forwarded to the US Department of Homeland Security Investigations (HSI) for onward transfer to Europol, or directly to the relevant EU Member State law enforcement authorities. HSI plays an intermediary role as currently Europol cannot receive information directly from private parties, including NCMEC or service providers. Reports which are received by Europol are cross-checked and forwarded to the relevant Member State authorities. For reports relating to the US, NCMEC is able to provide a number of additional services, such as verifying that the reported content constitutes CSA according to the definitions under US law, and providing information on where the same content has been detected previously. This service cannot be provided for non-US reports due to the much higher volumes (in 2020, 98% of the reports were non-US related)[57].

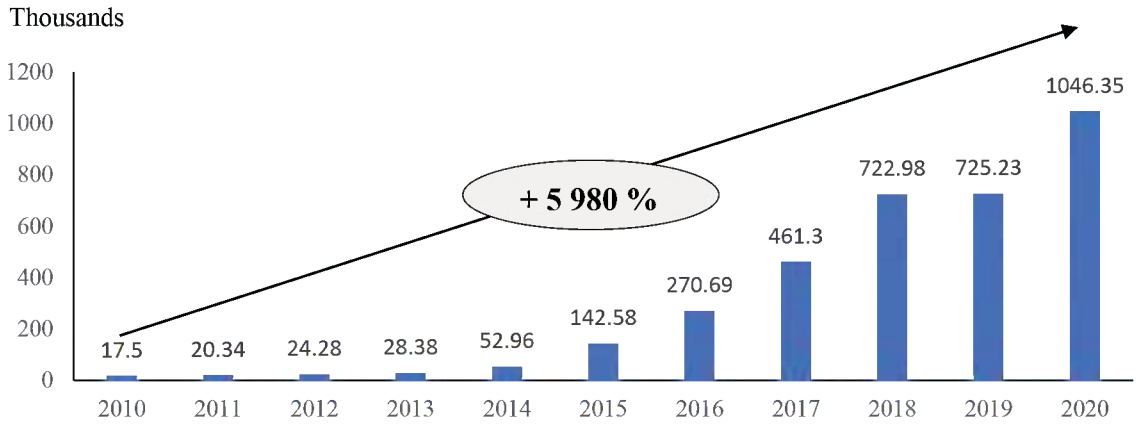
NCMEC has also a hotline function to receive reports from the public (independent from the above reporting by online service providers). It is part of the INHOPE network of national hotlines, which includes hotlines in most EU Member States where users can report CSAM that they may encounter accidentally; the hotlines then forward these reports to law enforcement and contact relevant providers to ensure removal. However, such reports from the public make up **less than 2%** of content found as it is rare for people to come across CSAM *and* report it[58]. The INHOPE hotlines facilitate the takedown of CSAM hosted outside the territory of the country where it is reported by identifying the country where the material is hosted and forwarding the information to the relevant hotline in that country for further notification to public authorities, or to the service provider if no hotline exists.

---

54 The functioning of the technology to detect the various types of CSA online is explained in detail in annex 8.
55 See section 1 on the "Interim Regulation".
56 Annex 6 contains details on reporting and the processing of CSAM reports.
57 NCMEC, 2020 data: out of 21.7 million reports, 494 000 originated in the US.
58 NCMEC, 2020 data: out of 21.7 million reports, 21.4 million were from service providers.

While still only very few companies engage in voluntary detection of child sexual abuse, the past few years have nonetheless seen a **strong increase** in reports of CSA online submitted by online service providers globally through NCMEC: from 1 million reports in 2010 to **over 21 million in 2020.** The number of reports concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.) has also dramatically increased: from 17 500 in 2010 to **more than 1 million in 2020**[59].

Figure 1: EU-related reports submitted by online service providers, 2010-2020



Box 3: new CSAM and self-generated content

Part of the increase in new CSAM is driven by self-generated child sexual abuse material. IWF reported a **77% increase** from 2019 to 2020 globally[60]. Whereas the first time the material is shared may be consensual, further resharing is typically not consensual. In a 2020 survey conducted by Thorn, 1 in 6 children aged 9 to 12 admitted that they had seen **non-consensually** reshared nudes of other children, up from 1 in 9 in 2019[61]. A separate survey by Economist Impact of 18-20 year olds on their childhood experiences found similar data: 18% of them reported experiencing a sexually explicit image of themselves being shared by a peer **without consent**[62].

First time sharing of self-generated material may be consensual but it may also be the result of **online grooming**. In the same survey conducted by Thorn, **50%** of the children aged 9 to 17 said that they had sent the nudes to someone they had never met in real life, up from 37% in 2019[63].

The amount of **grooming** cases reported globally **increased by 98%** in 2020 compared to the previous year (37 872 in 2020 vs 19 147 in 2019), presumably due to the **pandemic**, when both children and offenders spent more time online and at home[64].

The reports that service providers submitted in 2020 in relation to cases in the EU included **3.7 million** images and videos of **known CSAM**, **528 000** images and videos of **new CSAM**, and more than **1 400 grooming** cases[65].

---

59 NCMEC, 2020 data: The data does not include the UK in the first years of the period to ensure comparability.

60 Internet Watch Foundation (IWF), Annual Report 2020.

61 Thorn, Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020, 2020.

62 Economist Impact, WeProtect Global Alliance Global Threat Assessment, 2021.

63 Thorn, Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020, 2020.

64 NCMEC, Online Enticement Reports Skyrocket in 2020, 21 January 2021.

Reports indicate that some companies active and with servers in the EU have now become the **largest hosts of CSAM globally** (from hosting more than half of all CSAM detected in 2016 to 85% in 2020, with 77% in the Netherlands)[66].

Given the worsening situation, Member States have started to take action unilaterally, adopting sectoral rules to deal with the challenge, which are necessarily national in scope and risk further fragmenting the Internal Market (see problem driver section 2.2.2.).

Stakeholders' views
EU citizens are concerned about these developments. **93%** consider **important** the principle that **children should be protected in the online environment**, with **73%** of respondents considering this principle **very important** for inclusion in a potential future list of **EU digital principles**[67].

Prevention

Prevention is an essential component for tackling the problem at its roots.

There are two main types of prevention efforts:

1. Prevention efforts focused on **children** and their environment and on decreasing the likelihood that a child becomes a **victim**. Examples include **awareness raising campaigns** to help inform children, parents, carers and educators about risks and preventive mechanisms and procedures, as well as **training,** and efforts to detect and stop online grooming.
2. Prevention efforts focused on potential **offenders** and on decreasing the likelihood that a person **offends**[68]. Examples include prevention programmes for persons who **fear that they might offend**, and for persons who have already offended, to **prevent recidivism**[69].

Setting out effective prevention programmes remains challenging. Resources are limited and lack coordination, and efforts, where present, are rarely evaluated to assess their effectiveness. (see section 2.2.3. on problem drivers).

Assistance to victims

Assistance to victims is essential to mitigate the harm and severe consequences for children's physical and mental health caused by child sexual abuse (see section 2.1.3).

Victims require both **immediate and long-term assistance**, before, during and after criminal proceedings and taking into account the best interests of the child. This assistance must be specific, i.e. following an individual assessment of the special circumstances of each particular child victim, taking due account of the child's views, needs and concerns[70].

However, **immediate and long-term assistance** remains limited, not sufficiently coordinated between relevant actors within and between Member States and of unclear effectiveness (see section 2.2.3.). This leads to information gaps, hampers the sharing of best practices and lessons learnt and decreases the efficacy of efforts.

---

65 NCMEC, 2020 data.
66 Internet Watch Foundation (IWF), Annual Reports of 2016 to 2020.
67 Eurobarometer survey conducted in September and October 2021 (26,530 respondents from the 27 EU Member States).
68 In a recent survey to offenders in the Darkweb, 50% of offenders stated that they wanted to stop offending and expressed feeling of shame, guilt and self-harm. See Protect Children, CSAM Users in the Dark Web: Protecting Children Through Prevention, 2021.
69 Di Gioia, R., Beslay, L., 'Fighting child sexual abuse-Prevention policies for offenders, 3 October 2018.
70 As required by Article 19(3) of the CSA Directive.

2.1.2. Why is it a problem?

The fact that some child sexual abuse crimes are not adequately addressed in the EU is **a problem** because it results in victims not being rescued and effectively assisted as soon as possible, children being less protected from crimes, and offenders enjoying impunity. It affects **public security** in the EU and infringes children's fundamental rights under the Charter of Fundamental Rights of the EU (Charter)[71], including the right to such protection and care as is necessary for their well-being, the right to human dignity and the right to privacy. The continued presence and dissemination of manifestly illegal images and videos online, and the very heterogeneous approach of service providers, affects private and public interests, hampering **trust, innovation and growth** in the **single market for digital services**, in particular due to the **fragmentation** created by divergent national approaches trying to address the problem of CSA online (see problem driver section 2.2.2.).

Additionally, CSA has societal and economic costs. In particular, it contributes to an increased risk of serious mental and physical health problems across the lifespan, and exerts a substantial economic burden on individuals, families, and societies. There are **negative consequences at all stages**:

- **Before** the crime is committed: in the absence of proper preventative interventions, individuals who could have been stopped from abusing children may become first-time offenders, offenders are more likely to re-offend, and children are more likely to become victims if they and their carers lack awareness of the threat when using online services.
- **While** the crime is being committed: the consequences of not detecting and addressing the crimes swiftly include **prolonged suffering and harm** for victims. In addition, it reinforces the **perception of impunity**, reducing deterrence and facilitating further offending.
- **After** the crime has been committed: the consequences of not acting effectively after the crime include the inability to provide proper immediate and long-term **assistance to victims**, with negative effects for victims and society as described above. In addition, it may not be possible to prosecute offenders, which reduces opportunities for rehabilitation before, during and after criminal proceedings to prevent reoffending.

2.1.3. Who is affected and how?

First, **children** in the **EU and elsewhere**, who may fall victim to sexual abuse and suffer its negative effects, both in the **immediate and long-term**[72]. **Immediate effects** include physical injuries and psychological consequences (e.g. shock, fear, anxiety, guilt, post-traumatic stress disorder, denial, withdrawal, isolation, and grief), sexual behaviour problems and over-sexualised behaviour, academic problems, substance abuse problems, increased likelihood of involvement in delinquency and crime, and increased likelihood of teen pregnancy[73]. **Long-term effects** include psychological and social adjustment problems that can carry over into adulthood and affect married life and parenthood. They include negative effects on sexual and overall physical health; mental health problems including depression, personality and psychotic disorders, post-traumatic stress disorder, self-mutilation, attempted or completed suicide; and relational and marital problems including fear of intimacy and spousal violence.

Secondly, **online service providers.** Member States' efforts to tackle the challenge at national level create **distortions** in the single market for digital services (see problem driver section 2.2.2.), as providers have to comply with sector-specific rules under national laws at least in

---

71 See section 6.1.3 below.

72 Institut National de Santé Publique, Gouvernement du Québec, Consequences of child sexual abuse, accessed on 20 April 2021; ODI Report: The cost and economic impact of violence against children, p.20.

73 Masumova, F., A Need for Improved Detection of Child and Adolescent Sexual Abuse, May 2017; Darkness to Light, Child Sexual Abuse Statistics, accessed on 20 April 2021.

some of the jurisdictions where they are active, resulting in a more challenging business environment for companies, in particular for smaller companies that are already facing difficulties of competing with their largest counterparts.

Third, **users of online services.** The detection, reporting and removal of CSA online currently **lacks clarity, legal certainty and transparency**. As a consequence, the rights and interests of users can be negatively affected. This can occur, for instance, in relation to unjustified reporting or removals, which may affect not only the users initiating the communications in question but also those at the receiving end. The existing uncertainty may also have a **'chilling effect'** on legitimate forms of communications or hamper the full participation of children in online services as their parents and carers become more and more aware of the risks but do not have access to transparent information about the levels of risk and about what measures services take to protect children.

Fourth, **governments and public authorities.** The competent public authorities (e.g. law enforcement or governments at national, regional and local levels) dedicate significant resources to act against CSA. In particular, they put in place prevention programmes and measures to assist victims, and conduct investigations after they become aware of possible CSA. Inefficiencies in the current system lead them to seek local solutions to incentivise and obtain more information from providers.

Finally, **society** in general, given that CSA has consequences not only for the victims, but also for society as a whole[74]. **Social costs** correspond to the non-monetary consequences of the criminal acts, and include diminished quality of life for society and increased feelings of insecurity among individuals. **Economic costs** include those of police and judicial services (e.g. criminal prosecution, correctional system), social services, victim support service and victim compensation programmes, education, health, and employment costs.

Box 4: estimated costs of child sexual abuse

Victims of child sexual abuse require **immediate and long-term assistance**. The costs of providing such assistance can be significant. For example, the total lifetime costs of assistance to victims arising from new substantiated cases of child sexual abuse in the United States in 2015 was estimated at USD **1.5 billion** per year[75].

The long-term effects of child sexual abuse on victims also include lifelong **loss of potential earnings and productivity**[76]. The total lifetime cost of such losses arising from new substantiated cases of CSA in the US in 2015 was estimated at USD **6.8 billion** per year[77].

Overall, the total estimated costs of child sexual abuse in the US in 2015 were estimated at **USD 11 billion** per year[78].

2.2. What are the problem drivers?

2.2.1. Voluntary action by online service providers to detect online child sexual abuse has proven insufficient

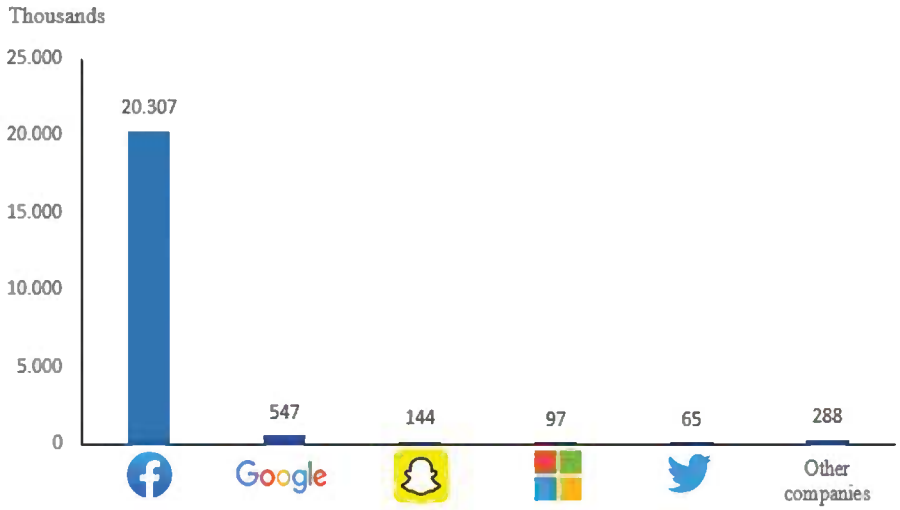
Voluntary action varies significantly among companies

74 Institut National de Santé Publique, Gouvernement du Québec, accessed on 20 April 2021.
75 Letourneau, E., The Economic Burden of Child Sexual Abuse in the United States, May 2018.
76 *Ibid.*
77 *Ibid.*, based on combined estimated productivity losses for non-fatal and fatal cases.
78 *Ibid.* The USD 11 billion/year include the costs due to violence and crime, and suicide deaths (USD 1 billion/year), and the costs due to loss of quality-adjusted life years (USD 1.6 billion/year), in addition to the victims assistance costs and productivity losses.

Online service providers are often the only entities capable of detecting that abuse involving their services is taking place. Because detection is **voluntary**, some online service providers take comprehensive action, others take some action, and there are providers that do not take any action against CSA at all. In addition, service providers often do not have access to **reliable information** on what content and behaviour is illegal in the EU to facilitate accurate detection, proactively and voluntarily, resulting in a risk of both over- and underreporting.

There are currently **1 630** companies registered to report to NCMEC, which is the main entity to receive reports of proactive searches that companies perform on their system, and the *de facto* global clearinghouse of reports of CSA online. This is a fraction of the online services used to commit these crimes. In 2020, of these 1 630 companies, **one,** Facebook, sent **95%** of reports, **5** sent **99%** of reports, and only **10%** sent **one report or more**[79]. There is no evidence that 95% of all the current cases of CSA online (including sharing of known and new CSAM, and grooming) occur on the services of that single company. In fact, experts agree that **comparable levels of abuse** occur in **similar services** from other companies, and the difference in detection levels is rather due to the **different intensity** of detection efforts[80]. For example, some providers may make efforts to detect abuse only in certain services they provide, or may make efforts to detect only certain types of abuse. This would mean that there is a **substantial amount** of CSA online that **remains undetected**.

Figure 2: breakdown of reports submitted by online service providers globally in 2020[81]



In addition, a number of service providers take action against users for suspected sharing of CSAM, e.g. by banning user accounts, but **do not report**. For example, WhatsApp indicates that it bans around 300 000 accounts per month for this reason alone[82]. However, it has been reported that WhatsApp reports to NCMEC only about 10% of these cases, as the evidence recovered is circumstantial only and in line with US legislation is insufficient for a criminal

79 National Centre for Missing and Exploited Children, 2020 Reports by Electronic Service Providers.
80 NetClean, Report 2019: A Report about Child Sexual Abuse Crime, p.7, 32-33; NetClean, Report 2016: 10 Important Insights into Child Sexual Abuse Crime, p.33.
81 National Centre for Missing and Exploited Children, 2020 Reports by Electronic Service Providers.
82 WhatsApp, How WhatsApp helps fight child exploitation, accessed on 20 September 2021.

investigation[83]. Where that is so, there is on the one hand a risk that users are banned on the basis of unclear and potentially insufficient evidence, while on the other hand actual abuse may not be reported and investigated. This can have a significant negative effect on the **fundamental rights** of users[84], and on the affected children.

These different approaches and the related risks also create asymmetries in the **single market for digital services**, as they have prompted a number of Member States to adopt or consider national legislation to create a stronger and more effective approach (see problem driver section 2.2.2).

Voluntary action is susceptible to changes in companies' policies.

Because detection is voluntary, companies may decide to change their policies **at will**. One example is Facebook's decision to implement **end-to-end encryption (E2EE)** on its private messaging service by default.

Existing detection efforts risk being severely hampered by the introduction of encryption in online services, which in spite of its benefits for cybersecurity and the protection of users' fundamental rights, such as freedom of expression, privacy, and data protection, also makes the detection of CSA online and the protection of fundamental rights of the victimised children more difficult[85], when not impossible.

*Box 5: **end-to-end encryption**, a policy change impacting child sexual abuse detection*

In March 2019, Facebook announced plans to implement **end to-end encryption (E2EE)** by default in its instant messaging service[86]. These plans have been reiterated afterwards[87], with the implementation taking place "sometime in 2023"[88]. In the absence of accompanying measures, it is **conservatively** estimated that this could reduce the number of total reports of CSA in the EU (and globally) by **more than half[89], and as much as two-thirds**[90]. These estimates were confirmed after Facebook announced that it had stopped the detection of CSA in its instant messaging service in December 2020[91], given the legal uncertainty it considered to be caused by the entry into force of the European Electronic Communications Code (see the information on the Interim Regulation in section 1). From 1 January to 30 October 2021 the number of reports received by law enforcement in the EU **dropped by two-thirds** compared to the same period in 2020 (972,581 reports vs 341,326 reports)[92], a **loss of 2 100 reports per day**. In total in 2021, while there was a 35% increase in global reports, the number of reports relevant for the EU dropped by 47%[93]. Whereas in this case the tools to

83 Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, May 2020. The number of Facebook reports in Figure 2 includes all Facebook platforms (i.e. also WhatsApp). According to the above, the number of WhatsApp reports would be around 400 000 versus around 20 million reports from Facebook platform.

84 Impact Assessment accompanying the DSA proposal, SWD(2020) 348 final, December 2020, p17.

85 EU strategy (footnote **Error! Bookmark not defined.**), p.2.

86 Facebook, A Privacy-Focused Vision for Social Networking, 12 March 2019.

87 Including during the UK's Home Affairs Committee hearing of 20 January 2021 on Online Harms.

88 Davis, A. (Head of Safety at Meta), We'll protect privacy and prevent harm, writes Facebook safety boss, Sunday Telegraph, 21 November 2021.

89 NCMEC, End-to-end encryption: ignoring abuse won't stop it, accessed 20 April 2021.

90 EU strategy (footnote 79), p.15.

91 Facebook, Changes to Facebook Messaging Services in Europe, 20 December 2020.

92 NCMEC.

93 NCMEC, 2021 data. The drop in reports is in particular due to the fact that Meta, the company responsibly for the majority of reports, stopped the detection efforts in the EU in December 2020 and did not resume until November 2021.

detect CSA were not used due to legal concerns, the practical effects are likely the same as an implementation of E2EE without mitigating measures[94] would cause: the impossibility to detect CSA, since the detection tools **as currently used do not work on E2EE systems.**

Google announced in November 2020 that it had started to roll out E2EE on Google Messages[95]. Other similar services with E2EE already incorporated (with presumably **similar if not higher levels of CSA[96]**) include WhatsApp, Apple's iMessage, Signal and Telegram.

In addition to affecting the detection of CSA online and the protection of fundamental rights of the victimised children, the use of E2EE without mitigating measures **reduces the means to prevent and combat CSA overall** by "turning-off the light" on a significant part of the problem, i.e. decreasing the evidence base, including data on the scale of detectable CSA online, which is essential to fight against overall CSA effectively through assistance to victims, investigations, and prevention.[97] In the absence of mitigating measures (e.g. tools that can detect CSA online in E2EE systems, see annex 9), currently the possible ways to detect CSA online in E2EE systems are:

1) **user reports**, i.e. either the child or the offender reports the abuse; and
2) **metadata**, i.e. the time of the online exchange, the user names, and data related to the online exchange other than its content. This also includes suspicious patterns of activity (e.g. if someone repeatedly sets up new profiles or messages a large number of people they do not know[98]).

Relying on **user reports** implies that the responsibility of reporting will be borne **solely by child victims** of sexual abuse in grooming cases, who in many cases are shamed or threatened into silence (see section 2.1.1. on underreporting), as the offender will obviously not report the abuse. This is already evident from the low number of user reports today.

Service providers **do not** consider **metadata** as an **effective** tool in detecting CSAM[99]. In addition, the use of **metadata** is **usually insufficient** to initiate investigations[100]. Moreover, it is likely to generate a much lower number of reports than the detection of content, despite the level of abuse being the same (if not higher). As an example, consider WhatsApp (E2EE and therefore uses metadata as the basis of detection) and Facebook Messenger (not E2EE and therefore uses content as the basis of detection). Whereas WhatsApp has around **50% more users** than Facebook Messenger (2 billion vs 1.3 billion[101]), and therefore, presumably, higher level of abuse proportional to the number of users, there were around **35 times** less reports

---

94 Mitigating measures refer to deploying E2EE in a way that it enables the continued detection of CSA online.

95 Google, Helping you connect around the world with Messages, 19 November 2020.

96 NSPCC, End-to-end encryption, Understanding the impacts for child safety online, April 2021.

97 WeProtect Global Alliance to end child sexual exploitation online, Global Threat Assessment, 2021.

98 Davis, A. (Head of Safety at Meta), We'll protect privacy and prevent harm, writes Facebook safety boss, Sunday Telegraph, 21 November 2021.

99 Pfefferkorn, R., Stanford Internet Observatory, Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers, 9 September, 2021. See in particular p.10-11.

100 WeProtect Global Alliance to end child sexual exploitation online, Global Threat Assessment, 2021, reporting a statement by the Virtual Global Taskforce, an international alliance of law enforcement agencies (including Europol, Dutch Police, Interpol, US Homeland Security Investigations, UK National Crime Agency, Colombian Police and others) against CSA online. See also Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, May 2020.

101 Statista, Most popular global mobile messenger apps as of October 2021, based on number of monthly active users. The overall numbers of users were the same in 2020.

from WhatsApp than from Facebook Messenger submitted to NCMEC in 2020 (400 000 vs 14 million)[102].

Europol reports that the widespread use of encryption tools, including E2EE apps, has **lowered the risk of detection** for those who offend against children[103]. Offenders are **well aware** of the possibilities that E2EE present to hide their abuse. In an analysis of offender forums in the Darkweb, it was found that a majority of discussions focused on topics such as technical tools for direct messaging or how to securely acquire and store content[104].

Voluntary action leaves decisions affecting fundamental rights to service providers and lacks harmonised safeguards

A voluntary system leaves private companies to make **fundamental decisions** with significant impact on users and their rights[105]. The challenges in this system are particularly evident when dealing with CSA, where there are fundamental rights and interests at stake on all sides – including the right to protection of their well-being and to privacy on the side of the child, the right to privacy and freedom of expression and information for all users. As a result, if the rights of the child are deemed important enough to justify interfering with the rights of all users and of service providers, then it may not be appropriate to leave the decision on whether and if so, how to do so to the service providers.

In addition, the current voluntary action by online service providers to detect CSA online lacks long-term perspective and harmonised safeguards applicable to all relevant service providers, including **transparency**. This is especially important as some of the voluntary measures that companies decide to take may interfere with users' rights, including those to privacy and data protection. It is unclear which tools are in use and how they are used, or which procedures are in place to improve the tools and limit the number of false positives. While there is an obvious need not to warn off perpetrators or inadvertently provide guidance on how to avoid detection, there may be room for more information. As a result, users at present may have no **effective redress** in case of **erroneous removals**; the possibilities of **scrutiny** are limited; and there is **no effective oversight** by regulators. In addition, the existence and effectiveness of **procedural safeguards** differs widely across providers.

The Interim Regulation introduced a number of **safeguards**, such as annual transparency reports, consultation with data protection authorities on their processing to detect CSA online, and complaint mechanisms, so that content that has been removed erroneously can be reinstated (see section 1).

A number of important safeguards are contained in the **DSA proposal**, which lays down harmonized transparency requirements in case of content moderation based on providers own initiative[106], as well as in relation to mechanisms for removal and related user complaints[107].

---

102 NCMEC and Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, May 2020.

103 Europol, Europol Serious and Organised Crime Threat Assessment (SOCTA), April 2021.

104 Analysis conducted in February 2021, as reported in WeProtect Global Alliance to end child sexual exploitation online, Global Threat Assessment, 2021.

105 Impact Assessment accompanying the DSA proposal, SWD(2020) 348 final, December 2020, p.25.

106 See in particular Article 13(1)(c).

107 These include a statement of reasons in case a provider of hosting services decided to remove or disable access to content and possibility of the recipient of the service to challenge any content moderation decision, see Articles 15, 17 and 18.

Given the gravity of impact on both sides – for the child victims, materials depicting their abuse, and the risk of (further) abuse, and for the suspected user, an accusation of having circulated CSAM – the above safeguards form an important baseline but **do not go far enough** in the present context. In particular, the stakeholder consultations have shown the importance of a **universal reporting obligation** for CSA online for the providers, using dedicated secure and fast channels, as well as of additional requirements on the technologies employed for automatic detection to ensure that they are both **effective** in detecting abuse and also **limit the number of false positives** to the maximum extent technically possible.

Voluntary action has failed to remove victims' images effectively

Victims are left on their own when images and videos of their abuse end up online. Under national criminal laws, hotlines in the EU are in principle not allowed to proactively **search for images and videos of a given victim**, on the victim's behalf, to effect removal. For the same reason, **victims themselves** are also **prohibited** from searching for **their own images and videos**, as the possession of CSAM is illegal *per se*. Absent a requirement for relevant services providers to take proportionate measures to detect, report and remove specified content, an effective removal system has not developed[108].

Box 6: Voluntary principles to counter online child sexual abuse

The US, UK, Canada, Australia and New Zealand (the 'Five Eyes'), together with leading online service providers, civil society and academia, announced in 2020 a set of **voluntary principles** for companies to tackle child sexual abuse online[109]. These address notably the detection, reporting and removal of CSAM, as well as detection and reporting of grooming. Although multiple companies have committed to implementing the voluntary principles, including Facebook, Google, Microsoft, Roblox, Snap and Twitter, there is a **lack of transparency** on the actions that companies are taking to implement those principles. As a consequence, there is a **lack of evidence of tangible results** of that commitment.

2.2.2. Inefficiencies in public-private cooperation between online service providers, civil society organisations and public authorities hamper an effective fight against CSA

This section describes the inefficiencies in public-private cooperation between the main actors in the fight against CSA, online and offline. In a majority of cases, the inefficiencies relate to regulatory issues.

Cooperation between public authorities and service providers

Cooperation between public authorities and service providers is of critical importance in the fight against CSA, particularly in relation to service providers' efforts to detect and report CSA online and remove CSAM.

[108] While the legislative proposal would mandate the Centre to proactively look for CSAM and could include a targeted liability exemption to shield the Centre and hotlines where necessary and appropriate, in addition, the Centre may need an authorisation from its host Member State to exclude that it is held liable for its proactive searches under national criminal law. Such an authorisation would be part of the conditions for establishing the EU agency in a given Member State (see section 5.2.2.1.). Similarly, to ensure service providers will not be held liable when searching their systems, the legislative proposal could include a specific exemption from liability, building on the exemption contained in the DSA.

[109] The voluntary principles are available here.

- **Legal fragmentation** affecting the **Internal Market**

Currently, although obligations under national law are increasingly introduced, companies offering online services in the EU still detect, report and remove CSA online from their services on a voluntary basis. There are at present no effective procedures under EU law for service providers to report to public authorities or to exchange information in a timely manner or swiftly react to requests and complaints. This hampers investigations and creates obstacles to addressing CSA and to protecting victims.

This has led to a number of Member States preparing and adopting individual legislative proposals at the national level to create stricter rules for providers who fail to cooperate with public authorities or do not put in sufficient efforts to detect and report CSAM. Some Member States adopted new legislation as recently as 2021 (e.g. Germany,[110] Austria) and others are currently preparing legislative proposals (e.g. Germany, France, the Netherlands) (see Annex 5). These efforts often involve establishing dedicated public authorities or designating existing authorities to enforce the new rules[111], as well as strict time-limits for service providers to remove CSAM upon becoming aware, subject to fines if they fail to do so[112]. At the same time, the reach of these efforts varies and they are constrained by the national laws of the Member States. The scope of relevant national laws and their obligations differ in terms of the services covered. For instance, some focus on social networks in general[113], others on hosting providers managing websites containing illegal content[114] and yet others on online platforms above a certain threshold (e.g. number of registered users and annual revenue)[115]. Approaches are by nature limited to national jurisdictions. Given the cross-border nature of the Internet, and by implication many service providers operating online as well as online CSA, such a fragmented approach hampers the proper functioning of the internal market. Moreover, such a fragmented approach cannot ensure the effective detection, reporting and removal of CSAM and the fight against grooming across the EU, beyond the borders of individual Member States having the above-mentioned national legislation in place. Compared to one horizontal framework established at EU level, such a Member State-based approach increases the costs of doing business in the EU as service providers have to adapt to various different sets of rules, which creates uncertainties and challenges in particular for smaller providers seeking to expand to new markets in the EU, and can stifle innovation and competition.

---

110 April 2021 Modification of the Netzwerkdurchsetzungsgesetz (NetzDG) to include detailed reporting obligations in case of child pornography; see annex 5, section 3 for further information.

111 For instance, in Germany, the draft Act amending the Protection of Young Persons Act provides for the restructuring of a national media supervising body into a federal agency to oversee the implementation of the draft Act's provisions. In France, the Draft law to regulate online platforms aims to create a new national (administrative) authority equipped for protecting minors (including combatting the commercial exploitation of the image of children under sixteen years of age on online platforms). See annex 5, section 3 for further information.

112 For instance the NetzDG in Germany, the Avia law in France or the Draft law on fighting child sexual abuse.in the Netherlands. See annex 5, section 3 for further information.

113 For example the NetzDG in Germany. See annex 5, section 3 for further information.

114 For instance Decree n° 2015-125 of February 5, 2015 in France. See annex 5, section 3 for further information.

115 For example the Draft law on measures to protect users on communication platforms (Communications Platform Act) in Austria. See annex 5, section 3 for further information.

Box 7: the CSAM issue in the Netherlands

As highlighted above, reports indicate that some service providers active and with servers in the EU have now become the **largest hosts of CSAM globally**, with more than half of all CSAM hosted in the Netherlands, given its strong internet infrastructure. The Dutch government has made several commitments to address this issue, including investing in **partnerships between the Dutch Government and the private sector**. This included a new **free service** called 'Hash Check Service' (operated by the EU co-funded Dutch INHOPE hotline EOKM) **made available to companies to scan their servers for known CSAM**. Given that there is a small group of Dutch companies that only cooperate to a lesser extent, and some companies not at all, the Netherlands is also preparing a **new law to deal with companies that fail to cooperate**. In the near future, companies will be under the supervision of a **governing body that will have the authority to impose administrative sanctions** on companies that fail to cooperate. In addition to criminal law, this procedure specifically aims to eradicate CSAM in a fast and efficient manner.

The national approaches create fragmentation on the Internal Market, hindering effective cooperation between public authorities and service providers in the fight against CSA. The continued presence and dissemination of CSAM, and the very heterogeneous approaches of service providers, affect both private and public interests, hampering trust, innovation and growth on the **Internal Market (i.e. single market for digital services)**. Such fragmentation increases compliance and operational costs of the actions in the fight against CSA for stakeholders such as online service providers that operate in several Member States and may lead to legal uncertainty. Non-compliant service providers may move to and continue operating from Member States where national rules are less strict. Given the cross-border and international dimension of online service provision as well as child sexual abuse online, a patchwork of national measures does **not effectively protect children**, and creates **distortions** in the functioning of the **single market for digital services.**

The proposed **Digital Services Act** will not be able to reduce this fragmentation to the extent necessary, given its horizontal nature and the specific challenges posed by CSA (see section 5.1.). For example, the DSA would not create removal obligations. Some Member States have already gone farther, like Germany, which for certain providers such as social networks has imposed removal obligations by law[116], as well as reporting obligations in case of detection of CSAM, specifying the data to be reported to federal law enforcement, as well as an obligatory notification to the user and other aspects[117].

- Varying **quality of reports**

While reports from service providers via NCMEC have led to many cases of children being rescued from ongoing abuse, and of offenders arrested, law enforcement authorities estimate that only around **75%** of reports they receive from service providers are actionable[118]. The most common reason is that the report contains material that **does not constitute child sexual abuse** under the Member State's law[119]. This is largely due to a simple fact: US-based service

[116] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – Network Enforcement Law), BGBl. 2017 I Nr. 61, 7.9.2017, § 3 n. 2 and 3.

[117] Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (Law to combat right wing extremism and hate crime), BGBl 2021 I Nr. 13, 1.4.2021, Art. 7 n. 3.

[118] Median of estimated % of reports that are actionable, see targeted survey to law enforcement (annex 2, section 1.1.3).

[119] Targeted survey of law enforcement authorities (see annex 2, section 1.1.3).

providers report to NCMEC material that may constitute CSA under **US law**[120], which may **include** content that is **not illegal in the EU** and **omit** content that is **illegal in the EU**. For example, the CSA Directive leaves up to Member States to make illegal sexual abuse material involving individuals appearing to be a child but in fact older than 18, whereas US legislation requires that the material involve an "identifiable minor" to be illegal. On the other hand, the CSA Directive criminalizes grooming only when the child is below the age of sexual consent, whereas it is always illegal in the US for any person under 18[121].

Further challenges arise as a result of a **lack of unified reporting requirements** which clearly set out the information to be included in reports. While US service providers are obliged to make reports to NCMEC, much of the information to be included in the report is left at the discretion of the provider[122]. The service that NCMEC provides for US-related reports (i.e. human review of the reports to ensure that they are actionable) is typically not available for EU-related reports, due to resource constraints. A **lack of sufficient information** is also one of the most common reasons cited by the law enforcement authorities of the Member States for a report not to be actionable[123].

- **Lack of resources** in law enforcement agencies

Absent the support provided by NCMEC to US authorities, each national law enforcement authority is left to its own devices when analysing CSAM, despite the support provided by Europol to help coordinate cases. This requires a significant investment of resources and makes it very difficult to deal effectively with the large amount of reports these authorities receive, and prevents an effective public-private cooperation against CSA.

- **Lack of feedback** from public authorities to service providers.

Currently, there is **no mechanism for systematic feedback** from law enforcement to companies on their reports. Where providers report content that is not illegal under the law of the relevant Member State, the provider is **not made aware** of that fact. This increases the likelihood of the provider reporting the same or similar content again in the future.

- Challenges due to the **international and cross-border nature** of CSA

There are several international and cross-border aspects to the fight against CSA online. In many cases, these are inherent in the cross-border nature of the Internet. As a result, a single incident of online abuse may involve perpetrators and victims located in multiple jurisdictions. While certain minimum standards relating to CSA crimes have been widely adopted in criminal law in many countries, and within the EU the CSA Directive contains specific requirements providing for a degree of harmonisation, specific national definitions and offences differ from one country to another.

In addition, long-standing difficulties with regard to **cross-border access to electronic evidence** pose a particular problem for the investigation of CSA online. Law enforcement frequently needs additional information during investigations from service providers, which are often located in another Member State, or in a third country. Existing judicial cooperation is **too slow** and direct cooperation between service providers and public authorities is **unreliable, inconsistent and lacks transparency and accountability**. Several legislative proposals and other ongoing initiatives aim to address these issues (see box 2 in Annex 6).

---

120 'Duty to Report', 18 U.S.C. §2258A(a).
121 See Articles 5(7) and 6 of the CSA Directive, and 18 U.S. Code § 2252A and § 2422 respectively.
122 'Contents of Report', 18 U.S.C. §2258A(b).
123 Targeted survey of law enforcement authorities (see annex 2, section 1.1.3).

Furthermore, due to the existing legal framework and the often important or even dominant market position of US service providers, Member States are **heavily dependent** in their fight against CSA on reports received from a third country, the US, through NCMEC.

Cooperation between civil society organisations and service providers

- Cooperation challenges in **notice and action procedures**.

When they receive a notice from civil society organisations requesting them to remove content, service providers in more than **25%** of cases refuse to take action to remove the notified content or take a considerable time period to do so[124]. Whilst there can be justified reasons for not taking action or for some delays in individuals cases (for instance, because of uncertainty as to whether the notified content actually constitutes CSAM under the applicable laws), there is a particularly problematic group of providers known as **'bulletproof hosting providers'**, which refuse to assume any responsibility for content stored on their servers[125]. It should be recalled that, **at present,** EU law does not provide for an obligation for providers to report or act upon notified content, not even where it manifestly constitutes CSAM. Under the eCommerce Directive (Art. 14) and the proposed DSA (Art. 5, see section 5.1.), hosting service providers' failure to act expeditiously to remove or disable access to illegal content (including CSAM) would lead to loss of the benefit of the liability exemption. In such cases, the service providers *may* – but not necessarily *will* – be liable under the applicable national laws of the Member States, depending on whether these national laws provide for liability for service providers.

Cooperation between public authorities and civil society organisations

- Limited impact of **hotlines' action** in the EU due to **regulatory gaps**.

Inability to search proactively. As noted, hotlines operating in Member States are under national criminal law in principle not allowed to search CSAM proactively. They therefore tend to rely exclusively on reports from the public, which are of **limited number and fluctuating in quality**. The number of user reports is significantly lower than those from proactive efforts, as the situations in which someone comes across CSAM unintentionally *and* reports it are limited[126]. Also, user reports are often inaccurate, in particular compared with reports from proactive searches[127]. For example, the only hotline that conducts proactive searches in Europe, IWF in the UK, reported that whereas about half of the reports it manages come from the public and half from proactive searches, only 10% of the total CSAM that it finds traces back to public reports vs 90% from proactive searches[128].

- Inefficiencies in cooperation on **assistance to victims**.

For **long-term assistance** to victims, there is room for improvement in the cooperation between public authorities and NGOs to ensure that victims are **aware** of the resources available to them. In addition, currently there is no cooperation between public authorities and

---

124 27% of allegedly illegal content URLs notified to service providers were not removed within 3 days, INHOPE 2020 Annual Report, May 2021.

125 See for example these cases in the Netherlands here and here.

126 In 2020, whereas service providers reported through NCMEC 65 million images and videos globally, INHOPE hotlines processed globally 1 million images and videos which originated from both the public and proactive searches by a limited number of non-EU hotlines.

127 About 25% of the reports the hotlines receive from the public include illegal content, see INHOPE Annual Report, April 2020.

128 IWF, 2020 Annual Report, April 2021.

hotlines or other NGOs to support victims at their request in searching and taking down the material depicting them.

- Inefficiencies in cooperation on **prevention**.

Inefficiencies in cooperation exist notably on prevention programmes **for offenders and for persons who fear that they might offend**. In some Member States, NGOs carry out these programmes with limited support from public authorities[129]. In addition, the coordination between public authorities and NGOs on the programmes they respectively offer at different stages is also limited (e.g. between the programmes that public authorities offer in prisons and the reintegration programmes that NGOs offer after the offender leaves prison) [130].

Cooperation between public authorities, service providers and civil society organisations

- Lack of legal certainty:
  - **For service providers.** The Interim Regulation did not create an **explicit** legal basis for service providers to proactively detect CSA, and it only provided a temporary and strictly limited derogation from certain articles of the e-Privacy Directive to allow the continuation of the voluntary measures to detect CSA, provided that these are lawful. Whereas some service providers invoke legal bases provided for in the GDPR for the processing of personal data involved in them carrying out their voluntary actions to tackle CSA, others find the GDPR legal bases not explicit enough. The uncertainty thus deters some service providers from taking such voluntary action.
  - **For hotlines.** The operation of hotlines is not explicitly provided for in EU law, and only five Member States explicitly regulate it[131], with others relying on memorandums of understanding. This leads to the **inability of hotlines to assess the content of reports** from the public in some Member States, or **to notify the service provider directly,** leading to fragmentation and ineffectiveness across the EU[132].

- Lack of operational standards:

Law enforcement agencies, online service providers and civil society organisations have separate systems and standards used in the detection, reporting and removal of CSA online. They vary not only between the different types of stakeholders (e.g. between law enforcement and service providers) but also between the same type of stakeholder (e.g. between law enforcement agencies in different Member States). This includes the use of multiple, differing databases of hashes used in the detection of known CSAM. This hampers the collective ability to efficiently and effectively detect, report and remove CSAM, to identify and rescue victims, and to arrest offenders.

Stakeholders' views

Public authorities[133] identified among the main challenges while investigating CSA cases: a) inefficiencies in public-private cooperation between service providers and public authorities, and b) inefficiencies/difficulties with access to evidence due to technical challenges. Over 80% referred to the increased volume of CSAM detected online in the last decade and further flagged that there are insufficient human and technical resources to deal with it. These same stakeholders state that a common baseline (also in terms of a common classification

129 Di Gioia, R., Beslay, L., Fighting child sexual abuse - Prevention policies for offenders, October 2018.
130 See for example the results of 2020 evaluation of Circles UK, and EU funded project CIRCLES4EU.
131 ICF et al. *Study on framework of best practices to tackle child sexual abuse material online*, 2020.
132 *Ibid*.
133 The term 'public authorities' in the stakeholders' views boxes refers to law enforcement authorities and other public authorities such as government ministries.

system and terminology) is required to support better law enforcement and judicial cooperation and information sharing consistent with the cross-border nature of offending in CSAM.
Civil society organisations stressed the need to improve cooperation between them and law enforcement authorities (74%) in the fight against CSA online (including by providing funding to enable cooperation, organizing joint trainings/meetings and ensuring better information sharing, as well as the need for legal recognition and a clear legal basis for the national hotlines). In addition, 73% of the respondents from civil society organisation pointed out that improved cooperation with service providers is needed.
Service providers highlighted the need for coordinated actions on a global level, and the importance of exchange of best practices.

2.2.3. Member States' efforts to prevent child sexual abuse and to assist victims are limited, divergent and lack coordination and are of unclear effectiveness

Prevention efforts

- Limited.
  In relation to the two main types of prevention efforts described in section 2.1.:
  - Prevention efforts to decrease the likelihood that a child becomes a victim. **Awareness raising**[134] **and training** is limited in availability, particularly to organisations and persons that come in regular and direct contact with children as part of their jobs or vocational activities, in addition to carers and parents. A vast majority of the abuse occurs in the circle of trust of the child. At the same time, those in regular and direct contact with children should have the knowledge and tools to ensure that children do not become victims, given their proximity to the child.
  - Prevention efforts to decrease the likelihood that a person offends.
    Research into what motivates individuals to become offenders is **scarce and fragmented**. This current lack of research makes it difficult to put in place effective programmes before a person offends for the first time, in the course of or after criminal proceedings, both inside and outside prison. As a result, there are currently very few programmes in place[135].
- Uncoordinated. Multiple types of stakeholders need to take action to enact a preventive approach that delivers results. This includes public authorities, the research community, NGOs, and providers of online services used by children. The various types of practitioners in this field do **not communicate sufficiently** with each other and with researchers on the effectiveness of the programmes, lessons learned and best practices; **language** can be a further barrier. Expertise and resources to establish and implement such initiatives are not evenly distributed in the EU, and successful programmes are mostly local endeavours. There are **overlapping efforts** in some areas, e.g. Member States designing similar programmes and campaigns in parallel[136], whereas other areas, such as reaching out to potential offenders, are **not sufficiently addressed**.
- Unclear effectiveness. The few programmes that exist are **rarely evaluated** to assess their effectiveness and usability[137]. A recent systematic review of the published empirical literature on child sexual abuse perpetration prevention interventions found **only five**

[134] The Commission- funded network of Safer Internet Centres is a good example. It raises awareness on online safety and provides information, resources and assistance via helplines and hotlines on a wide range of digital safety topics including grooming and sexting.
[135] For an overview of prevention programmes in the EU and third countries, see Di Gioia R., Beslay, L. (2018) Fighting child sexual abuse: prevention policies for offenders – Inception Report, EUR 29344 EN, doi: 10.2760/48791
[136] Di Gioia, R., Beslay, L., 'Fighting child sexual abuse-Prevention policies for offenders, 3 October 2018.
[137] *Ibid.*

published evaluation studies, and these were methodologically limited (e.g. four examined the same intervention only on adults in Germany, and the other one focused only on children aged 5 to 12)[138].

Assistance to victims' efforts

- Limited. Victims of CSA do not always receive the **tailored and comprehensive assistance** required[139], such as support in trying to stop the sharing and distribution online of the images and videos depicting their abuse, which perpetuates the harm.
- Uncoordinated. Victims of CSA require comprehensive support that brings together all relevant sectors, including health, legal, child protection, education and employment. Such **coordination** between relevant actors within and between Member States is lacking. The existing initiatives do not systematically make use of existing best practices and lessons learned in other Member States or globally. This translates into **information gaps** on help resources, gaps in specialised support, and **overall inefficiency** of efforts.
- Unclear effectiveness. There is little data on whether survivors have access to appropriate support, and existing research suggests that the level of satisfaction with support received is low[140].

Box 8: main sources of evidence on current efforts on prevention and assistance to victims

The CSA Directive requires Member States to put in place prevention measures of programmes of the two main types described in section 2.1.1. (i.e. programmes focused on children or on possible offenders), as well as assistance to victims measures. The Commission has been **monitoring the transposition of the CSA Directive since 2013**, when the deadline for Member States to transpose it expired. One of the main challenges for Member States concern the transposition of the articles concerning **prevention and assistance to victims**[141].

Member States have generally struggled to put in place the required prevention programmes or measures, in particular those for offenders and for people who fear that they might offend, as well as assistance to victims programmes. In some cases, these **programmes have not been put in place yet and in others they are in place but they do not fully comply with the requirements of the Directive**. The Commission organised six dedicated workshops in 2018 and 2019 to support Member States in the transposition of these and other provisions and better understand the challenges.

These workshops, together with additional bilateral exchanges between the Commission and Member States, revealed a need for **more structured and continuous support**, as some aspects of prevention and assistance to victims have not been traditionally an area of focus for Member States' action in the fight against CSA. The shortcomings typically originate in a **lack of expertise in relevant areas, as well as difficulties in communication and coordination between key actors**, e.g. different ministries. In particular when it comes to measures targeting (potential) offenders, there remains significant room for improvement.

---

138 Seto, M.; Letourneau, E.; Overview of perpetrator prevention evidence and existing programmes, October 19, 2021.

139 Unicef, Action to end Child Sexual Abuse and Exploitation: A Review of the Evidence 2020, 2020.

140 For example, a recent study by the Dutch hotline EOKM shows that 81.7% of the boys who had been victims of sextortion and were in touch with a counsellor were not satisfied with the support received.

141 Report from the Commission assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 871 final.

In addition to the evidence gathered through monitoring the transposition of the Directive and supporting its implementation, the **feedback from stakeholders** during the consultation activities, in particular NGOs focused on child's rights, shows the need for improving awareness and education of children, parents, and caregivers. This feedback also included the need for improving the availability of effective prevention programmes for offenders and persons who fear that they might offend, as well as the assistance to victims' programmes[142].

2.3. How likely is the problem to persist?

The problem of CSA is likely to continue **worsening,** driven by the issues identified in the problem drivers section.

Children will continue to spend more time online and thus be more **exposed to predators** operating online. Similarly, predators will most likely also be spending more time online than before, as teleworking arrangements expand and become part of the post-pandemic new normal, and in response to the increase in opportunities to encounter children online.

Relevant services **will continue to be misused** for the purpose of CSA, in particular those that do not adopt meaningful **voluntary measures**. It is unrealistic to expect that, in the absence of incentives or obligations, the relevant service providers would implement sufficient voluntary measures, given that **many have failed to do so to date** despite the evident proliferation of CSA online. Images and videos will continue to stay online. Smaller players in particular will continue to be dissuaded by the **lack of legal certainty**. The fragemented legal framework can also lead to **high compliance and operational costs** for all service providers offering their services in the EU, since their obligations might differ and be more burdensome in one Member State than in another.

In the absence of EU action, Member States will see a need to step up and fill the gap, as some have already done or are in the process of doing. The **increasing legal fragmentation** concerning obligations on service providers to detect and report CSA online (known and new material and grooming) and to remove that material, as well as the **uneven application of voluntary measures**, would continue, in particular after the Interim Regulation expires. There are already inefficiencies in public-private cooperation between online service providers and public authorities (such as law enforcement authorities) in exchanging information in a timely manner or swiftly reacting to requests and complaints. This hampers investigations and creates obstacles to addressing child sexual abuse online and to protecting victims. Such inefficiencies would continue and potentially escalate as the overall volume of illegal activity and content grows

The current technical solutions used to detect CSA online do not function in E2EE electronic communications. It is likely that more service providers would incorporate **end-to-end encryption** without effective measures to protect children. Encryption is an essential tool for ensuring cybersecurity and the protection of users' fundamental rights such as freedom of expression, privacy and personal data, but at the same time makes the detection of CSA online (and therefore the protection of fundamental rights of the child) much more difficult, if not impossible. This could result in more online 'safe havens' where offenders can freely exchange CSAM without fear of discovery and reprisal, normalise these crimes, actively encourage others to abuse children to generate new material, and where children may be groomed and abused online.

[142] Targeted online roundtable with NGOs and feedback from open public consultation (see annex 2, section 3).

It is unlikely that, across the board, companies will unilaterally divert investment into developing **technical solutions** that allow reliable detection of CSA in encrypted systems, as well as a high level of privacy and protection of other fundamental rights, security against unauthorised access and transparency (see Annex 9 for a possible set of assessment criteria for these technical solutions). Deployment of these technical solutions would require financial resources to develop the solution for feasible deployment at scale and align it with companies' current infrastructures. Smaller companies with limited resources are especially likely to encounter more difficulties, since work in this area is relatively novel and technical tools although available, must be tailored to the specific service.

An example of the development of these tools is the announcement of new 'Child Safety' initiatives[143] by **Apple**. Apple is working towards deploying technical tools to detect known CSAM on users' devices prior to encryption and storage in the cloud. The solution uses well-developed hashing technology to generate a hash of the image the user is uploading and match it against a database of hashes of verified CSAM (see Annex 8). This takes place on the user's device prior to the image being encrypted, and does not interfere with the encryption safeguarding the transfer of data, preserving in this respect the privacy and security of data, and allowing detection of known CSAM.

However, a number of companies and privacy NGOs state that there is no possibility to deploy such tools to detect CSA in the context of encrypted electronic communications that would ensure protection of privacy and security of communications. While they do not interfere with the encryption as such, these tools are seen as violating the spirit of end-to-end encryption to the extent that it suggests a wholly private exchange where even illegal content is shielded, for the benefit of ensuring everyone's privacy. It is therefore likely that spontaneous developments in encrypted communications that take into consideration children's safety and privacy and all fundamental rights at stake will **remain limited**, given in particular the legal uncertainty and vocal opposition from some stakeholders.

As children will be increasingly exposed to predators online, **prevention** will play a particularly important role. Parents and children will need the knowledge and tools to protect themselves. Without a solid and structured approach to awareness raising and education to benefit children, parents and caregivers, children will continue to fall victim to sexual abuse in greater numbers. This concerns both online abuse, which may be followed by crimes committed offline, but it applies also to purely offline abuse. While awareness of the problem is currently on the rise in a number of Member States when it comes to abuse in organised sports or other activities targeting children, an effective and systematic prevention response is still lacking. Whether sexual abuse takes place offline or online, children will therefore often continue to lack information on where to seek help, and the adults around them will not be in a position to notice or remedy the problem.

On the opposite side of the problem, people who are attracted to children will continue using the online space to find victims. Those who may want to seek support to overcome this attraction will often not dare to come forward in fear of legal consequences and social stigma. Instead, they will likely continue to seek information online, and often become drawn in by other predators into committing crimes, rather than finding professional help. Therefore,

[143] For more information see Apple's post on Expanded Protections for Children. On September 3 2021, Apple announced that it would delay the implementation of the tools to gather additional feedback before deploying them. At the time of writing, two of the three tools announced have been deployed (a tool to detect nudity in Messages, and expanded guidance in Siri, Spotlight, and Safari Search, whereas the tool to detect known CSAM remains to be deployed.

initiatives addressing more apparent aspects of prevention, such as awareness raising initiatives, will not be enough to address the entire problem, and the CSA issue is likely to continue growing. While there are some initiatives that reach out to persons who fear they may offend, without EU-level support and coordination, they will likely continue to be limited, unevenly distributed and of varying effectiveness.

Increased online activity and consequent exposure of children to predators will unavoidably result in **more victims**. Victims will continue having difficulties to access **long-term assistance**. Without more developed support system in all EU Member States, the situation of victims will continue to vary. However, even in Member States with more advanced support systems, many victims will be left to face the psychological, physical and economic consequences of CSA without proper assistance, once the immediate proceedings around the crime are closed. In cases where the crime is never reported, victims and their families may not know where to seek help, or that they should be entitled to it.

Another problem that the victims will likely continue to face on their own are efforts to have their **images and videos taken down** swiftly and effectively. As this is rather a matter of practical action against illegal content rather than of harmonised criminal law, it could not adequately be addressed in a revision of the CSA Directive or the Victims' Rights Directive[144], and it is too specific of a problem to have been included in the DSA proposal. As long as there is no proactive search for these images and videos, they will often stay online.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

In accordance with settled case law by the Court of Justice of the EU, the legal basis of a legislative initiative has to be determined in light of the content and aim of the envisaged measures. Given that these measures are in part still under assessment, at this stage, no definitive conclusions can yet be drawn in this respect.

That said, given the problems that this impact assessment is addressing and the solutions proposed, Article 114 TFEU was identified as the most likely legal basis for an EU intervention. Article 114 TFEU is the basis for measures which have as their object the establishment and functioning of the internal market. In particular, Article 114 is the appropriate legal basis to address differences between provisions of Member States' laws which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market, and to prevent the emergence of future obstacles to trade resulting from differences in the way national laws have developed[145].

This initiative aims to ensure the proper functioning of the internal market, including through the harmonisation of rules and obligations concerning certain online service providers in relation to providing services which are at high risk of being used for child sexual abuse and exploitation online. As highlighted above under Section 2.2.2, Member States have started taking action unilaterally, adopting or considering rules to deal with the challenge posed by child sexual abuse online, which are necessarily national in scope and risk fragmenting the Digital Single Market. This initiative aims to ensure common rules creating the best conditions for maintaining a safe online environment with responsible and accountable behaviour of service providers. At the same time, the intervention provides for the appropriate

[144] Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, OJ L 315, 14.11.2012.

[145] See, C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.

supervision of relevant service providers and cooperation between authorities at EU level, with the involvement and support of the EU Centre where appropriate. As such, the initiative should increase legal certainty, trust, innovation and growth in the single market for digital services.

Articles 82 and 83 TFEU, which constitute the legal basis for the CSA Directive, provide a basis for criminal law rules concerning, inter alia, the rights of victims of crime and the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension such as sexual exploitation of children. As the present initiative would not seek to harmonise criminal law, Articles 82 and 83 TFEU are not the appropriate legal basis.

3.2. Subsidiarity: necessity of EU action

A satisfactory improvement as regards the rules applicable to relevant online service providers active on the internal market aimed at stepping up the fight against CSA **cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way**. In particular, a single Member State cannot effectively prevent or stop the circulation online of a CSA image or video, or the online grooming of a child, without the ability to cooperate and coordinate with the private entities who provide services in several (if not all) Member States. As presented above under Section 2.1., several Member States took, or in the process of taking, the initiative to adopt national laws in order to step up against the proliferation of CSA online. Although these approaches share the same objective, their way of achieving that objective is somewhat different, targeting for instance different types of services and introducing varying requirements and different enforcement measures.

In the absence of EU action, Member States would have to keep adopting individual national laws to respond to current and emerging challenges with the likely consequence of **fragmentation and diverging laws** likely to negatively affect the **internal market**, particularly with regard to online service providers active in more than one Member State (see problem driver section 2.2.2.). Individual action at Member State level would also fail to provide a unified system for cooperation in the fight against these crimes between public authorities and service providers, leaving them to deal with different legal systems and diverging rules instead of one harmonised approach.

This initiative would build on the DSA proposal, which creates a harmonised baseline for addressing all illegal content, to create a **coherent system throughout the EU** for the specific case of CSA content, which is characterised in particular by its non-public nature and the gravity of the crimes. Such a coherent system cannot be achieved at Member State level, as also set out in detail in the Impact Assessment accompanying the DSA proposal[146].

3.3. Subsidiarity: added value of EU action

Reduce fragmentation and compliance/operational costs, improving the functioning of the internal market

Legal fragmentation (divergence in national legislation to address these issues) increases **compliance and operational costs** of the actions in the fight against CSA for stakeholders such as online service providers that operate in several Member States and may lead to legal uncertainty in particular when the fragmentation also causes **conflicts of laws**. EU action would provide **legal certainty** and a **coherent approach** applicable to entities operating in

[146] Impact Assessment accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, SWD (2020) 348 final.

several Member States, facilitating the scaling up and streamlining of their efforts in the fight against CSA and improving the functioning of the **Digital Single Market**.

Given the **cross-border** aspects of the problem, having regard to the inherent cross-border nature of the Internet and to the many services provided online, the **number of policy areas** concerned (single market for digital services policy, criminal law, economic issues, and fundamental rights including the rights of the child, freedom of expression, privacy and data protection), and the **large range of stakeholders**, the **EU seems the most appropriate level** to address the identified problems and limit legal fragmentation. As previously described, CSA, in particular in its online aspects, frequently involves situations where the victim, the abuser, and the online service provider are **all under different national legal frameworks, within the EU and beyond**. As a result, it can be very challenging for single countries to effectively define the role of and cooperation with online service providers without common rules and without fragmenting the Single Market (see problem driver section 2.2.2.).

Facilitate and support Member States' action on prevention and assistance to victims to increase efficiency and effectiveness

While Member States are best placed to assess the gaps and needs, and implement action in their local context, they often lack information on what prevention and assistance to victims programmes are available, how effective they are, and how to approach their implementation in practice – who needs to be involved, what are the technical and legal pre-requisites and estimated costs. EU level action can provide a forum for exchange of necessary information and expertise to avoid duplication of efforts and blind spots. EU action can also help identify best practices and lessons learned at national level (from Member States or third countries) and incorporate them into EU-level initiatives, so that **other Member States can benefit from them**. This may also **prevent a "whack-a-mole"** effect in which a Member State successfully addresses a problem in its territory but **the problem just moves to another Member State** (e.g. hosting of CSAM online).

While some exchange in this area exists, the feedback from experts in the field indicates there is a need for a structured framework for such exchanges. EU level action promoting and disseminating research would help to enrich the evidence base in both areas and could possibly even link initiatives across Member States, boosting efforts. EU action could also include practical support to local interventions, e.g. translations of existing materials from another Member State, possibly leading to significant cost savings at national level.

The EU level action on prevention and assistance to victims at issue here would **not impose any additional obligations** beyond those included in the CSA Directive. Indeed, the main focus of the present initiative is on strengthening the functioning of the internal market by setting common rules aimed at combating the misuse of online services for CSA-related purposes. Nonetheless, the action could also contribute to **facilitating and supporting** Member States' work to comply with the existing obligations, notably through the sharing of expertise and best practices benefitting from the central position it occupies in connection to its principal tasks regarding the detection and reporting of online CSA.

Reduce dependence on and facilitate cooperation with third countries

Currently, in practice, law enforcement authorities of the Member States **depend almost entirely on NCMEC**, a private organisation located in the US, as the main source of reports of CSA online. EU action could ensure, among others, that such dependence is reduced and that the detection, reporting and removal of CSA online is done **through EU mechanisms that operate according to EU rules**, including the necessary **safeguards**. In addition, EU

mechanisms could be more closely linked to what is illegal in the EU and its Member States, rather than relying on definitions from third-country jurisdictions. This would enhance the precision of efforts, reduce the impact on third parties, and better target measures.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objective

The general objective is to improve the functioning of the internal market by introducing clear, uniform and balanced EU rules to prevent and combat CSA, notably through imposing detection, reporting and removal obligations on certain online service providers.

4.2. Specific objectives

There are 3 specific objectives that address the problem drivers identified in section 2.2.:

1. Ensure the effective **detection, reporting and removal** of online CSA where they are **currently missing.** This specific objective is of particular relevance to problem driver 1, as the current voluntary action by online service providers and under diverging national laws is insufficient to effectively detect, report and remove CSA online across the EU, i.e. by not detecting some crimes or by not being effective in dealing with those detected. It is also of relevance to problem driver 2, since part of the current inefficiencies in the detection, reporting and removal process are due to inefficiencies in public-private cooperation.
2. Improve **legal certainty, transparency and accountability and** ensure **protection of fundamental rights**. This specific objective is of particular relevance to problem driver 1, as the current voluntary action by online service providers and the action taken under diverging national laws is not sustained on a clear, uniform and balanced EU-level framework that provides long-term legal certainty, transparency and accountability and ensures protection of fundamental rights. This objective therefore reflects the need to create a **clear framework**, with the appropriate safeguards to ensure **respect for children's rights and all users' rights**, including the right to freedom of expression, right to private life and communications as well as data protection, and to provide regular information about its functioning, including e.g. **transparency reports on technologies used** for the identification of CSA content.
3. Reduce the **proliferation and effects** of CSA through harmonisation of rules and **increased coordination** of efforts. This specific objective is of particular relevance to problem drivers 2 and 3. Coordination issues are at the core of the inefficiencies in public-private cooperation in problem driver 2, and improved coordination could boost Member States' efforts on prevention and assistance to victims.

Contribution to relevant SDGs

The three specific objectives directly contribute to achieving the most relevant SDGs for this initiative, 5.2., eliminate all forms of violence against women and girls, and 16.2., end abuse, exploitation, trafficking and all forms of violence against children.

Specific objectives 1 and 3 also directly contribute to achieving other SDGs of relevance, such as SDG 1 on poverty and SDG 3 on health, by reducing the proliferation and effects of CSA and ensure the detection, reporting and removal on CSA online where it is currently missing. Contributing to prevent and/or stop the abuse can reduce the negative consequences on health, including mental health, which may have a negative impact on the economic future

of the child (e.g. through substance abuse or decreased productivity). Specific objective 3 helps achieve SDG 4 on education (e.g. through the awareness raising campaigns or the exchange of related best practices facilitated by the EU Centre). Finally, specific objective 2 helps achieve SDG 9 on industry, innovation and infrastructure (e.g. as the initiative aims to support service providers efforts to fight against CSA online, including through increasing legal certainty and the required safeguards that do not hamper innovation on the technologies to detect, report and remove CSA online).

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

In the **baseline scenario** no further EU policy action is taken. The following section assesses the most likely scenario in the absence of the initiative, i.e. how the existing and already planned policy instruments would address the problems and objectives for EU action identified:

1. Legislation

Existing and upcoming EU legislation is not likely to effectively address challenges in detection, reporting and removal of CSA online and prevention of CSA, and assistance to victims. The proliferation of CSA online would be expected to continue in line with current developments. Specifically, the **added value** (i.e. what it can achieve **in preventing and combatting CSA) and the limitations** of the existing and upcoming EU legal instruments are the following:

Horizontal instruments

The GDPR:

- **What it can achieve** in the fight against CSA: online service providers have relied on legal bases in the GDPR for the processing of personal data required in relation to their **voluntary** activities to combat CSA online, e.g. under e.g. legitimate interest (Art 6(1)(f)) or vital interest (Art. 6(1)(d)) considerations.
- **Limitations**: the GDPR as a horizontal instrument does not contain CSA-specific provisions, i.e. provisions that explicitly allow or mandate the processing of personal data for the purpose of combatting CSA online.

The ePrivacy Directive and its proposed revision

- **What it can achieve** in the fight against CSA: the ePrivacy Directive and its proposed revision allow restrictions of certain rights and obligations under their scope, inter alia to prevent or prosecute CSA. Such restrictions require a proportionate legislative measure, under national or EU law. With the entry into force of the Interim Regulation, subject to compliance with a set of conditions, certain rights and obligations are temporarily limited (Articles 5(1) and 6(1) of the ePrivacy Directive for certain providers of online communications services), for the sole purpose of detecting and reporting CSA online and removing CSAM.
- **Limitations**: As horizontal instruments, the ePrivacy Directive and its proposed revision do not contain CSA-specific provisions. Member States are notably responsible for enforcement through their competent national authorities (see also Interim Regulation below).

The eCommerce Directive

- **What it can achieve** in the fight against CSA: with regard to hosting services, the eCommerce Directive is notably the basis for the notice and action mechanism in which parties such as users or hotlines notify online service providers of the presence of CSAM available in their services, so that it can be removed.
- **Limitations**: the eCommerce Directive does not contain CSA-specific provisions, i.e. provisions that explicitly enable or oblige online service providers to detect, report or remove CSA online. Furthermore, as noted, while failure to act expeditiously can lead to the hosting service providers not being able to invoke the liability exemption (and could thus be held liable under national law), there is no legal obligation upon the service providers to act, even when notified of manifestly illegal CSA.

The Digital Services Act

- **What it can achieve** in the fight against CSA: the **DSA proposal**[147], once adopted, will:
    - provide a horizontal standard of obligations for content moderation by providers of intermediary services; eliminate disincentives for these providers' voluntary efforts to detect, identify and remove, or disable access to illegal content; and create obligations for them to provide information on their content moderation activities and on their users when requested by national authorities. These provisions are likely to encourage providers to implement voluntary measures and will also create more transparency and accountability for providers' content moderation efforts in general;
    - create due diligence obligations tailored to certain specific categories of providers (notice and action mechanism[148], statement of reasons, internal complaint-handling system, reacting swiftly to notices issued by trusted flaggers, notification of suspicions of criminal offences etc.) and transparency reporting obligations. In particular, it will oblige very large platforms to assess risks and implement the necessary risk mitigation measures on their services. These measures will encourage users and trusted flaggers to report suspected illegal content and providers to follow-up on these reports more swiftly. The obligations on very large platforms are also likely to contribute to lessening the prevalence of illegal content online and users' exposure to such content;
    - establish rules on its own implementation and enforcement, including as regards the cooperation of and coordination between the competent authorities. This can lead to faster and more efficient content moderation efforts across the EU, including with regard to CSAM.
- **Limitations**. Due to its general and horizontal nature and focus on public-facing content, the DSA only addresses the issue of CSA partially. Its approach is appropriate for the wide range of heterogeneous illegal content for which the DSA sets the overall baseline, but it does not fully address the particular issues concerning the detection, reporting and removal of CSA online. Specifically:
    - **Voluntary detection**: the DSA does **not specify the conditions** for the processing of personal data for the purpose of voluntarily detecting CSA online;
    - **Mandatory detection**: the DSA does **not include any obligation** to detect CSA online. Obligations to carry out **risk assessments** and take effective **risk**

147 Impact Assessment accompanying the DSA proposal, SWD(2020) 348 final, December 2020.

148 The DSA proposal includes an obligation on providers of hosting services to process the notice received (e.g. by hotlines combatting CSAM), including taking a decision on any follow-up to it, and the possibility of sanctions for non-compliance.

mitigating measures, as applicable, apply only to the largest online platforms, consistent with their general nature;

- **Reporting**: although it contains some provisions in this respect, the DSA does **not provide for a comprehensive CSA reporting obligation,** since it focuses on cases where an offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place. Also, given the diverse nature of content that could be concerned, the DSA does not determine specific reporting requirements (i.e. what minimum information should the report contain) and does not provide for the involvement of a body like the EU Centre in the reporting process.
- **Removal**: like the eCommerce Directive (see above), the DSA sets out liability exemptions that encourage removal, it but does **not include** any removal obligations[149].

In particular, while the DSA, once adopted, should show significant impact especially when it comes to publicly accessible content, its effect is likely to be less pronounced on content exchanged secretly and in non-public channels (e.g. in interpersonal communications), as is typical for the majority of CSA online. Considering this and the above limitations, the DSA will not eliminate the **risks of legal fragmentation** introduced by the national initiatives on combatting CSA online. These are likely to provide a more specific and targeted approach than the DSA, and partially targeting different services, in order to ensure an effective and targeted response to CSA online.

The Victims' Rights Directive

- **What it can achieve** in the fight against CSA: as a horizontal instrument, the Victims' Rights Directive covers the assistance, support and protection to all victims of crime. The CSA Directive contains additional specific rules that respond more directly to the specific needs of CSA victims.
- **Limitations**: the Victims' Rights Directive refers to the need to cooperate with other Member States to improve the access of victims to the rights set out in the Directive but it does not contain specific mechanisms to do so. And, as mentioned above, this Directive does not address only CSA victims, for which dedicated mechanisms to facilitate the exchange of best practices, which take into account their specific needs, may be required.

Sector-specific legislation

The Child Sexual Abuse Directive

- **What it can achieve** in the fight against CSA: the CSA Directive focuses on defining the role of Member States and their public authorities in preventing and combating these crimes, and to assist victims. Specifically, the Directive defines criminal behaviour online and offline, sets the minimum level of maximum sanctions, and requires Member States to ensure adequate assistance and support to victims, as well as to put in place prevention measures.
- **Limitations**: as a criminal law instrument, the CSA Directive does not aim to regulate online service providers and so it does not provide sufficient specification of the role of

[149] The DSA proposal (and the e-Commerce Directive) establish the conditions under which a service provider **cannot be held liable** in relation to illegal content in its services and not the conditions under which a provider can be held liable, as this is up to national or EU law (such as this proposal on CSA) to determine.

service providers and the procedures to apply. In addition, the scope of the actual obligation (as a criminal law instrument) has to be limited to the own territory, which makes it a less effective tool given the global nature of the Internet.

The Interim Regulation

- **What it can achieve** in the fight against CSA: it makes it possible for providers of number-independent interpersonal communications services to **continue or resume their voluntary measures** to detect and report CSA online and remove CSAM, provided they are lawful and, in particular, meet the conditions set.
- **Limitations**: as a **temporary** measure with the aim of bridging the period until long-term legislation (that is, the present initiative) is put in place, it applies only for **three years** (until 3 August 2024) and does **not establish a legal basis** for any processing of personal data. The service providers within the scope of the Interim Regulation would therefore not be able to continue their voluntary activities when the Regulation ceases to apply. In addition, the Interim Regulation is not suitable to offer a long-term solution, since it only addresses one specific part of the problem, for a limited subset of services (number independent interpersonal communication services), and relies fully on voluntary approaches.

The Europol Regulation and its proposed revision

- **What it can achieve** in the fight against CSA: the **revised mandate of Europol** should enable Europol, in cases where private parties hold information relevant for preventing and combatting crime, to directly receive, and in specific circumstances, exchange personal data with private parties. Europol would analyse this data to identify all Member States concerned and provide them with the information necessary to establish their jurisdiction. To this end, Europol should be able to receive personal data from private parties, inform such private parties of missing information, and ask Member States to request other private parties to share further additional information. These rules would also introduce the possibility for Europol to act as a technical channel for exchanges between Member States and private parties. Such a development would contribute to increasing the level of cooperation between the three aforementioned stakeholders, potentially improving the effectiveness of CSA investigations.
- **Limitations**: in and of itself, the revised mandate of Europol will not contribute to a comprehensive solution to address CSA online, which requires a multi-faceted approach. Enabling a more efficient exchange of personal data between Europol and private parties is a necessary but not a sufficient condition for achieving this objective.

2. Coordination

EU level cooperation in investigations

- **What it can achieve** in the fight against CSA: the existing EU level cooperation in investigations has produced significant successes in the fight against CSA[150] and will likely continue to do so.
- **Limitations**: the ability of Europol and law enforcement agencies in the EU to cooperate in investigations is limited by the resources that they can allocate to this crime area. For example, Europol has only been able to examine 20% of the 50 million unique CSAM

[150] See for example here and here.

images and videos in its database[151]. The EU Centre could play an important role in supporting Europol in these tasks.

EU level cooperation in prevention

- **What it can achieve** in the fight against CSA: the **network of experts on prevention** will continue developing and adding more members, both researchers and practitioners, mostly from the EU but also globally, so that it can ultimately support Member States in implementing the prevention articles of the CSA Directive.
- **Limitations**: currently, the Commission services themselves are supporting the work of the network by coordinating its work and providing a secretariat. However, there are limits to the level of support these services can provide to the network, in particular as the network expands. The activities of the network could therefore be constrained to a level that would not allow it to reach its full potential of support to Member States.

EU level cooperation in assistance to victims

- **What it can achieve** in the fight against CSA: the Victims' Rights platform would faciliate the exchange of best practices mostly on **horizontal** issues related to victims' rights, and mostly on **policy-related** issues,
- **Limitations**: the focus on horizontal issues could limit the effectiveness of the platform for CSA victims, given the specificities of these crimes and their short- and long-term effects on victims.

Multi-stakeholder cooperation at EU and global level

- **What it can achieve** in the fight against CSA: at EU level, the EU Internet Forum (EUIF) has faciliated discussion between public authorities and online service providers in the EU in the fight against CSA at all levels, from ministerial to technical (see annex 8 for an example of output of technical discussions under the EUIF). It is expected that similar discussions continue in the future.
  At global level, the WPGA has advanced countries' commitment towards a more coordinated response to the global fight against CSA, based on global threat assessments, and a model national response. These have helped to clarify the challenges and assist member countries in setting achievable practical goals, and it is expected that they will continue to do so in the future.
- **Limitations**: at EU level, the focus of the EUIF is to faciliate targeted exchanges between public authorities and online service providers. The forum is not designed for discussions with a wider variety of stakeholders, including practitioners. Moreover, participation is voluntary and there are no legally binding obligations.
  At global level, the EU will continue supporting global efforts through the WPGA. In the absence of a single European information hub, exchanges of expertise and best practices with leading centres worldwide (e.g Australian Centre to Counter Child Exploitation, NCMEC, Canadian Centre for Child Protection) will be limited. This will in particular concern initiatives on prevention and assistance to victims, leaving EU Member States to their own devices.

3. Funding

- **What it can achieve** in the fight against CSA: action using EU funding is likely to continue in the current project-based form, both as calls for proposals as well as research

[151] European Parliament Intergroup on Children's Rights expert meeting on EU legislation on the fight against child sex abuse online, 15 October 2020, see 59:29.

projects. EU-funded projects will continue to facilitate development of e.g. relevant IT tools for law enforcement and interventions aimed at preventing CSA and helping victims.

- **Limitations**: the current project-based efforts would be extended from grant to grant without long-term sustainability. Such long-term perspective may be supported by individual Member States with a national focus, but a comprehensive EU-wide approach and reinforced framework will continue to be lacking. The risk of projects duplicating existing efforts, will still be high; moreover, the update of successful projects will likely remain limited to participating countries.

***

In summary, the existence and magnitude of the problem suggests that the **existing policy instruments** in the fight against CSA (legislation, coordination and funding) are not sufficient to ensure an effective response:

- **Legislation**: the horizontal instruments (such as the eCommerce Directive, the ePrivacy Directive and its proposed revision or the DSA proposal) address some of the problems and challenges but, given the specific challenges of CSA, can only provide limited and partial solutions. The sectoral instruments (the CSA Directive, the Europol Regulation or the Interim Regulation) focus on particular aspects of the problem such as harmonisation of criminal laws or improving police investigations, which again by themselves are not able to provide a comprehensive EU-level solution. Also, none of these instruments define the role of service providers in combating child sexual abuse specifically enough to provide them with legal certainty and do not include effective obligations for the providers relevant to the fight against child sexual abuse.
- **Coordination**: inefficiencies persist despite the existing mechanisms, particularly in some areas of prevention and assistance to victims. The sharing of best practices and expertise between Member States is minimal and unsystematic. The current level of ambition and of collaboration between the various public and private stakeholders results in ad-hoc and temporary solutions and is rarely effective in addressing CSA. As a result, Member States have been facing difficulties in fulfilling some of their obligations under the CSA Directive, which ultimately means that prevention measures are not sufficient to protect children and stop offenders from committing crimes, and victims do not receive appropriate support.
- **Funding**: action using EU funding is mostly project-based, and the uptake of EU funding is not optimal. For example, some Member States do not always make use of the funds available to them to tackle CSA (e.g. through the Internal Security Fund national programmes), possibly due to lack of knowledge on what funding is available and where it could be applied. Projects that take place, either national or cross-border, run the risk of replicating what has already been done due to lack of coordination.

Considering the above, the **most likely scenario in the absence of the initiative** (long-term solution) would include the following:

- following the end of the period of application of the Interim Regulation (three years after its entry into force), and in the absence of other legislation of this kind at EU or Member State level, providers of number-independent interpersonal communications services would **no longer be permitted** to detect and report CSA, and would not be able to continue deploying their voluntary measures with the adequate safeguards protecting users' fundamental rights, while the proliferation of CSA online would continue. As such service providers are currently the source of the majority of reports

made by service providers[152], the number of such reports (and therefore overall reports) could eventually decrease significantly;

- a similar drop in reports could be expected with the broader deployment of E2EE by default in these services;
- Member States' law enforcement authorities would continue to receive the (fewer) reports through NCMEC, submitted by a small number of service providers and assessed in accordance with US law, which has different definitions of illegal content than EU law. The quality of the reports would remain at today's levels;
- victims' images and videos will continue to circulate online. Law enforcement authorities will be **unaware of the undetected crimes** and unable to identify and rescue victims and investigate and prosecute these cases;
- the full potential of the hotlines would remain underutilised as they would continue to lack a legal basis to search for CSAM proactively, despite the higher effectiveness compared to being totally dependent on users' reports;
- without **harmonised standards** on the responsibilities and actions expected from service providers in the fight against CSA, their different approaches will fail to offer a **reliable standard** for the protection of users' rights[153];
- the worsening situation would increase pressure on Member States to take action **on a national level** once the Interim Regulation expires to address the legal vacuum creating a risk of further **fragmentation** of the Single Market. A patchwork of national measures would **not effectively protect children**, given the cross-border and international dimension of the issues, and would create **distortions** in the functioning of the **single market for digital services.** While these will be partially addressed by the DSA, once adopted, a significant degree of fragmentation is expected to persist and possibly grow, given the manifestly illegal nature of CSAM and the specific channels for its dissemination and proliferation (see problem driver section 2.2.2.);
- without further EU facilitation of efforts, Member States' action on **prevention and assistance to CSA victims** is not likely to significantly improve. The sharing of best practices between Member States will continue to be punctual and unstructured, an the current limitations in effectiveness of existing programmes are likely to persist, as well as the **duplication of efforts**.

Baseline costs

In the baseline scenario, no costs would be incurred by the creation and running of the Centre or any new organisation. However, the **inefficiencies** in the prevention, investigation and assistance to victims of child sexual abuse are expected to have a negative economic impact on society. A higher number of victims will experience a diminished quality of life, likely resulting also in productivity loss, and will require significant support, putting a strain on public services.

The economic impact on public authorities will depend upon the level of action taken by service providers, which will dictate the number of reports received by those authorities. The economic impact on service providers will depend on their level of engagement against these crimes. The existing **legal fragmentation and legal uncertainty** would remain and could act as a barrier to growth and innovation within the single market for digital services and hamper

[152] See section 2 and annex 6, section 2.

[153] As noted in the impact assessment for the DSA, in the absence of a targeted regulatory framework, companies are setting and enforcing the rules themselves, driven mainly by their commercial interests and not consistently addressing the societal concerns inherent to the digital transformation they are enabling.

the fight against CSA. In the absence of a central hub fragmented efforts would continue, driving up the economic costs for individual entities.

As seen in box 4, the impact of CSA on its victims generates significant costs. Assuming similar costs and prevalence of CSA in the US as in the EU, adjusting for the larger population in the EU, the estimated annual CSA costs in the EU (and therefore the **cost of no action**) is **EUR 13.8 billion**[154].

5.2. Description of the policy options

In the determination of available policy options, three main considerations played a decisive role.

First, there are **important rights at stake:** on the one side, the rights of the child to be protected and the interest in preventing the circulation of CSAM as illegal content violating the intimacy and right to privacy of the victim; on the other side, the rights of all users especially to freedom of expression, privacy of communications and data protection. Naturally, the rights and interests of the providers, such as freedom to conduct business, are to be taken into account as well.

Second, offenders have proven savvy at moving to services that are less effective in detecting CSA online. Consequently, the policy options need to ensure an **even application of the rules**, in order to avoid simply pushing the problem off from one platform and onto another.

Third, more effective measures may not amount to imposing a **general obligation** on providers of intermediary services **to monitor** the information which they transmit or store, **nor actively to seek facts** or circumstances indicating illegal activity. The Commission has recently confirmed its commitment to this principle, as reflected at present in Article 15(1) of the e-Commerce Directive[155] and in Article 7 of the DSA proposal.

Box 9: prohibition of general monitoring obligations

The exact meaning and extent of the prohibition to impose a general monitoring obligation is only gradually becoming clear. A case-by-case assessment is required to determine whether in a given situation the prohibition is respected or violated. The Court of Justice of the EU (CJEU), in its case law, has indicated certain criteria for deciding whether an obligation to monitor the information which intermediary service providers transmit, or to actively seek facts or circumstances indicating illegal activity, is to be considered general and thus prohibited. Thus far, the CJEU has dealt with this question in the context of copyright infringement and defamation, where the illegality or not of content may not be immediately apparent. It has not yet had to assess a similar obligation with regard to manifestly illegal content such as most CSAM. Also, the case law available thus far relates to obligations resulting from orders based on national law, not EU legislation. The precise content and scope of the obligations in question are naturally also an important factor to be considered.

Based on the case law of the CJEU, it is required that a fair balance be struck between all relevant and conflicting fundamental rights as stake, such as those mentioned above. For instance, it ruled[156], in the context of combating intellectual property rights infringements, that it is not allowed to impose an obligation which cumulatively meets the following conditions:

---

154 Includes direct costs (victims' assistance) and lifelong loss of potential earnings and productivity, see section 6.2.2. on benefits for more details (box 20).

155 OJ L 178, 17.7.2000, p. 1–16.

156 Cases C-70/10 and C-360/10 - SABAM.

- applies for all customers *in abstracto* and as a preventative measure, in particular without further specification of the content to be identified;
- at providers' own cost;
- for an unlimited period; and
- is based on a system for filtering most of the information to identify electronic files (stored on a provider's servers), including future content.

In a different context, namely, an order aimed at tackling a particular item of content that the national court had held to be defamatory, as well as content equivalent thereto, the CJEU ruled[157] in essence that:

- a service provider can in principle be ordered to take measures to detect and remove the item of defamatory content, even if it means monitoring the content provided by other users than the one who had initially posted the content;
- such an obligation can also be extended to content equivalent to the defamatory content, subject however to a number of conditions (only minor differences as compared to the defamatory content, sufficient specifications by the court issuing the order, no need for an independent assessment by the service provider).

All policy options that can be considered therefore need to meet a number of specific requirements in order to limit any interference with fundamental rights to what is strictly necessary and to ensure **proportionality** and compliance with the prohibition of general monitoring obligation:

- Obligations have to be **targeted** to those services which are at **risk of being used** for sharing CSAM or for grooming children.
- They have to strike an **appropriate balance** between the **interests and (fundamental) rights** associated with ensuring an effective approach to combating CSA and protecting children and their rights, on the one hand, and on the other hand the interests and rights of all users, including freedom of expression, privacy of communications and data protection, as well as avoiding an excessive burden on the service provider.
- To ensure that balance, they have to contain appropriate **conditions and safeguards** to ensure **proportionality, transparency and accountability**. Given the significant impact on fundamental rights, the effectiveness of the measures and of these conditions and safeguards should be subject to dedicated monitoring and enforcement mechanisms.

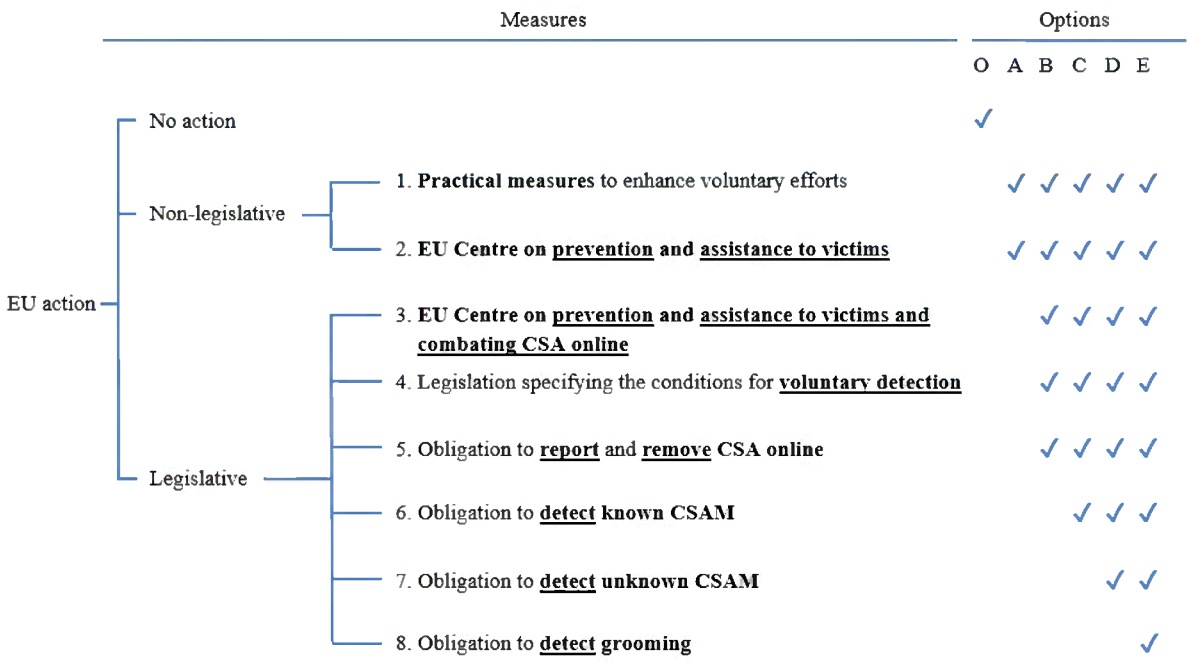
In line with the above requirements, the policy options assessed take a graduated approach, addressing the problem drivers from different angles and in various degrees, with an increasing level of obligations and intrusiveness. This **cumulative logic** was chosen because the measures that form the options not only are not mutually exclusive, but are also **complementary**, presenting **synergies** that the combined options can benefit from.

As a result, in addition to the baseline, **five options** are retained for assessment, as first presented in the intervention logic in table 1. The **building blocks** of these options are the retained policy **measures** that resulted from scoping and analysing the full spectrum of possible EU intervention, from non-legislative action to legislative action.

Figure 3 below shows how the measures combine to form the retained policy options:

[157] Case C-18/18 – Facebook Ireland.

Figure 3: overview of policy options and corresponding measures



The retained policy options were selected for their potential to contribute to creating a level playing field across the EU, lessening legal fragmentation, increasing efficiency in tackling the problem (e.g. by facilitating Member States action through sharing of expertise), and creating more balanced circumstances for all the affected providers, while also contributing to reducing their compliance and operational costs.

*5.2.1. Option A: **practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims,** and establishing an **EU Centre** on **prevention and assistance to victims***

This option is non-legislative and includes **practical measures** to stimulate cross-sectorial cooperation among relevant stakeholders in **prevention and assistance to victims**, and **enhance voluntary detection, reporting and removal** of CSA online by relevant online service providers, within the boundaries of the existing legal framework (measure 1). This option also includes an **EU Centre** to support and facilitate **information sharing** on **prevention and assistance to victims** (measure 2).

1. **Practical (i.e. non legislative) measures** to enhance and support **voluntary efforts** of relevant information society service providers to **detect, report and remove** CSA online, and to enhance **prevention and assistance to victims**. Examples of practical measures to enhance **detection, reporting and removal** include developing codes of conduct and standardised reporting forms for service providers, improving feedback mechanisms and communication channels between public authorities and service providers, and facilitating the sharing of hashes and detection technologies between service providers. Examples of practical measures to enhance **prevention and assistance to victims** include facilitating research and the exchange of best practices, facilitating coordination, and serving as a hub of expertise to support evidence-based policy in prevention and assistance to victims.

2. **EU Centre on prevention and assistance to victims.**

This measure would create an EU-funded **expertise hub**, managed by the Commission with support from a contractor (similar to the **Radicalisation Awareness Network, RAN**[158]). Among others, it would support Member States in implementing the relevant provisions of the CSA Directive (e.g. through expert workshops), and serve as a hub of expertise to support evidence-based policy and avoid duplication of efforts. It would also help develop and disseminate **research and expertise**, and facilitate dialogue among stakeholders. This would allow Member States to benefit from **best practices and lessons learned** in the EU and globally. Having both prevention and assistance to victims in the same hub would increase the possibilities for coherence and cross-fertilisation between both strands of work.

The purpose of **prevention** efforts led by the EU Centre would be to **support Member States** in **putting in place tested and effective prevention measures** that would decrease the prevalence of CSA in the EU and globally. The scope of these efforts would cover the two main types of prevention initiatives, i.e. 1) those that reduce the likelihood that a child becomes a victim (e.g. awareness raising and educational campaigns and materials for schools), and 2) those that reduce the likelihood that a person (re)offends. The Centre would facilitate Member States' action on prevention by serving as a hub of expertise at the service of Member States, notably to help avoid duplication of efforts and to foster an evidence-based approach to prevention policies.

Under the lead of the EU Centre, a **network of experts on prevention** would facilitate the development of these efforts, the involvement of multiple stakeholders and the sharing of best practices and lessons learned across Member States. The network would enable a **virtuous cycle of practice to research and research to practice**, while enabling the **cascading down** of best practices and new developments from EU and global level to national and regional levels. The Centre would support the work of the network by e.g. hosting relevant repositories of best practices, providing statistics and other data relating to the prevalence of offending, offender profiles and pathways, and new crime trends particularly those relating to perpetrators' use of technology to groom and abuse children.

The EU Centre will **not have any power to impose any initiative on prevention** to Member States, i.e. it will not coordinate in the sense of determining "which Member State is obliged to do what". Its tasks in this respect will be ancillary to its principal tasks, which relate to the implementation of the detection and reporting processes.

With regard to **assistance to victims**, the Centre would play a similar role: **facilitate** the implementation of the **practical measures** on assistance to victims by serving as a **hub of expertise** to support the development of evidence-based policy and research on assistance to victims, including victims' needs and the effectiveness of short and long-term assistance programmes. In addition, the Centre could provide resources to help victims **find information** on support that is available to them locally or online. The Centre would not provide assistance to victims directly when those services are already provided or would be best provided at national level, to avoid duplication of efforts. Also, the Centre would serve as a **facilitator** at the service of Member States, including by sharing best practices and existing initiatives across the Union. In that sense, it would facilitate the coordination of Member States' efforts to increase effectiveness and

[158] See here for more information about the Radicalisation Awareness Network. The hub would not take the form of an agency.

efficiency. Similarly to prevention, the Centre will **not have any power to impose any initiative on assistance to victims** to Member States, including on issues concerning health, legal, child protection, education and employment.

The possibility to create an **EU Centre** on prevention and assistance to victims is further explored in Annex 10, as implementation choice A. As existing entities or networks cannot be expected to fulfil this role, a central entity is the most viable solution. The Centre could also help to improve the cooperation between service providers and civil society organisations focusing on prevention efforts.

*5.2.2. Option B: option A + legislation 1) specifying the conditions for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal***

This option combines the non-legislative option A with legislation to improve the **detection, reporting and removal** of CSA online, applicable to service providers offering their services in the EU. It would provide 1) a **long-term regulatory framework for voluntary detection** (measure 4); 2) put in place **mandatory reporting** in case CSA online is found (measure 5); and 3) set up an **EU Centre** to **facilitate detection, reporting and removal of CSA online**, as well as **prevention and assistance to victims** (measure 3).

1) **Legal framework for voluntary detection of CSA online**. This measure would build on and complement the DSA proposal, to address the specific challenges inherent in CSA that cannot be addressed with general systems building on notification by users and trusted flaggers as envisaged by the DSA, and provide a framework for relevant service providers to **voluntarily** detect CSA online, including **known and new CSAM and grooming**. It would replace the **Interim Regulation**, building on its **safeguards** in a more comprehensive framework, covering all relevant services, i.e. also those defined in the DSA and not only the electronic communications services within the scope of the Interim Regulation (i.e.. providers of instant messaging and email). The legal framework would provide increased legal certainty also when it comes to the basis and conditions for processing of personal data for the sole purpose of detection of CSA online.

   Given in particular the impact on fundamental rights of users, such as personal data protection and confidentiality of communications, it would include a number of mandatory **limits and safeguards** for voluntary detection. These would notably include requiring service providers to use technologies and procedures that ensure **accuracy, transparency and accountability**, including supervision by designated national authorities. The legislation could set out the information rights of users and the mechanisms for complaints and legal redress.

   Stakeholders' views from the open public consultation on voluntary measures

   The percentage of responses to the open public consultation from each of the main stakeholder groups that indicated that the upcoming legislation should include voluntary measures to detect, report and remove CSA online was the following: public authorities 25%, service providers 13%, NGOs 9%, and general public 10%. The support for voluntary measures was highest for known material and lowest for grooming (e.g. 11.3% for known material, 9.7% for new material and 6.5% for grooming in the NGO group).

2) **Legal obligation to report CSA online**. Relevant service providers would be required to **report to the EU Centre** any instance of suspected CSA that they become aware of, based on voluntary detection measures or other means, e.g. user reporting. This obligation would build on and complement the reporting obligation set out in Article 21 of the DSA

proposal, covering the reporting of criminal offences beyond those involving a threat to the life or safety of persons (e.g. possession of CSAM). In order to enforce the reporting obligations, competent national authorities in the Member States would be designated. The legislation would also include a number of **conditions** (e.g. to ensure that the reports contain actionable information) and **safeguards** (e.g. to ensure transparency and protection of personal data, see section 5.2.3.).

Legal obligation to remove CSA online. As mentioned earlier, under the eCommerce Directive and the DSA proposal, hosting service providers are required to expeditiously remove (or disable access to) CSAM that they obtain actual knowledge or awareness of, or risk being held liable due to the resulting unavailability of the liability exemptions contained in those acts. Given that this system encourages but not legally ensures removal, it would be complemented by rules ensuring a removal obligation in cases of confirmed CSA online; where necessary, national authorities would be empowered to issue a **removal order** to the concerned providers requiring them to remove the specific CSAM on their services. The rules would be accompanied by the necessary **conditions** (e.g. to ensure that the removal does not interfere with ongoing investigations) and **safeguards** (e.g. to ensure transparency and protection of personal data and freedom of expression), including rules on **redress**. Member States' **national authorities would be competent for enforcement**, relying where relevant also on the expertise of the Centre.

SMEs would also be required to report and remove in accordance with the above rules**,** benefiting however from additional support by the Commission and the Centre through:

- **tools to facilitate the reporting and removal**, made available by the EU Centre **at no cost**, for SMEs to use in their services if they wish, reducing their financial and operative burdens;
- **guidance**, to inform SMEs about the new legal framework and the obligations incumbent on them. This guidance could be disseminated with the help of industry associations; and
- **specific training**, delivered in collaboration with Europol and the national authorities.

3) **EU Centre to prevent and counter CSA**. The Centre would incorporate the supporting functions relating to **prevention and assistance to victims** of measure 2 and add the ability to support the **detection, reporting and removal** efforts, including by helping ensure **transparency and accountability**. Specifically, it would:
   - facilitate **detection** by providing online services clear information on what is CSA in the EU through access to a **database of CSA indicators** (e.g. hashes, AI patterns/classifiers) to detect CSA in their services. The Centre would help create and maintain this database of indicators that would reliably enable the detection of what is defined as CSA **according to EU rules** (notably the CSA Directive), as determined by courts or other independent public authorities. The material would come from multiple sources including previous reports from service providers, concluded investigations by law enforcement, hotlines or direct reports from the public to the EU Centre (e.g. from survivors requesting the Centre for support to have materials depicting their abuse taken down). The Centre would also facilitate access (in particular to SMEs) to free-of-charge technology that meets the highest standards for the reliable, automatic detection of such content;
   - facilitate **reporting**, by becoming the recipient of the reports of CSA concerning the EU that providers detect in their online services. The Centre would serve as an

intermediary between service providers and other public authorities (notably law enforcement authorities), supporting the reporting process by 1) **reviewing the reports** to ensure that those other public authorities do not need to spend time filtering out reports that are not actionable and can make the most effective use of their resources; and 2) **facilitating the communication** between those other public authorities and service providers in case of requests for additional information from public authorities or requests for feedback from service providers (if needed);

- facilitate **removal**, by notifying in certain cases to the service providers materials considered to be known CSAM and requesting removal, as well as following up on these requests. This would entail **supporting victims** that request to have **material** that features them taken down; no such service exists to date. The Centre could also be given a mandate to conduct in certain cases searches of CSAM, using the databases of indicators[159]. The Centre could track whether the removal has taken place. Where removal is not effected in a timely manner, the Centre could refer to national authorities for action (e.g. issuing of removal orders).

Box 10: distribution of tasks between the EU Centre and Member States

Prevention and assistance to victims: the Centre, although this would not constitute its principal task, it could, through the functions described in section 5.2.1., help **facilitate** Member States' efforts in these two areas, notably to comply with their **obligations** under the CSA Directive. This initiative would not introduce new obligations on Member States on prevention and assistance to victims, including in relation to the cooperation with the Centre, which would remain an **optional resource** at the service of Member States that wish to benefit from it.

Detection, reporting and removal of CSA online: the Centre, through the functions described above, will also serve as a **facilitator** of Member States' efforts on investigations, as well as a **facilitator** of service providers' efforts to comply with the obligations under this initiative, particularly in relation to detection and reporting. The Centre would not have the capacity to initiate or conduct investigations, as these will remain under the responsibility of national law enforcement, or coordinate them, as this will remain under the responsibility of Europol. It will not be empowered to order service providers to remove CSAM, either.

Given the key functions above, the Centre would become **a fundamental component of the legislation**, as it would serve as a **key safeguard**, by acting **both as the source of reliable information about what constitutes CSA online** and as a **control mechanism** to help ensure the effective implementation of the legislation. The Centre would ensure **transparency and accountability**, by serving as a **European hub** for the detection, reporting and removal of CSA online. In receiving reports, the Centre would notably have visibility on the effectiveness of detection (including rates of false positives), reporting and removal measures, and on the spreading of CSAM and grooming across different platforms and jurisdictions.

Box 11: independence of the EU Centre

To be able to play its main role as a **facilitator** of the work of service providers in detecting reporting, and removing the abuse, and of the work of law enforcement in receiving and investigating the reports from service providers, it is essential that the Centre be **independent**

[159] The proactive search could be done using a "web crawler", similar to the one used in Project Arachnid by the Canadian Centre for Child Protection.

- from service providers, to be able to serve both as the source of reliable information about what constitutes CSA online, providing companies with the sets of indicators on the basis of which they should conduct the mandatory detection, and as a control mechanism to help ensure transparency and accountability of service providers; and
- from law enforcement authorities, as the Centre must be neutral to be an effective facilitator and must ensure that it maintains an objective, fair and balanced view.

To ensure that, it will be subject to **periodic reporting** to the Commission and to the public. The Centre should also be **independent from national public entities** of the Member State that would host it, to avoid the risk of prioritising and favouring efforts in this particular Member State.

The Centre would also **reduce the dependence** on private organisations in third countries, such as NCMEC in the US, for the fight against CSA in the EU. The Centre would operate within the EU and **under EU rules** and would reduce the need for **international transfers of personal data** of EU residents to third countries, notably the US.

To be able to carry out its functions, specifically to support the process of detection, reporting and removal, the Centre would, in accordance with the EU's personal data *acquis*, be provided with the appropriate **legal basis** to allow it to **process personal data** where needed. The Centre would be able to cooperate with service providers, law enforcement, EU institutions, but also with similar entities worldwide, such as NCMEC, given the global nature of CSA.

Discussion of the implementation choices for the Centre

This section summarises the process to determine the preferred implementation choice for the Centre, explained in detail in Annex 10.

The process had three stages: 1) mapping of possible implementation choices; 2) analysis of the choices and selection of the most promising ones for further analysis; 3) qualitative and quantitative analysis of the retained choices and determination of the preferred choice.

1) Mapping of possible implementation choices

Currently there is no entity in the EU or in Member States that could perform the intended functions for the Centre without significant legislative and operational changes, and therefore no obvious/immediate choice for the implementation of the Centre.

The process to determine the implementation choices started with a **mapping** of existing entities and their present functions and forms in order to identify **possibilities to build on existing structures** and make use of existing entities, or simple use them as possible references or benchmarks for setting up a new entity of the same type. For the mapping purposes, the examples were divided in two main types, depending on whether they required specific legislation to be set up:

1) entities that **do not require specific legislation** to be set up:
   a) Centre embedded in a unit in the European Commission (DG HOME, e.g. Radicalisation and Awareness Network, RAN).
   b) Entity similar to the EU centre of expertise for victims of terrorism.

2) entities that **require specific legislation** to be set up:
   a) Centre **fully embedded** in an **existing entity**:
      - EU body:
        - Europol;

        - Fundamental Rights Agency (FRA).
    - Other:
        - national entity (public or private such as an NGO);
        - international entity (e.g. INHOPE network of hotlines).

b) Centre set up as a **new entity**:
    - EU body:
        - executive agency (e.g. European Research Executive Agency, REA, European Education and Culture Executive Agency (EACEA));
        - decentralised agency (e.g. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), European Institute for Gender Equality (EIGE), European Union Intellectual Property Office (EUIPO)).
    - Other:
        - national entity:
            - foundation set up under national law (e.g. Academy of European Law (ERA), set up under German law);
            - Member State authority (e.g. new Dutch administrative authority to combat CSA and terrorist content online, under preparation).
        - international entity:
            - inter-governmental organisation (e.g. European Space Agency (ESA), European Organisation for the Safety of Air Navigation (EUROCONTROL));
            - joint undertaking (public-private partnership, e.g. Innovative Medicines Initiative, Clean Sky Joint Undertaking);
            - non-governmental organisation (e.g. CEN/CENELEC, EuroChild).

The mapping also included three relevant entities outside of the EU, which carry out similar functions to those intended for the EU centre, and which could provide useful references in some areas (e.g. costs, organisational issues, etc).

- US National Centre for Missing and Exploited Children (NCMEC);
- Canadian Centre for Child Protection (C3P); and
- Australian Centre to Counter Child Exploitation (ACCCE).

Finally, the mapping also included possible **combinations** of the above choices (i.e. functions distributed between several entities), in particular with **Europol**:

- Europol + a unit in the Commission;
- Europol + and NGO (e.g. a hotline);
- Europol + new national entity.

2) Analysis of the choices and selection of the most promising ones for further analysis

The analysis of the possible choices took into account the following criteria:

- **Functions**, i.e. the ability to effectively carry out the intended functions to contribute to achieving the specific objectives of the initiative. Specifically:
    - Facilitate prevention efforts.
    - Facilitate support to victims.
    - Facilitate the detection, reporting and removal of CSA online, including by ensuring **accountability and transparency**.

- **Forms,** i.e. the form in which the Centre is set up, and the extent to which that form supports carrying out the intended functions. Specifically:
    - Legal status: both the legal basis to set up the centre (if any) and the legislation to allow it to perform its functions (e.g. processing of personal data).
    - Funding: the sources that would allow the centre to ensure **long-term sustainability and independence** of the centre, while avoiding conflict of interest.
    - Governance: it should ensure 1) proper **oversight** by the Commission, and other relevant EU institutions and Member States; 2) **participation** of relevant stakeholders from civil society organisations, industry, academia, other public bodies (in particular considering that the Centre would need to work very closely with Europol, the Fundamental Rights Agency, and national authorities); 3) ensuring **independence** and **neutrality** of the centre from overriding private and political interests, to be able to maintain a fair and **balanced view of all the rights at stake** and to play its main role as **facilitator.**

Each of the possible implementation choices mapped earlier was analysed according to the above criteria. This detailed analysis led to discarding a number of possible choices, in particular having the **Centre fully embedded in Europol**, notably due to:

- **Challenges to carry out certain tasks in connection to the assistance to victims and prevention**, particularly by acting as a hub for information and expertise, some of which are significantly different from the core law enforcement mandate of Europol. Adding these tasks would require a revision of the mandate and significant capacity building efforts, with the risk that these tasks are eventually deprioritised compared to the core tasks of supporting investigations. While Europol has an explicit empowerment to set up centres under Art. 4 of the Europol Regulation, these centres are of a different nature and refer to internal departments focusing on implementing Europol's existing mandate in relation to specific types of crime. This empowerment therefore cannot be used to expand Europol's mandate to cover the new tasks.
- **Constraints of being part of a larger entity**. Being part of a larger entity could limit the ability of the centre to dispose of its own resources and dedicate them exclusively to the fight against CSA, as it could be constrained by other needs and priorities of the larger entity. It may also limit the **visibility** of the centre, as child sexual abuse is only one of the many types of crime Europol deals with. Moreover, embedding fully the Centre in Europol could create an imbalance and it would be difficult to justify that Europol expands its mandate to cover prevention and assistance to victims only in the area of child sexual abuse. This could lead to Europol gradually deviating from its core law-enforcement mandate and covering prevention and assistance to victims in multiple crime areas, becoming a "mega centre" of excessive complexity to be able to attend to the specificities of the different crime areas adequately.
- **Difficulties to appear as an independent and neutral facilitator**. The intended main role for the Centre is to serve as a **facilitator** to both service providers and law enforcement authorities of the process of detection, reporting and removal of CSA online. Europol's core mandate, however, is to support law enforcement. This may prevent Europol from appearing to all parties involved as an independent and neutral facilitator in the entire detection, reporting and removal process. Furthermore, service providers expressed during the consultations legal concerns about working too closely with law enforcement on the detection obligations, in particular if they are required to use the database of CSA indicators made available by the Centre for these detection

obligations. There is a risk that that content data of CSA online (i.e. images, videos and text) could not be used for prosecution in the US. This is due to the US legal framework (US Constitution) preventing from using content data detected by companies acting as **"agents of the state"** as it could be the case if the companies were mandated to detect content data using a database of indicators (e.g. hashes/AI classifiers) provided by law enforcement rather than by a non-law enforcement entity.

Another choice that was discarded following analysis was setting up the Centre as a **private law body** under the national law of the Member State hosting it. The main reason is that the Centre would not be able to carry out effectively the function of supporting the detection, reporting and removal of CSA online. These tasks imply implementing EU law, which in principle only Member States or the Commission can do.

The detailed analysis of all the possible implementation choices resulted in three "legislative" choices (i.e. that require legislation to set up the Centre) retained for the final assessment[160]:

1. Creating a self-standing, independent **EU body** (i.e. a dedicated decentralised agency) with all the intended centre functions: to support detection, reporting and removal of CSA online, and facilitate Member States' efforts on prevention and assistance to victims.
2. Tasking **Europol** with supporting detection, reporting and removal of CSA online and creating an **independent private-law entity** (or tasking an existing one) for prevention and assistance to victims.
3. Tasking the **Fundamental Rights Agency (FRA)** with all functions.

3) Qualitative and quantitative analysis of the retained choices and determination of the preferred choice.

Qualitative analysis

1. Centre as a self-standing **EU body (decentralised EU agency)**:

Arguments in favour:

- **Independence**, which would allow it to help ensure **transparency and accountability** of companies' efforts to detect CSA online and serve as a major safeguard and a **fundamental pillar** of the long-term legislation. Independence is essential to the centre's key function as facilitator and intermediary between private companies and public authorities. The legislation setting it up could be designed in a way that 1) guarantees the **sustainability** of the Centre through stable EU funding; 2) the governance is such that it ensures **appropriate oversight by the Commission**, and includes the participation of Member States and relevant stakeholders.
- Ability to **dispose of its own resources**, fully dedicated to the fight against CSA. Staff dedicated solely to the mandate of the Centre, rather than having to meet other objectives as part of a larger entity. Possibility to receive secured funding from the EU budget. Political accountability for its financial management would be ensured through the annual discharge procedure and other rules ordinarily applicable to decentralised agencies.
- Greater **visibility** of EU efforts in the fight against CSA, which would help facilitate the cooperation between the EU and stakeholders globally.

[160] The non-legislative choice (i.e. practical measures) was also retained for final assessment for comparison purposes (see annex 10), excluded here for simplicity. Legislation is required to enable the Centre to achieve its intended objectives, notably to support detection, reporting and removal of CSA online (e.g. to manage the database of indicators, or to review the reports from the service providers).

- Possibility to carry out **all relevant functions** in the same place (contribute to the detection of CSA online, support and assist victims and facilitate prevention) and liaise with all relevant stakeholder groups, which creates higher EU added value and a more effective and holistic response against CSA.

Arguments against:

- **Annual costs** would likely be slightly higher than in the other choices. These annual costs are indicative and could be higher or lower depending on the precise set-up and number of staff needed (see cost summary table in the quantitative assessment section below). The budget to cover this funding would need to be found within the scope of 2021-2027 Multiannual Financial Framework, from the Internal Security Fund budget.
- It will require significantly **more time and effort** to set up (including the decision on the seat of the agency) and get it fully operational as we cannot build on existing institutional legal frameworks (although these could serve as a reference) and would have to create a new mandate, and find, hire and train a number of dedicated non-law enforcement experts, including for management and control functions. The need for increased supervision would entail an increased workload at DG HOME and additional staff could be needed.
- The **cooperation with Europol and national law enforcement** would have to be created anew.

2. **Part** of the Centre within **Europol** and **part** as an **independent entity**:

Arguments in favour:

- **The annual costs** will most likely be lower than creating a new body as the Centre would benefit from economies of scale with Europol, (e.g. building, infrastructure, governance, management and control system), although building and governance costs could be offset by those of the new entity (see cost summary table below).
- The part of the Centre as part of Europol could directly **benefit from its expertise and established mechanisms** (including concerning personal data protection) to deal with the reports from service providers.

Arguments against:

- The ability of the Centre to serve as a **major player and safeguard** in the detection and reporting process, a key feature of the long-term legislation, would appear limited as it would not be independent from law enforcement.
- In the case of **false positives**, companies would be reporting innocent persons to law enforcement directly.
- The ability of the Centre to **dispose of its own resources** and dedicate them to the fight against CSA may be limited by other needs and priorities of Europol in other crime areas. This could also jeopardize its **ability to deliver** on these additional and visible tasks.
- Europol would be dedicating a **substantial amount of resources** to tasks such as manually reviewing the reports from companies to filter false positives, determining the jurisdiction best placed to act, etc. That may not be the best use of law enforcement's resources, which could be otherwise dedicated to conduct investigations leading to the rescue of victims and the arrest of offenders, given the limited availability of law enforcement officers.

- **Less visibility** of EU efforts in the fight against CSA, as these would be split between two entities, and Europol's area of focus is vast, which could limit its ability to facilitate the cooperation between the EU and stakeholders globally.

3. Tasking the **Fundamental Rights Agency (FRA)** with all functions:

Arguments in favour:

- **Annual costs** would most likely be slightly lower than creating a new body, as the centre could benefit from economies of scale with FRA (e.g. governance, management and control system). The initial costs would also be slightly lower than creating a new body or in the Europol+ option, thanks to the possibility to leverage the existing building and infrastructure (see cost summary table below).
- The focus of FRA on **fundamental rights** could reinforce the perception of **independence**, which is key to help ensure **transparency and accountability** of companies' efforts to detect CSA online and of the outcome of the follow up of the reports by law enforcement. This would also allow FRA to serve as a major **safeguard** of the detection process.
- In the case of **false positives**, companies would not be reporting innocent persons to law enforcement directly.
- Possibility to carry out **all relevant functions** in the same place (contribute to the detection of CSA online, support victims and facilitate prevention) and liaise with all relevant stakeholder groups.

Arguments against:

- The ability of the Centre to **dispose of its own resources** and dedicate them to the fight against CSA may be limited by other needs and priorities of FRA. This could jeopardize its **ability to deliver** on these additional and visible tasks.
- Although it would be possible to build on the existing institutional framework to some extent, **repurposing** it may still entail **significant effort** to accommodate these new tasks in a **long-existing and established entity.**
- The setup of FRA and its governance structure are specific to its current mandate. Significant changes to that mandate and the governance structure would be required in order to integrate the EU Centre into FRA. Given past difficulties in revising the mandate of FRA, there would also be significant additional risks in reopening the relevant regulation.
- The **cooperation with Europol** and **national law enforcement** would have to be created anew.
- The **annual and initial costs** may be lower than creating a new body but they will still be **substantial**, e.g. to find, hire and train a number of dedicated non-law enforcement experts, and to carry out the centre functions (including manually reviewing the reports from companies to filter false positives, determining the jurisdiction best placed to act, and supporting Member States on prevention and assistance to victims).
- There would be a **significant imbalance** in FRA's mandate: as it would double in size, half of it would be dedicated to CSA and the other half to its current tasks.

Quantitative analysis

Costs.

The following table summarises the estimated costs for the three retained implementation choices of the EU Centre[161]:

[161] These costs estimates refer to 2022 costs and to the Centre operating at full capacity. The estimates do not take into account inflation and the related accumulated costs during the ramp-up period until the Centre operates at full capacity. See the legislative financial statement accompanying the legislative proposal for more exact cost estimates taking into account inflation and the breakdown of different staff positions.

Table 2: summary of estimated costs for the implementation options of the EU centre

			1. EU body (e.g. agency)	2. Europol + separate entity		3. FRA
				Europol	Separate entity	
Staff (number of people)	Detection, reporting, removal	Operational staff	70	70	N/A	70
		Overheads staff	15	5		5
	Prevention	Operational staff	10	N/A	10	10
		Overheads staff	4		4	2
	Assistance to victims	Operational staff	10		10	10
		Overheads staff	4		4	2
	Total staff (number of people) [162]		**113**	**75**	**28**	**99**
				103		
Staff (MEUR/year)			**15,9**	10,6	3,9	**13,9**
				14,5		
Infrastructure (MEUR/year)		**Initial costs**	5	4	1	4
		Annual costs	3,2	2,4	1,2	3,2
				3,6		
Operational expenditure (MEUR/year)			6,6	2,5	3,5	6,6
				6		
Total annual costs (MEUR)			**25,7**	**15,5**	**8,6**	**23,7**
				24,1		
Total initial costs (MEUR)			**5**	**5**		**4**

[162] 28 posts corresponding to the prevention and assistance to victims functions in all options could be non-EU staff and be covered by a call for proposals/grant. They would therefore not be part of the EU establishment plan and would not have impact on the future EU budget (e.g. pensions, etc).

As a reference, existing agencies of comparable size have the following actual **annual costs**:

		FRA	EMCDDA
Staff	Number of people	105	100
	MEUR/year	14,7	12,2
	People/MEUR	7,1	8,2
Infrastructure (MEUR/year)		2,2	2,1
Operational expenditure (MEUR/year)		7,4	4,7
Total (MEUR/year)		**24,3**	**19**

As indicated above, 28 posts corresponding to the prevention and assistance to victims functions in all options could be non-EU staff and be covered by a call for proposals/grant. In particular, in the case of option 2, Europol + separate entity, the possibility to cover these posts through a call for proposals/grant would not remove the need for a separate entity, as the envisaged prevention and assistance functions are currently not carried out by any organisation. Even if an existing entity applied for the potential call for proposals/grant, it would need to expand to accommodate the 28 posts, with the estimated infrastructure costs of e.g. rental of buildings, IT systems and audits, and the operational expenditure costs of e.g. support to expert networks, translation and interpretation, dissemination of knowledge and communication (see Annex 10, section 4.2.). Furthermore, a single separate entity should deal with both the prevention and assistance to victims functions to ensure organisational efficiency, given the strong interlinkages between both functions.

Annex 4 includes additional information on the points considered in the above estimates.

Benefits.
The main quantitative benefits derive from savings as a result of **reduction of CSA** associated costs, i.e. savings relating to offenders (e.g. criminal proceedings), savings relating to victims (e.g. short and long-term assistance), and savings relating to society at large (e.g. productivity losses).

It is assumed that the implementation choice that is the **most effective** in fulfilling the functions of the Centre would also be the one helping achieve that highest reduction of CSA and therefore the one with the highest benefits. Annex 4 contains estimates of these benefits, to be taken into account for the sole purpose of comparing the options. As it is expected that a dedicated EU agency would be the most effective in fulfilling the Centre functions, it would also be the one generating the highest benefits.

Preferred option

The analytical assessment and comparison process above indicates that the preferred implementation option for the Centre would be a **dedicated EU decentralised agency**[163]. This is the option that would best contribute to achieve the specific objectives of the initiative, while respecting subsidiarity and proportionality and protecting fundamental rights. It will be possible to provide the EU agency with the necessary legal framework to carry out its functions, in particular those in relation to facilitating the detection, reporting and removal of CSA online.

The a dedicated and decentralised **EU agency,** in accordance with the common approach agreed by the European Commission, the European Parliament and the Council of the EU in 2012[164]. As an EU agency, it would be financially independent and be funded by the EU, which would further support the Centre's independence.

In addition to the **periodic reporting** to the Commission and to the public described above, the Commission and Member States would further supervise the Centre and its activities, in accordance with the general rules applicable to decentralised EU agencies[165]. These rules include in particular a governance structure that supports both the independence of the agency and the participation of relevant stakeholders, notably through a management board with representatives of all Member States and the Commission, an executive board, and an executive director appointed following an open and transparent selection procedure.

In terms of organisation, the Centre would work closely with the **European Police Agency (Europol)**, the EU Agency for **Fundamental Rights (FRA)** (e.g. in contributing to transparency and accountability as well as to assessments of the fundamental rights impact of new measures)**, national law enforcement and other relevant authorities,** as well as the national **hotlines.** This setup would ensure that **existing resources** can be relied upon to the **maximum** extent possible while preserving the **independence** that is **fundamental** to the role of the Centre.

Box 12: relations between the Centre as a new EU agency and Europol

The Centre as a new EU agency would **cooperate closely** with Europol, in particular on facilitating the reporting of CSA online, as described above.

The Centre would be the **recipient of the reports** from service providers. It would review these reports and ensure that they are **actionable**, i.e. that they are not manifestly unfounded and could thus lead to law enforcement authorities to initiate an investigation where they deem this necessary and appropriate. In doing so, the Centre would ensure that possible **false positives** do not reach law enforcement and the service providers are informed of the possible errors. These tasks could free up resources at Europol and national law enforcement agencies, which are currently dedicated to filtering the reports.

Once the Centre confirms that the report is actionable, it would forward it to Europol and/or national law enforcement **for action** in accordance with the existing rules, including as regards Europol's mandate. Europol could enrich with criminal intelligence the reports

[163] To be funded by the Internal Security Fund managed by the European Commission Directorate General for Migration and Home Affairs.

[164] Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies, 2012.

[165] See the Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies, 2012.

received from the Centre, identifying links between cases in different Member States, sharing the reports with national law enforcement agencies and supporting these agencies by facilitating cross-border investigations. The Centre would not have any competence to launch investigations; this would remain under the exclusive competence of national law enforcement authorities.

The Centre would also notably cooperate closely with Europol on the preparation of the **databases of indicators**, on the basis of which the service providers would be required to detect CSA online, building on existing databases at Europol and at national level. New material from reports (from service providers, hotlines and/or the public) and finished investigations by law enforcement will, where justified in view of confirmation by courts or independent administrative authorities, be added to these databases in the form of newly generated indicators, to ensure that they remain updated and as relevant as possible.

Box 13: European Parliament views on the EU Centre

The European Parliament has **welcomed**[166] the idea to establish the European Centre to prevent and counter child sexual abuse that the Commission first announced in the 2020 EU strategy for a more effective fight against child sexual abuse, following the **call** of the Parliament **in 2019 for an EU child protection centre**[167] that would help ensure an effective and coordinated response to child sexual abuse in the EU.

In addition, during the negotiations for the Interim Regulation, Members of the European Parliament repeatedly expressed their expectations that an EU Centre could help limit the international transfers of personal data of EU citizens to the US, hold companies accountable, and publish transparency reports about the detection, reporting and removal process.

Stakeholders' views on the EU Centre to prevent and counter CSA

All the main stakeholder groups that responded to the open public consultation supported the creation of an **EU Centre** that would provide additional support at EU level in the fight against CSA online and offline, to **maximize the efficient use of resources** and **avoid duplication** of efforts. The support was highest among academia and research institutions (100% of responses), as well as public authorities and NGOs (85% of responses). 40% of the responses from service providers, business associations and the general public expressed explicit support.

More than half of the responses (51% of all responses to the consultation) indicated that the Centre could 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**. It could also **support victims** in ensuring removal of child sexual abuse material online depicting them. The Centre could serve as a hub for connecting, developing and disseminating research and expertise, as well as facilitating the communication and exchange of best practices between practitioners and researchers.

Public authorities pointed out that the Centre could maintain a **single EU database** of hashes of known CSAM in order to facilitate its detection in companies' systems (76% of responses from this group). The Centre could also **support taking down CSAM** identified through hotlines (62% of responses from this group).

Service providers indicated in the targeted consultations that they would prefer to **report to an EU Centre rather than to law enforcement directly**, as they currently do in the US with NCMEC.

Stakeholders' views on new CSA legislation from the open public consultation

[166] European Parliament resolution of 17 December 2020 on the EU Security Union Strategy (2020/2791(RSP)).

[167] European Parliament resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child (2019/2876(RSP)).

Respondents from **public authorities** (62% of the total responses from this group), **companies** (56%), **business associations** (60%) and **civil society organisations** (74%), supported new legislation to ensure legal certainty for those involved in the fight against CSA. In particular, the legislation should notably:

- provide the right incentives for the detection of CSAM;
- provide a clear legal basis for the processing of personal data to detect, report and remove CSA online;
- clarify and resolve conflicts and fragmentation in existing, pending and proposed legislation across Member States as well as at EU level; and
- be future-proof (i.e. that it remains effective despite future technological developments)

5.2.3. Option C: option B + mandatory detection of known CSAM

This option builds on option B and imposes on relevant providers an **obligation to perform a risk assessment** on whether their services are likely to be used for the sharing of known CSAM and propose **mitigating measures** to reduce that risk**.** Where the risk assessment (after proposing the mitigating measures) reveals a level of risk that is not minor, national competent authorities would issue **orders to detect** material that has **previously been reliably confirmed** by courts or other independent public authorities as constituting CSAM. These orders would be limited in time and would apply regardless of the technology used in the online exchanges, including whether the service is encrypted, to ensure that the legislation is technology neutral. The obligation to detect would be limited to relevant service providers in this context, i.e. those identified as the main vectors for sharing and exchange of known CSAM. Only a subgroup of the providers required to submit a risk assessment would receive a detection order, based on the outcome of the risk assessment taking into account the proposed mitigating measures. The legislation would list possible risk factors that the providers should take into account when conducting the risk assessment. In addition, the Commission could issue guidelines to support the risk assessment process, after having conducted the necessary public consultations.

Known CSAM is the most common type of CSA online currently detected (in 2020 service providers reported seven times more known images and videos than new ones, and 2600 times more known images and videos than grooming cases, see section 2.1.1.). The detection of new CSAM and grooming would remain voluntary, whereas reporting and removal (upon the reception of a removal order) would be mandatory for all types of CSA online, as described in option B. In order to ensure its effectiveness, effective and proportionate sanctions would be instituted for providers who fail to comply with the obligation. These sanctions would be imposed by Member States' competent national authorities. More specifically, the process would look as follows:

Mandatory risk assessment

Relevant service providers would be required to assess the risk that their services are misused to distribute **known** CSAM. The risk factors to consider could include, depending on the service concerned:

- the business model of the service provider,
- its corresponding user base, including whether the service is available directly to end users (as opposed to, e.g., providing services to businesses),
- the verification of user identity in the registration process,
- the possibility to share images and videos with other users, e.g. by message or through sharing of a link to resources hosted on the service provided,
- in services offering a chat/messaging functionality, the possibility to create closed groups, which can be joined upon invitation from a member only,
- the way in which the services are designed and operated,

- the ways in which the services are actually used, and any corresponding impact on the risk of distribution of **known** CSAM,
- previous detection of CSAM on the service or on a similar service with a comparable risk profile.

As part of the risk assessment, the service provider could request support from the Centre and/or competent national authorities in performing detection tests on representative anonymised samples, in order to establish the presence or not of known CSAM.

Providers would then be **required to report** to the **competent national authority** on the **risk assessment** and on any **mitigating measures** that they plan to adopt or have already adopted. The competent national authority would review the risk assessment and determine whether the assessment has been properly conducted and whether the mitigation measures proposed by the service provider are sufficient. If needed, the competent national authority could request the service provider to resubmit the risk assessment or additional information pertaining to it.

Detection order

On the basis of this risk assessment and the criteria laid down in the initiative, the competent national authority would decide whether a **detection order** for **known** CSAM should be issued to each specific service provider, by a court or an independent administrative authority (which could be the national authority if it meets the independence criteria). A service provider falls under the jurisdiction of the Member State in which it has its main establishment or in which – if it has no main establishment in the EU – it has designated a legal representative, building on the approach already adopted in the Terrorist Content Online Regulation[168] and proposed in the DSA. Competent national authorities would cooperate in a network to ensure harmonised application of the rules, building where possible on the structures to be put into place for the DSA. The detection order would be limited in time and renewable based on an updated risk assessment, and would be accompanied by specific supervisory powers for the authorities, including on the detection technology deployed, and by measures to ensure transparency. Suitable redress for affected service providers would be provided for.

Support by the EU Centre

The EU Centre would support service providers in three ways:

1) By providing practical or technical information to service providers that could help them giving effect to their legal obligations and contributing to the preparation of guidance and best practices documents where needed;
2) By making available to service providers a **database of indicators** of known material (e.g. hashes and URLs[169]) that providers would be required to use to facilitate accurate detection of known CSAM. The indicators would correspond to material confirmed as illegal in the EU, as set out above.

   In addition, the Centre would also facilitate access for service providers to **free-of-charge detection tools**. These **tools** would be automated and have a **high accuracy rate**, and have proven reliable for over a decade (see box 14 below and annex 8, section 1)[170]. Providers would not be mandated to use the tools provided by the

[168] OJ L 172, 17.5.2021, p. 79–109.

[169] The URLs in this database would point to a specific image or video, rather than an entire website.

[170] They have to date been made available inter alia by NCMEC and are available for use subject to a licensing agreement that limits the use of the tool to the detection of CSAM, to the exclusion of any other content.

Centre, as long as their tools meet the requirements (safeguards) specified in the legislation (see below). Responsibility for the use of these tools and any resulting decisions by the service providers would remain with the service provider themselves.

3) By **reviewing the reports** submitted by service providers to ensure accurate reporting to law enforcement, and providing support, including through feedback on accuracy, to further improve accuracy levels, to prevent imposing excessive obligations on the providers and in particular to avoid imposing the obligation to carry out an independent assessment of the illegality of the content detected.

The support of the Centre would be particularly useful to **SMEs**, which would also be subject to the above requirements and could thus also receive a detection order from national authorities. The Centre and the Commission could provide additional support to SMEs in the form of **guidance**, to inform SMEs about the new legal framework and the obligations incumbent on them. This guidance could be disseminated with the help of industry associations. It may also be possible to provide **specific training**, in collaboration with Europol and the national authorities.

Box 14: hashing and URL detection tools

Hashing is the most common technology to detect known CSAM. The most broadly used example is Microsoft's **PhotoDNA**[171]. It creates a unique digital fingerprint ('hash') of the image or video and compares it to a database containing hashes of material verified as being CSAM. If the hash is not recognised, no information is kept. The technology does not identify persons in the image/video and does not analyse the context.

- PhotoDNA has been in use for **over 10 years** by organisations globally, including service providers, NGOs and law enforcement in the EU[172]. Its rate of false positives is estimated at no more than 1 in 50 billion, based on testing[173]. Microsoft provides PhotoDNA for free, subject to a licensing agreement requiring strict limitation of use to the detection of CSAM. Organisations wishing to use the technology must register and follow a vetting process by Microsoft to ensure that the tool will be used by the right organisation for the sole purpose of detecting CSAM.
- Other examples of hashing technology used for these purposes, and operating on similar principles, include YouTube CSAI Match[174], Facebook's PDQ and TMK+PDQF[175].
- The largest database of hashes is held by **NCMEC**, with more than **four million hashes of CSAM images and 500 000 hashes of CSAM videos**[176]. Every hash contained in the database has been viewed and agreed upon as being CSAM by two experts at NCMEC on the basis of strict criteria (see Annex 8).

URL lists are also used to detect known CSAM. Currently they are typically prepared by national authorities (e.g. law enforcement, such as the National Centre for Combating Child Pornography in Italy, or the Judicial Police in France, OCLCTIC, supervised by the National Commission on Computing and Freedoms, CNIL, and supported by the national hotline Point

171 Microsoft's information on PhotoDNA.
172 More information is available here.
173 Testimony of Hany Farid, PhotoDNA developer, to House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, 16 October 2019.
174 YouTube CSAI Match.
175 Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer.
176 NCMEC, as of September 2021.

de Contact[177]) and transmitted to internet service providers to block access[178]. Some Member States (e.g. Bulgaria) use **Interpol's Worst of List** (IWOL), which contains addresses with images and videos that depict severe abuse, with real children, younger than 13, and which have been verified by public authorities from at least two different countries or agencies[179].

Stakeholders' views from the open public consultation on mandatory detection

Public authorities that responded to the consultation were in favour (81% of respondents) of mandatory detection, including in encrypted systems.

Some companies (31%) and **business associations** (40%) supported that such obligation shall not apply regardless of whether these services use encryption. Business associations also stressed the role of encryption in ensuring the online safety and confidentiality of communications of marginalised groups and groups at risk, and that encryption should not be weakened.

Children's rights NGOs were in favour of mandatory detection also in encrypted systems, while pointing out that it should be in line with applicable privacy and other laws.

Privacy rights NGOs stressed the need of preserving strong encryption, and opposed all solutions identified to detect CSA in encrypted systems.

Individuals stressed that service providers should not be obliged to detect CSA online in encrypted services.

Conditions and safeguards

The obligation to detect known CSAM would apply **regardless of the technology deployed in the online exchanges**. As described in the problem definition (section 2.2.1.), some technologies used in online exchanges require adaptation of existing detection technology to detect CSA online: for example, while the principal methodology of comparing hashes would remain unchanged, the point in time at which identification is performed would need to be adjusted in end-to-end encrypted communications, to take place outside the communication itself. In addition, a number of companies have developed tools that seek to identify CSA online using metadata. While these tools are not yet comparable to content-based analysis tools[180] in terms of accuracy, child protection and accountability, they could possibly develop to an equivalent standard in the future. Also, some providers have already deployed tools that perform content-based detection in the context of end-to-end encrypted communications, demonstrating the swift development of technologies in this area.

The legislative proposal should remain technology-neutral also when it comes to possible solutions to the challenge of preventing and detecting online child sexual abuse. Under this option, the obligation to detect known CSAM would therefore be an **obligation of results**, meaning that detection has to be of sufficient overall effectiveness regardless of the technology deployed. For example, in a test sample where a specified percentage of material constitutes known CSAM, the detection tool should correctly identify a comparable amount of CSAM, in line with the state of the art in detection technology when it comes to accuracy. This is to be demonstrated by the service providers. The legislation would set out conditions for the technologies deployed and corresponding supervision powers for national authorities, without however specifying the technologies that must be put in place to enable detection, to

177 CNIL, Rapport d'Activité 2020.

178 Article 25 of the CSA Directive includes a provision for voluntary blocking of websites containing and disseminating CSAM. For more information, see the report from the Commission assessing the implementation of that Article, COM(2016) 872.

179 Interpol, Blocking and categorizing content.

180 Pfefferkorn, R., Stanford Internet Observatory, Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers, 9 September, 2021. See in particular p.10-11.

ensure that the legislation remains **proportionate**, **technology neutral** and **future proof**. Service providers would be free to implement the technical solutions that are most compatible with their services and infrastructures, provided they meet the standards (see below for details on standards).

The obligation to detect regardless of the technology used in the online exchanges is **necessary** to ensure not only that the services that, following the risk assessment, should be detecting known CSAM, **can do so in practice**, but also to **prevent creating a negative incentive** to put in place certain technologies solely to avoid the detection obligations. It would therefore ensure that the legislation **achieves its general objective** of improving detection, reporting and removal of CSA online.

The obligation to detect regardless of the technology used in the online exchanges, together with all the required **safeguards** (see below), is also **necessary** to help ensure **a fair balance of the affected fundamental rights**[181].

Box 15: Detection of CSA online in end-to-end encrypted communications

End-to-end encryption (E2EE) is an important example of a technology that may be used in certain online exchanges. While beneficial in ensuring privacy and security of communications, encryption also creates secure spaces for perpetrators to hide their actions, such as trading images and videos, and approaching and grooming children without fear of detection[182].This hampers the ability to fight these crimes and lowers the protection of the fundamental rights of the child and therefore creates a **risk of imbalance** in the protection of all the fundamental rights at stake. Any solution to detect CSA needs to ensure a fair balance between:

- on the one hand, the fundamental rights of all users, such as privacy and personal data protection, the freedom to conduct a business of the providers, and
- on the other hand, the objective of general interest associated with tackling these very serious crimes and with protecting the fundamental rights of children at stake, such as the rights of the child, human dignity, prohibition of torture and inhuman or degrading treatment or punishment, and privacy and personal data protection.

The Commission organised in 2020 an **expert process** under the EU Internet Forum to answer the following question: given an E2EE electronic communication, are there any technical solutions that allow the detection of CSA content while maintaining the same or comparable benefits of encryption (e.g. privacy)? [183] Annex 9 summarises the work of experts from academia, service providers, civil society organisations and governments, which

[181] As announced in the EU strategy to tackle Organised Crime 2021-2025, in parallel to this initiative, the Commission is steering a process to analyse with the relevant stakeholders the existing capabilities and approaches for lawful and targeted access by law enforcement authorities to encrypted information (i.e. **any kind of content**, not necessarily illegal in and of itself) in the context of criminal investigations and prosecutions and will suggest a way forward in 2022. The scope of this process is therefore different from **proactive** detection by online service providers, solely on their own systems, of whether CSAM is being exchanged or grooming is taking place. While different in scope, both initiatives will need to be coherent with the general position of the Commission to promote strong encryption and avoid any general weakening.

[182] See in particular, Interpol, General Assembly Resolution on Safeguarding children against online child sexual exploitation, 24 November 2021.

[183] In a different process with a different scope, the Commission is also analysing with relevant stakeholders the existing capabilities and approaches for lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions. The Commission will suggest a way forward in 2022 based on a thorough mapping of Member States' efforts to deal with encryption and a multi-stakeholder process to explore and assess concrete options.

finished at the end of 2020. The expert group mapped the possible solutions and highlighted the most promising ones following a technical assessment across five criteria: effectiveness, feasibility, privacy, security and transparency. In relation to the question asked, the expert group concluded at the time that **such technical solutions did exist** at different levels of development, but had not been deployed at scale yet[184].

In August 2021, **Apple** announced the launch of its new 'Child Safety' initiatives[185], including on-device detection of known CSAM. This solution, similar to two of the solutions identified by the expert group as the most promising, appears to be a viable and technically mature solution to detect known CSAM outside the context of electronic communications, and regardless of whether or not any electronic communication is encrypted[186]. In September 2021, Apple announced that the deployment of this solution would be delayed to gather additional feedback from customers, advocacy groups, researchers, and others before launching it, in view of criticism in particular from privacy advocacy groups[187]. It has since deployed detection of images containing nudity sent or received by a child through on-device analysis on incoming and outgoing images, providing a warning to children not to view or send them. When sending or receiving such images, children have the option to notify someone they trust and ask for help[188].

Meta's **WhatsApp**, which is end-to-end encrypted, has also been deploying tools to identify CSAM on its messaging service, based on unencrypted data associated with the communication[189]. However, Meta has also acknowledged the limitations of its current detection tools in public government hearings, indicating that it expects lower numbers of detection compared to unencrypted communications,[190] and has referred far fewer cases to NCMEC compared to Meta's Facebook Messenger[191].

While companies would be free to decide which technology to deploy, the competent national authority will be empowered and required to supervise. If needed, it could make use of the technical expertise of the EU Centre and/or independent experts to determine relevant technical or operational issues that may arise as part of the authority's assessment whether the technology that a given service provider intends to use meets the requirements of the legislation. In particular, the competent national authorities would take into account the availability of the technologies in their decision to impose a detection order, ensuring the effective application of the obligation to detect. In the cases in which the technology to detect CSA online was not yet available to be deployed at scale, the legislation could foresee for the competent authorities the possibility to consider this circumstance when deciding the start date of application of the detection order on a case by case basis. The EU Centre and the

184 Technical solutions that could be applied to identify CSAM URLs in E2EE communications are already in use today. For example, services like WhatsApp or Signal scan the URLs of a message before it is encrypted for spam and malware, and to show the user a preview of the webpage the URL points to.

185 For more information see: https://www.apple.com/child-safety/.

186 For a technical summary of how the tool works, see here. Instead of scanning images in the cloud, the system performs on-device matching using a database of known CSAM image hashes provided by NCMEC and other child safety organizations. Apple further transforms this database into an unreadable set of hashes that is securely stored on users' devices. Differently from the solutions identified in the expert process under the EU Internet Forum, Apple's solution does the hashing and matching when the image is uploaded to iCloud, not when the image is sent or received in a communication (as in the expert process' solutions).

187 The plans in relation to the launch of the tool remained unchanged at the time of writing, see here.

188 As reported on CNET.

189 See WhatsApp's FAQs on this matter.

190 House of Commons, Home Affairs Committee hearing of 20 January 2021, Q125-142.

191 NCMEC and Wired, Police caught one of the web's most dangerous paedophiles. Then everything went dark, May 2020.

Commission could facilitate the exchange of best practices and cooperation among providers in the deployment efforts of new technologies.

The legislation would specify the necessary **safeguards** to ensure proportionality and a fair balance between all the affected fundamental rights. In particular, as service providers put in place technical solutions that allow the detection of CSA online regardless of the technology used in the online exchanges, there is a need to regulate the deployment of these solutions, rather than leaving to the service providers the decision on what safeguards to put in place.

Service providers have strong incentives already to ensure that all tools they deploy are reliable and as accurate as possible, to limit false positives. In addition, safeguards are of particular importance to ensure the fair balance of fundamental rights in the context of interpersonal communications, where the level of interference with the relevant fundamental rights, such as those to privacy and personal data protection, is higher compared to e.g. public websites.

The legislation would set out three types of safeguards, on 1) what **standards** the technologies used must meet, 2) safeguards on **how** the technologies are deployed, and 3) **EU Centre**-related safeguards. They would, as far as possible, build on the detailed safeguards of the Interim Regulation, to ensure coherence and minimise disruption. These safeguards could include or be based on:

1) **Standards** the technologies must meet:

- be in accordance with the state of the art in the industry;
- be sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of CSA, subject to independent expert certification;
- be the least privacy-intrusive, including with regard to the principles of data protection by design and by default laid down in the GDPR;
- not be able to deduce the substance of the content of the communications but solely be able to detect **patterns** which point to possible CSA (i.e. only determine whether the content matches known CSAM, without assessing or extracting anything else);
- make use of the **indicators** provided by the EU Centre to detect known CSAM (see below on EU Centre-related safeguards);

2) **How** the technologies are deployed, i.e. when deploying these technologies the providers should:

- conduct a **prior data protection impact assessment and a prior consultation** procedure as referred to in the GDPR, to be repeated when the technologies are significantly modified;
- establish **internal procedures** to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data;
- ensure **human oversight**, where necessary. While the tools for detection of known CSAM are accurate to such a high degree that human review of each and every hit is not required, the oversight should encompass spot checks and tests to ensure the continued reliability and verify consistent accuracy rates;
- establish appropriate **redress mechanisms** to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views;
- **inform users** in a clear, prominent and comprehensible way:
    - of the fact that the service providers **use** technologies to detect known CSAM and how they use those technologies;

    - which consequences such use may have for the users and avenues for redress related thereto;
- **retain the content data and related traffic data** processed for the purpose of detecting known CSAM and its subsequent actions (reporting, removal and possible other consequences, redress, responding to competent law enforcement or judicial authorities' requests) **no longer than strictly necessary** for those purposes, and no longer than the maximum period defined in the legislation;
- **give** competent authorities **access to data**, solely for supervisory purposes; and
- **publish transparency reports** on how the technologies used have been deployed, including operational indicators such as error rates (see section 9 on monitoring and evaluation).

3) **EU Centre**-related safeguards. The Centre would be a fundamental component of the legislation and will serve as a **key safeguard** by:

- making available to service providers the indicators that they should use to detect known CSAM **according to EU rules** (notably the CSA Directive), as determined by courts and other independent public authorities (see description of EU Centre under option B);
- **reviewing the reports** submitted by the companies and contributing to ensure that the **error rate** stays at **a minimum** in particular by making sure that possible reports submitted by mistake by service providers (i.e. do not contain CSA online) are **not forwarded** to law enforcement, and **providing feedback** to service providers on accuracy and potential false positives to enable continuous improvement;
- facilitating access to **free-of-charge technology** that meets the highest standards for the reliable, automated detection of CSA online;
- publishing **annual transparency reports** which could include the number and content of reports received, the outcome of the reports (i.e. whether law enforcement took action and if so, what was the outcome), and lists of service providers subject to detection orders, removal orders and sanctions (see section 9).

Given the key role of the Centre, the legislation should also include a set of **safeguards** to ensure its proper functioning. These could include:

- carrying out **an independent and periodic expert auditing** of the **databases of indicators** and its management thereof;
- carrying out **independent expert verification or certification** of tools to detect, report and remove CSA online that the Centre would make available to service providers;
- creating **clear and specific legal bases** for the processing of personal data, including sensitive personal data, necessary for the performance of the Centre's functions, with the appropriate limitations and safeguards;

In addition, as a decentralised EU agency, the Centre would be subject to all corresponding transparency and accountability obligations that generally apply to such agencies, including supervision by the EU institutions.

Stakeholders' views on safeguards from the open public consultation

Public authorities indicated that it is critical to implement robust **technical and procedural safeguards** in order to ensure **transparency and accountability** as regards the actions of service providers.

NGOs pointed out that the new legislation should provide **legal certainty** for all stakeholders (e.g. service providers, law enforcement and child protection organisations) involved in the fight against CSA online and

improve **transparency and accountability.** Almost 75% of views from NGOs underlined that **transparency reports** should be **obligatory and standardized** in order to provide uniform quantitative and qualitative information to improve the understanding of the effectiveness of the technologies used as well as about the scale of CSA online. Legislation could foster the development of an EU-wide classifications of CSAM.

Business associations highlighted that it is critical to publish **aggregated statistics** on the number and types of reports of CSA online received in order to ensure **transparency and accountability** regarding actions of service providers (40% of their replies). Moreover, some respondents (including companies and business associations) reflected that fully harmonised definitions (beyond the minimum harmonisation provided by the CSA directive) would help reduce EU fragmentation.

Academic and research institutions also stated that transparency reports should be **obligatory**, and evaluated by an independent entity (75% of their replies). All of them stated that these reports need to be standardized in order 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.

*5.2.4. Option D: option C + **mandatory detection** of **new** CSAM*

This option is the same as option C but adding mandatory detection of material that **has not been previously verified as CSAM** (i.e. 'new', as opposed to 'known', CSAM). As described in section 2.1.1., the detection of **new content** (i.e. not previously identified as CSAM) often reveals **ongoing or recent abuse** and therefore implies a heightened need to **act as soon as possible** to rescue the victim.

As in option C, to ensure that the legislation is technology neutral, the obligation would apply **regardless** of the technology used in the online exchanges.

The detection of grooming would remain voluntary, whereas reporting and removal of confirmed CSA would be mandatory for all types of CSA online, as described in option B.

Mandatory risk assessment

Expanding the risk assessment outlined in Option C, service providers of relevant services, notably providers of interpersonal communication and hosting services, would be required to also assess the risk that their services are misused to distribute **new** CSAM. As there is no difference between "known" and "new" CSAM beyond its having been seen and confirmed by an authority, the distribution vectors are typically identical. Hence, risks and experiences relating to the detection of known CSAM could be taken into account in this regard. However, the risk factors would also take into account the specificities of new CSAM, and in particular the risk that the service is used to distribute self-generated material (see box 3 in the problem definition, section 2.1.1.). For interpersonal communications services, the risk assessment should also include an analysis of objective factors that may point to a heightened likelihood of sharing of CSAM, which could possibly include group size, gender distribution, frequency of exchange and frequency and volume of images and videos shared. In addition, the risk assesment could be based, e.g., on spot checks, particularly in the absence of previous experience on the same or comparable services.

The service providers would be **required to report** to the **competent national authority** on the **risk assessment**, including the **mitigating measures** that they plan to adopt or have already adopted, and the same considerations as in option C would apply.

Detection order

Similarly to option C, on the basis of this risk assessment, the competent national authority would decide whether a **detection order** for **new** CSAM should be issued to a service provider, for one or more relevant services it provides. The order should be limited to the

strictly necessary; where possible and technically feasible, particularly for interpersonal communications services based e.g. on the objective factors identified in the risk assessment, it should be limited to relevant parts of a given service. The detection order would be limited in time and renewable based on an updated risk assessment. Suitable redress for affected service providers would be provided for.

Support by the EU Centre

The EU Centre would support service providers in three ways:

1) By making available to providers the **database of indicators** of **new** material (e.g. AI classifiers) that providers would be required to use to detect **new** CSAM, while ensuring a **technology neutral** approach. The indicators would be based on material determined by courts or other independent public authorities as illegal under EU law.
2) By making available to providers, **free-of-charge, technologies** to facilitate detection. Providers would not be mandated to use the technologies provided by the Centre and would be able to use other tools, as long as they meet the standards and provide for the safeguards specified in the legislation (see below).
3) By **reviewing the reports** submitted by service providers to ensure accurate reporting to law enforcement, and providing support, including through feedback on accuracy, to prevent imposing excessive obligations on the providers and in particular to avoid imposing the obligation to carry out an in-depth assessment of the illegality of the content detected, which can be relevant in particular in borderline cases. If possible CSAM is detected by the EU Centre, it will be added to the database of indicators of known CSAM only after public authorities have confirmed the illegality of the content. It could then also be used to improve the database of new CSAM indicators.

The support of the Centre would be particularly useful to **SMEs**, which would also be subject to the above requirements and could thus also receive a detection order from national authorities. the Centre and the Commission would provide additional support to SMEs in the form of **guidance**, to inform SMEs about the new legal framework and the obligations incumbent on them. This guidance could be disseminated with the help of industry associations. It may also be possible to provide **specific training**, in collaboration with Europol and the national authorities.

Box 16: technology to detect new CSAM

New CSAM often depicts **ongoing abuse** and therefore implies an **urgency to act swiftly** to rescue the child. Given the importance of this material, making its detection mandatory would ensure that more of it is detected and therefore more victims can be swiftly safeguarded.

The detection of **'new' content**, as compared to that of known content through hashes, typically relies on an algorithm which uses indicators to rank the similarity of an image to images already reliably identified and hence identify the likelihood of an image or video constituting CSAM. While the **patterns** that the AI algorithm is trained to identify cannot be equated one to one to known material, they are similarly designed to identify equivalent content. The reliability of such tools, as with any algorithm, depends on the specificity of the content and availability of quality training data, i.e. content already reliably identified as CSAM. Given the large volumes of "known" CSAM, automated identification of new CSAM has had a good basis for development and would be rendered more effective through the continuous expansion of the database of known CSAM confirmed by independent authorities. In addition, as opposed to situations where context is of relevance and needs to be analysed

(e.g. a slanderous expression reported on in a press article), the dissemination of CSAM is always illegal regardless of context. As a result, the challenge for automated detection is significantly lower in detecting what is often termed "manifestly illegal" content, compared to performing context-dependent assessments.

It is important to note that the process is similar to that for detection of known CSAM in that the classifiers are not be able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible CSAM. In other words, they are solely able to answer the question "is this content likely to be CSAM?", yes or no, and they are not be able to extract any other information from the content such as identifying specific persons or locations (i.e. they ignore all other content information transmitted).

The detection of new content is in general more complex than the detection of known content. Due to the nature of new material, after it is flagged by software, it requires **systematic human review** to ascertain its potential illegality. The accuracy rate nonetheless lies significantly above 90% (see annex 8, section 2 for an industry example that can be set at 99.9%, which means that only 0.1% of the content **automatically flagged** is non-illegal). Annex 8 section 2 contains additional information on new CSAM detection technology.

Conditions and safeguards

As in option C, the obligation to detect **new** CSAM would apply **regardless of the technology deployed in the online exchanges**, and as an **obligation of results,** to ensure that the legislation remains **technology neutral** and as **future proof** as possible.

Also, as in option C, the **competent national authorities**, on the basis of the risk assessment conducted by the service provider (including mitigating measures adopted), and, if needed, in consultation with the EU Centre and its technical experts on the technologies deployed, would determine whether a **detection order** should be issued to a given service provider. They would remain competent to verify the compliance with conditions and safeguards and to supervise the tools deployed, in cooperation with data protection authorities and the EU Centre's technical experts, where appropriate.

The legislation would specify the necessary **safeguards** to ensure a fair balance between all the affected fundamental rights. The safeguards could include **all** those described in option C extended to new CSAM, on 1) the technologies used, 2) how they are deployed, and 3) EU Centre-related safeguards. Given the high but comparatively lesser accuracy rates that detection tools for new content can have, the tools should be deployed in such a manner as to limit the number of false positives to the extent possible. The final determination of whether an image or video constitutes CSAM has to be made by a court or independent national authority. In addition, the **material** used to prepare and improve the indicators (AI classifiers) made available by the EU Centre could be subject to **periodic expert auditing** to ensure the quality of the data used to train algorithms.

*5.2.5. Option E: option D + **mandatory detection** of **grooming***

This option includes the policy measures of option D and adds mandatory detection of grooming for certain providers of interpersonal communications services as the key vectors for online grooming. It would therefore comprise the mandatory detection of the **three main forms** of CSA online: **known and new CSAM and 'grooming'** (solicitation of children), limited to the service providers relevant for each of the types of content, which are different for grooming: while CSAM can be shared in various ways, such as by message, sharing links

to image hosts or other means, grooming requires a direct communication channel between the offender and the child. Whereas known and new CSAM depict **crime scenes** of abuses already committed, grooming can indicate abuse that is **ongoing and/or about to happen** and which therefore **could be prevented or stopped**, protecting the child from harm.

As in options C and D, to ensure that the legislation is technology neutral, the obligation would apply **regardless** of the technology used in the online exchanges. Reporting and removal (upon the reception of a removal order) would be mandatory for all types of CSA online, as described in option B.

The services in scope in options C, D and E could be:

- for the risk assessment, reporting and removal obligations: relevant providers that provide or facilitate access to services enabling the dissemination of CSAM and grooming;
- for the obligations to detect known and new CSAM: a more narrow category of relevant service providers, in particular providers of hosting and interpersonal communication services;
- for the obligation to detect grooming: interpersonal communications services.

Mandatory risk assessment

Expanding the risk assessment outlined in options C and D, relevant service providers would be required to also assess the risk that their services are misused for **grooming**. Subject to further assessment, the **risk factors** to consider specific to grooming could include:

- the user base, including whether the service is available directly to end users (as opposed to, e.g., providing services to businesses),
- the verification of user identity in the registration process,
- whether the services are likely to be accessed by children or otherwise where children make up a significant proportion of a service's user base;
- the existence of functionalities of the service enabling adults to search for other users of the service (including children), e.g. if the profiles are searchable by default to all users;
- the existence of functionalities of the service enabling adults to contact other users (including children), in particular via private communications, e.g. if private messaging is enabled by default to all users and if private messaging is an integral part of the service;
- whether the services enable sharing images and videos via private communications for all users;
- whether robust age verification measures are in place (in particular to prevent adults from pretending to be children);
- whether the service offers grooming reporting tools that are effective, easily accessible and age appropriate;
- past experience with grooming on the same or a comparable service.

The service providers would then be **required to report** to the **competent national authority** the **risk assessment**, including any **mitigating measures** that they plan to adopt or have already adopted.

Detection order

Similarly to options C and D, on the basis of this risk assessment, the competent national authority would decide whether a **detection order** for **grooming** should be issued to a service provider, for one or more of its services. Where it is possible based on the risk assessment and technically feasible to limit the detection to a part of the service, the order should be limited to what is strictly necessary: for example, to perform detection only in one-on-one exchanges as

opposed to groups. This detection order would also be limited in time and renewable based on an updated risk assessment. Suitable redress for affected service providers would be provided for.

Support by the EU Centre

The EU Centre would support service providers in three ways:

1) By making available to providers the **database of indicators** of **grooming** (e.g. AI classifiers) that providers would be required to use to detect **grooming**, while ensuring a **technology neutral** approach. The indicators would be based on grooming cases determined by courts or other independent public authorities.
2) By making available to providers, **free-of-charge, technologies** to facilitate detection. Providers would not be mandated to use the technologies provided by the Centre and would be able to use other tools, as long as they meet the requirements and provide for the safeguards specified in the legislation (see below).
3) By **reviewing the reports** submitted by service providers to ensure accurate reporting to law enforcement, and providing support, including through feedback on accuracy, to prevent imposing excessive obligations on the providers and in particular to avoid imposing the obligation to carry out an independent assessment of the illegality of the content detected. If possible grooming is detected by the EU Centre, it could be used to improve the database of grooming indicators, after public authorities have confirmed the illegality of the content.

The above three-way support of the Centre would be particularly useful to **SMEs**, which would also be subject to the above requirements and could thus also receive a detection order from national authorities. The Centre and the Commission would provide additional support to SMEs in the form of **guidance**, to inform SMEs about the new legal framework and the obligations incumbent on them. This guidance could be disseminated with the help of industry associations. It may also be possible to provide **specific training**, in collaboration with Europol and the national authorities.

Box 17: technology to detect grooming

The detection of **grooming**, as compared to that of known content through hashes, typically relies on an algorithm which uses content indicators (e.g. keywords in the conversation) and metadata (e.g. to determine age difference and the likely involvement of the child in the communication) to rank the similarity of an online exchange to online exchanges reliably identified as grooming, and hence determine the likelihood of an online exchange to constitute grooming. The classifiers are not be able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible grooming. In other words, they are solely able to answer the question "is this online exchange likely to be grooming?", yes or no, and they are not be able to extract any other information from the content such as identifying specific persons or locations (i.e. they ignore all other content information transmitted).

The accuracy rate lies around 90%, which means that 10% of the content **automatically flagged for human review** is determined by the reviewers as non-illegal). The detection of grooming is therefore also based on AI patterns/classifiers, like the detection of new CSAM, and in general more complex than the detection of known CSAM. Due to the nature of grooming, after it is flagged by software, it requires **systematic human review** to ascertain its potential illegality. In addition, the tools are constantly fed with data to continuously improve

the detection process. Annex 8 section 3 contains additional information on grooming technology.

Despite the increase of grooming (see section 2.1.1.) and value of grooming detection to stop ongoing abuse and prevent imminent one, only **one third** of service providers that detect any form of CSA online detect grooming[192].

Conditions and safeguards

As in options C and D, the obligation to detect **grooming** would apply **regardless of the technology deployed in the online exchanges**, and as an **obligation of results,** to ensure that the legislation remains **technology neutral** and as **future proof** as possible.

As in options C and D, the **competent national authorities** would be given the necessary competences for effective oversight to determine whether conditions and safeguards are respected, also in terms of the deployment of technologies.

The legislation would specify the necessary **safeguards** to ensure proportionality and a fair balance between all the affected fundamental rights. The safeguards could include **all** those described in option C extended to grooming, on 1) the technologies used, 2) how they are deployed, and 3) EU Centre-related safeguards. In addition,

- the **material** used to prepare and improve the grooming indicators (AI classifiers) made available by the EU Centre could be subject to **periodic expert auditing** to ensure the quality of the data used to train algorithms;
- the service provider could be obliged to **report back** to the competent data protection authority on the measures taken to comply with any written advice issued by the competent supervisory authority for technologies to detect grooming, following and in addition to the prior data protection impact assessment and consultation;
- the technologies used to detect grooming should be limited to the use of **relevant key indicators and objectively identified risk factors** such as one-on-one conversations (as grooming very rarely takes place in a group setting), age difference and the likely involvement of a child in the scanned communication.

Stakeholders' views on mandatory detection from the open public consultation

Public authorities indicated that mandatory detection of known (71% of responses) and new CSAM (57%), and grooming (48%) should be covered by the possible legislation.
Child rights NGOs were in favour of mandatory detection and removal of known (78% of responses) and new CSAM (61%), and grooming (51%).
Privacy rights organisations opposed any mandatory detection measures and stressed the need to respect the requirements of necessity and proportionality to ensure the respect of fundamental rights of users, also with regard to privacy and confidentiality.
Service providers expressed little support for imposing legal obligations to detect known CSAM (12.5% of responses), new CSAM (6%) and grooming (6%). They flagged that, if there are any obligations, they should be formulated in terms of best reasonable efforts at the current state of technology, be in line with other EU legislation (e.g. e-commerce directive and DSA), and should not impose an excessive burden on SMEs. They raised questions of conflict of laws between the US and the EU emerging from detection and reporting obligations.
Individuals that responded to the open public consultation also expressed little support for imposing legal obligations for service providers to detect known CSAM (20% of responses), new CSAM (14%) and grooming (13%). At the same time, there was general support for a possible role of EU Centre managing a single EU database of known CSAM to facilitate detection.

[192] Survey carried out by the WeProtect Global Alliance, WeProtect Global Alliance Global Threat Assessment, 2021.

Box 18: YouGov survey on citizens' views on online child protection and privacy

A recent survey[193] carried out in eight Member States (DE, FR, IT, NL, PL, SE, ES, HU) in September 2021 in which nearly 9 500 adults participated found that:

- A majority (73%) of respondents believed that **children are not safe online.**
- Nearly 70% of respondents said they would **support a European law to mandate** online platforms to **detect and report** CSAM images and grooming, with technology scanning their photos and messages, even though this means giving up certain personal privacy.
- A majority of respondents (76%) **considered detection** of CSA online to be **as or more important** than people's personal privacy online.
- Most respondents in the qualitative research groups did not know that hash detection tools to address online CSAM existed or that anti-grooming tools had been developed. Once participants learnt about these tools, "they were angry that they weren't being used and turned on at all times". Participants in these groups held to this view even when they were told that their data could be scanned to achieve this.
- A majority of respondents (68%) felt that there is not much, if any, privacy online vs 25% of respondents who believed that it does.

5.3. Measures discarded at an early stage

The process of building the retained options started with scoping the widest spectrum of measures and discarding a number of them along the way, which included notably:

- **Indefinite continuation of the Interim Regulation**, i.e. extending indefinitely the current period of application of three years. This measure was discarded because it would not address in a satisfactory way the problem drivers, in particular problem driver 1, concerning the insufficient **voluntary** action by online service providers, and 2 on the lack of legal certainty (the Interim Regulation does not establish a legal basis for any processing of personal data). Also, the Interim Regulation only covers a subset of service providers whose services affected by CSA online. The possible combination of this measure with other options (including the practical measures in option A) would not be able to address these fundamental shortcomings.
- **Obligations to detect CSA online** (known and/or new CSAM, and/or grooming) **limited to technologies that currently make possible such detection** (e.g. unencrypted services). These measures were discarded because the legislation would not be effective in achieving the general objective of improving the functioning of the internal market by introducing harmonised EU rules for improving identification, protection and support for victims of CSA. Moreover, rather than improving the fight against CSA online, these measures could worsen it, by unintentionally creating an incentive for certain providers to use technologies in their services to avoid the new legal obligations, without taking effective measures to protect children on their services and to stem the dissemination of CSAM.

Annex 10 contains a further analysis of discarded options for the Centre.

[193] ECPAT, YouGov, Project Beacon, November 2021.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1. Qualitative assessment

The qualitative assessment of the policy **measures** (which form the policy options), is available in annex 4, section 1. This section focuses on the qualitative assessment of the policy **options** retained for analysis. It analyses the most relevant impacts, i.e. social, economic and fundamental rights, in addition to those related to the UN SDGs. The consistency of the options with climate law, the 'do no significant harm' principle and the 'digital-by-default' principle was taken into account throughout the assessment where relevant.

6.1.1. Social impact

All proposed measures except the baseline scenario would improve, to differing degrees, the protection of online users, particularly the young and vulnerable, and enhance the ability of authorities to prevent and respond to cases of online CSA.

6.1.1.1. Option A: **practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims,** and establishing an **EU Centre** on **prevention and assistance to victims**

The **practical measures** to enhance voluntary detection, removal and reporting of online CSA would improve the prevalence and effectiveness of voluntary measures to some extent, and would increase the number of related reports and investigations. The measures would also likely improve the efficiency and quality of reporting from service providers to law enforcement authorities, and allow more efficient use of resources by both. Uncertainty as to the legal basis for the necessary processing of personal data would remain, leading to **fragmented efforts**.

Establishing an **EU Centre** that could perform certain tasks relating to **prevention and assistance to victims** would help facilitate coordination and the implementation of practical measures in these areas. While these measures would to some extent improve efficiency in public-private cooperation, a number of difficulties would remain, in particular regarding a reliable source of hashes, a single European reporting point, accountability and transparency regarding providers' efforts, and the need for clear and comprehensive information on the prevalence of CSA online.

Finally, this option would likely not be sufficient in providing **effective assistance to victim**s of CSA, or to **prevent** CSA. While the practical measures included here may facilitate dialogue and exchange of information, they would **not be sufficient** to support the implementation of a holistic, evidence-based approach. The Centre's impact would be limited, as it would be supported by minimal resources and the support it could offer would be restricted. In particular in view of the significant impact of providers' efforts on the wellbeing of children and the rights of all users, the resulting continuation of a patchwork approach would fall short of the objectives.

Therefore, this option would **not fully address the problem drivers**.

6.1.1.2. Option B: option A + legislation 1) **specifying the conditions** for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal**

This option would specify the conditions for service providers' **voluntary detection,** reporting and removal of online CSA, eliminating key obstacles to voluntary efforts by providing legal certainty. This would allow services within the scope of the ePrivacy Directive (and its proposed revision) to adopt or continue voluntary efforts, following the lapsing of the Interim Regulation in 2024, as well as other relevant services. The **reporting obligation** would ensure both swift investigations to identify offenders and, where possible, identify and rescue victims, as well as independent verification of the illegality of the content.

The **removal obligation** would help ensure that service providers that have become aware of the existence of CSAM in their services take it down swiftly. This would limit revictimisation and would contribute to prevention efforts, given the effect that viewing CSAM has on increasing the probability of future offending (see box 1).

These obligations would also help create a **level playing field** for relevant providers active in the EU, as they would all need to comply with one framework for the detection, reporting and removal obligations.

The creation of EU-level databases of indicators of CSA online would facilitate service providers' determination of **what constitutes CSA online** under EU law. By maintaining a **single, reliable database in the EU of indicators** to facilitate detection of CSA online in companies' systems, the Centre would lead to significant improvements in the relevance of reports received by EU law enforcement authorities, reducing the number of reports of materials that do not constitute CSA online under the laws of the relevant Member State, and further eliminating erroneous removals. An increase in the volume of reports can be expected with the introduction of mandatory reporting and the creation of an EU database. Importantly, the database and the support provided by the EU Centre can be expected to contribute to an improved quality of reports. This in turn can be expected to result in **greater numbers of victims rescued and of perpetrators identified, prosecuted and convicted.** The consequential deterrence effects can support the prevention of future offending. The Centre would also act as a central point for reporting in the EU, supporting both service providers and hotlines, reducing the reliance on reports from third country organisations, and improving the ability of relevant authorities to respond to cases of online CSA also in particular across jurisdictions.

In addition, the Centre could facilitate, directly and in cooperation with hotlines, the removal of CSAM relating to a victim, **at the request of a victim**, by conducting searches and by notifying providers of content requesting it to be removed. In addition, the creation of a dedicated EU Centre would send an important message about the dedication of the EU as a whole to combating child sexual abuse more effectively and to ensuring that rules apply online as they do offline. It would place the EU at one level with those leading the fight against child sexual abuse worldwide, and would **reduce dependence on third-country entities**, both for operational reports and for strategic and horizontal information about threats and trends, areas where the EU and its Member States to date have very limited visibility. The social impact of the creation of an EU Centre to prevent and counter child sexual abuse is described further in annex 10, sections 4-6.

However, there are also some drawbacks to this option from the perspective of social impacts. As described in Section 2, experience has shown that service providers' **voluntary action by itself has been insufficient**. Only **12%** of service providers responding to the open public

consultation on the DSA reported that they used automated systems to detect illegal content they host[194]. This is reflected in the annual reports provided by NCMEC, which show that only a small percentage of providers registered to make reports to NCMEC have done so, that many of those who do make reports make very few of them, and that tools for the detection of CSA online are not widely used. Therefore, beyond ensuring that voluntary measures in interpersonal communications services can continue after the Interim Regulation expires, clarifications on the legal basis is unlikely to cause a significant increase in the use of voluntary measures.

Therefore, while option B would have a greater impact than option A through greater support for detection, reporting and removal efforts, it still **would not fully address the problem drivers**.

6.1.1.3. Option C: option B + **mandatory detection** of **known** CSAM

This option differs from Option B in two important aspects when it comes to its social impact. First, because it would introduce an **obligation to detect known CSAM**, and secondly because it would do so regardless of which technology is in use in the online exchanges.

The additional benefits of this option compared to Option B would be to ensure that the **detection of known CSAM** would no longer be dependent only on the voluntary action of providers. Detection would be focused on specific items of CSAM, which have earlier in an independent, reliable, specific and objective manner been found to be illegal. The detection would also be case-specific and limited in time, whilst assistance, safeguards and independent oversight would be provided for. Together with the aim of tackling particularly serious crimes, this all contributes to the conclusion that the obligation is in line with the prohibition on imposing **general monitoring** obligations. This option would also ensure that detection of known CSAM is performed regardless of the technology used. This would create a level playing field for relevant service providers, counteracting fragmentation and hence would have a positive effect on the realisation of the Single Market, building on the baseline harmonisation that the DSA is expected to provide.

In terms of the **protection of children** against the circulation of materials depicting their abuse, the obligation to detect is expected to have a **positive impact**. Over time, the overall number of images and videos depicting CSA available on services within scope should be reduced significantly, and, with it, the instances of **secondary victimisation** inherent in the continued viewing of the abuse. At the same time, it should entail a significant increase in the number of relevant service providers participating, in the volume of detection and reporting, and hence in the proportion of overall cases investigated and number of children identified and removed from abusive situations.

This would also have a positive impact on the overall **confidence of users** in services, as their exposure to CSAM would also be reduced. This positive impact would extend also to society's expectation that services do not facilitate the sharing of CSAM. While the targeting of specific services would possibly somewhat reduce the overall effectiveness of the obligation which could be greater if more services were included in scope, this can be justified in light of the greater impact that such detection might have.

For the detection of known content, the availability of **reliable indicators of what constitutes CSAM** under EU law and of **free-of-charge technologies** facilitating automatic detection would support service providers in their identification of relevant content and help

[194] Out of a total of 362 providers. Impact Assessment accompanying the DSA proposal, p59.

ensure proportionality of requirements. Known CSAM is the most common type of child sexual abuse online. The **tools** to detect it (see annex 8, section 1) have a **high accuracy rate** and have been reliably used for over a decade. The obligation to detect known material would **level the playing field** and ensure the detection of that content where is currently missing, with all the necessary **safeguards**. The **EU Centre** would make available the database of indicators of known material (e.g. hashes, URLs) that providers should use. The detection obligation might also encompass materials that victims have referred for detection and removal, or materials from concluded law enforcement investigations and that have been verified as CSAM by public authorities.

As a downside, such an obligation could result in occasional **false positives**, that is, in images and videos erroneously identified as CSAM. Given the gravity of an allegation of being involved in CSA, reporting could have a **negative impact** in the case of false positives and needs to be accompanied by safeguards ensuring that false positives are prevented as much as possible and that, where they occur, all data generated in relation to the false positives are erased, other than what is required for the improvement of automatic detection tools. Therefore, the Centre could provide an independent verification of the illegality of the content, eliminating manifestly unfounded reports, before forwarding reports that are not manifestly unfounded to Europol and national law enforcement authorities for action. Those authorities would, in addition, naturally still carry out their own assessments to determine whether further actions is necessary and appropriate in each individual case.

Given the impact on fundamental rights of all users, additional strict **safeguards** would apply, building on and going beyond those set out above for voluntary detection and for the reliability of the database of indicators. These could include **independent expert auditing** of the database of indicators and regular supervision and verification of the procedures of the Centre (with the involvement of data protection authorities as needed), independent expert certification of tools for automated detection to ensure **accuracy,** as well as additional **transparency and accountability** measures such as regular reporting. The legislation could also set out information rights of users and mechanisms for complaints and legal redress (see section 5.2.3.).

The application of an obligation **regardless of the technology used in the online exchanges** (including encryption) would ensure a level playing field regardless of service providers' choice of technology and would likely significantly increase the effectiveness of the obligation. On the other hand, it could potentially limit the effective exercise of users' right to privacy when it comes to the content of their communication and increases the burden on service providers as detection currently remains more challenging in E2EE communications. It is therefore only in light of the particularly egregious nature of CSA that such an obligation can be considered. This option would need to take into account the requirement of ensuring that the benefits of encryption for the privacy of all users are not compromised in the process of protecting children and identifying offenders. Technical solutions would therefore need to be carefully considered and tailored to balance these objectives. The obligation to detect would apply following a decision by the competent national authorities on a case by case basis, following the analysis of a risk assessment submitted by the service provider and taking into account technical feasibility.

The uniform application by all relevant online service providers to detect, report and remove known CSAM, regardless of the technology used in the online exchanges, would, over time, significantly affect the availability of CSAM on services falling within the scope of the initiative. It would decrease the blind spot caused by perpetrators' use of certain technologies

to share CSAM and abuse and exploit child victims. This would make private communications safer for children and help ensure that evidence of CSA can be found, leading to the identification of child victims.

6.1.1.4. Option D: option C + **mandatory detection** of **new** CSAM

The impacts of this option would be the same as option C, plus those of establishing a legal obligation for mandatory detection of new CSAM regardless of the technology used in the online exchanges.

The basic rationale for treating previously identified (i.e. known) and new CSAM the same is that both concern the same types of content, the difference between that the former has been independently confirmed as constituting **illegal material** under EU law whereas for the latter that has not (yet) occurred.

The additional challenge lies in the fact that detection of new CSAM relies on a **different technology**, which does not use hashes or URLs for individual images and videos but rather relies on **pattern recognition**, as set out in annex 8, section 2. The reliability and efficacy of such technologies is quite advanced, ensuring error rates in the low percentages, yet the burden on relevant service providers in ensuring the accuracy of efforts is significantly higher and would require an additional degree of human oversight and **human confirmation** of suspected CSAM.

Whereas the **proportion** of materials currently flagged as suspected new CSAM is significantly lower than that of known CSAM, new CSAM requires **systematic human verification**. The additional burden would need to be proportionate and compatible with the prohibition of general monitoring and active fact-finding as well as the need to strike a fair balance between the relevant fundamental rights at stake.

Such a balance may be supported by important objectives with respect to the interest of the child that would not otherwise be accomplished. Whereas the detection of known material reduces the **re-victimisation** of the child depicted in those images and videos and, at times, the investigation initiated with such a report may lead to uncovering ongoing abuses, this material depicts **past abuse**, which in some cases may be years old. By its nature, previously undetected CSAM usually depicts more recent and at times still ongoing abuse, provides particularly valuable leads, and is therefore treated as highest priority by law enforcement. The added value of detecting new CSAM in terms of the ability to identify and rescue children is significant. The **positive social impact** on children's welfare consequently is significantly higher than in the case of detection of known content alone.

The prompt detection of new material also allows for **prevention** of its distribution, and the possibility of it 'going viral' in circles of abusers, by adding it to the databases of known material that feed the automated detection tools. The subsequent detection based on the comparison with these databases can also provide important information about the way in which CSAM is disseminated online and the circles of abusers, facilitating detection and effective action against such groups, which would have a significantly positive social impact of tackling the problem closer to its roots.

The application of an obligation to detect new CSAM regardless of the technology used in the online exchanges carries similar considerations as those laid out under Option C. It would ensure that obligations are applicable to all service providers regardless of choice of technology, which is likely to produce better effectiveness of the obligation to detect new CSAM. In particular, any solution used in this context would have to ensure both the benefits that encryption provides for privacy of all users and the protection of the fundamental rights

of children. Solutions would need to be carefully considered and tailored to balance these objectives. This obligation is likely to increase the burden on service providers to deploy technical solutions that detect new CSAM in E2EE communications, including similar type of administrative burdens as to detection on new CSAM in un-encrypted communications to ensure accuracy, and mitigate error rates, including through **human review.**

Similarly to Option C, uniform application by all relevant online service providers to detect, report and remove new CSAM, regardless of the technology used in the online exchanges, would, over time, significantly affect availability of CSAM on services falling within the scope of the initiative.

6.1.1.5. Option E: option D + **mandatory detection** of **grooming**

The social impacts of this option would be the same as option D, plus those of establishing a legal obligation on relevant service providers for mandatory detection of grooming regardless of the technology used in the online exchanges.

Whereas the current number of reports of suspected grooming is significantly lower than that of CSAM, in particular known CSAM, grooming requires **systematic human verification**. The additional burden would need to be proportionate and compatible with the prohibition of general monitoring and active fact-finding as well as the need to strike a fair balance between the relevant fundamental rights at stake.

Such a balance may be supported by important objectives with respect to the interest of the child that would not otherwise be accomplished. Whereas the detection of known material reduces the **re-victimisation** of the child depicted in those images and videos and, at times, the investigation initiated with such a report may lead to uncovering ongoing abuses, this material depicts **past abuse**, which in some cases may be years old. In contrast, the identification and stopping of grooming is a measure that can serve to **protect children from falling victim to imminent abuse, or to stop ongoing abuse**. This is of particular relevance in the current situation in the pandemic, where children have been exposed to a significantly higher degree of unwanted approaches online including grooming. The **positive social impact** on children's welfare consequently is significantly higher than in the case of detection of CSAM alone.

The **detection** of grooming typically relies on tools for automatic text analysis, which are trained on verified grooming conversations and assess a given exchange according to risk factors identified on the basis of the verified grooming cases. Such tools are at the moment slightly lower in accuracy than tools for the automatic detection of known or new CSAM (see box 16 in section 5.2.4.) and would therefore require additional conditions and safeguards to avoid reports of false positives. The comparably higher invasiveness of text analysis tools and lower accuracy rate therefore has to be weighed against the interest in more effective protection of the child, particularly in calibrating the tool to avoid false positives at the expense of increasing the number of false negatives. In addition, where detection can be limited to parts of a service, determined on the basis of objective factors, this further contributes to ensuring the appropriate balance.

6.1.2. Economic impact

The assessment of the economic impact of the different options focuses on the impact on **service providers and public authorities** concerned by the measures.

The quantitative assessment is included in section 6.2. For a detailed assessment of the economic impact of establishing the Centre see annex 10.

6.1.2.1. Option A: **practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims,** and establishing an **EU Centre** on **prevention and assistance to victims**

Compared to the baseline scenario, the **practical measures** to enhance the voluntary detection, removal and reporting of CSAM would to some extent improve the quality of procedures and the cooperation between the private and public sector. In particular, the training of EU practitioners and the sharing of guidelines and best practices should have a positive impact and generate efficiency savings both for providers and for public authorities.

The practical measures to enhance actions on **prevention and assistance to victims**, including establishing an EU Centre as a hub without legal personality, would generate limited costs to the EU budget. They would have a potential to limit expenses on the side of the Member States, which could make use of existing research and expertise. The Centre's activities in the areas of prevention could lead to a reduction in relevant offences, while its victim support role could contribute to the recovery of victims, reducing the long-term impact of these crimes on victims and society. In all areas, the Centre's work could reduce duplication of efforts. However, this positive impact would be limited and would depend on the willingness of actors to cooperate.

The practical measures addressed to **authorities** to **improve cooperation with service providers** (training, standardised forms, online portal) would generate some moderate costs for them, but also improve the quality of reports and should therefore lead to a net reduction of costs for both service providers and public authorities. Likewise, the set-up of a feedback mechanism and communication channel would cause some moderate integration and maintenance costs but the benefits of such mechanism are expected to outweigh the expenses.

The practical measures addressed to **service providers** (streamlining of policies) would similarly generate moderate costs for them, in particular if changes to procedures have to be implemented, but public authorities would have a clear point of entry, reducing transaction costs, and would not have to adapt to a variety of individual service providers' policies, leading to cost reductions for public authorities. The Application Programming Interfaces (APIs) that public authorities could make available to allow service providers to remotely check hashed images and videos from their service against databases of hashes would generate moderate integration and maintenance costs for relevant public entities. However, as mentioned above, using common APIs would reduce transaction costs and overall costs in the long-run.

Supporting measures, technology and expertise sharing across platforms could limit potential economic burdens on relevant online service providers. Similar to service providers, the public sector would also benefit from interoperable tools and increased cooperation. There will also be a positive economic impact on expenses related to victim support.

6.1.2.2. Option B: option A + legislation 1) **specifying the conditions** for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal**

The economic impacts of this option are the same as in option A, plus those of clarifying the legal basis for the voluntary detection of CSA by relevant online service providers, a reporting and removal obligation, and the cost of establishing and maintaining an EU Centre.

Reporting obligations under this option could lead to:

- **additional costs to law enforcement authorities**, to adequately respond to the likely increase in reports from service providers. Furthermore, if law enforcement receives more reports where action is required due to more extensive and reliable datasets provided by the Centre, additional costs could be expected concerning identification of victims and offenders, investigations, criminal proceedings and support to victims and their families;
- **additional costs to service providers**, e.g. in technological developments and/or acquisition and maintenance, infrastructure expenditure and expert staff recruitment and training, in particular with regard to SMEs.

For both the public and the private sector, administrative and compliance costs could arise from **implementing new legislation**. On the other hand, the economic impact of (voluntary) earlier detection of CSA would be expected to be significantly positive with regard to the quality of life of survivors, their productivity, and reduced costs of lifelong victim support. In addition, a positive effect on the **Single Market** could result from additional legal clarity and certainty, thus **limiting compliance costs**.

Establishing an **EU Centre** would incur significant cost to the EU budget. However, the Centre would also contribute to limiting expenses for other stakeholders, including public authorities and service providers, by streamlining activities in an economic manner. The Centre's activities would support both law enforcement authorities and online service providers in the detection and reporting of CSA online, leading to greater efficiencies. It would facilitate compliance and reduce the costs of complaints and associated judicial proceedings by making available reliable information on content that is illegal in the EU. The Centre would also help streamline and facilitate **hotlines' efforts**, including with regard to proactive searches. In addition, more extensive and reliable datasets of e.g. hashes would help law enforcement prioritise their actions, reducing the time spent filtering out non-actionable reports. The Centre's activities in the area of **prevention** could lead to a reduction in relevant offences, while its **victim support** role could contribute to the recovery of victims, reducing the long-term impact of these crimes on victims and society. In all areas, the Centre's work could **reduce duplication of efforts**. In the long run, the Centre's activities would therefore lead to a **decrease in the economic costs** of CSA.

6.1.2.3. Option C: option B + **mandatory detection** of **known** CSAM

The impacts of this option are those outlined for option B plus those derived from the obligation to detect **known material.** For both the public and the private sector, administrative and compliance costs would arise from **implementing new legislation.**

For **service providers**, the introduction and maintenance of systems for the **detection**, where applicable, and the new or increased generation of reports would result in costs, also in relation to follow-up requests for further relevant data from public authorities, and for handling complaints and requests for review by affected users. However, they would benefit from the fact that this option would limit further **fragmentation** of the Internal Market with regard to administrative procedures and obligations required from hosting service providers. A number of service providers could build on systems they already have in place. In addition, the Centre would provide important support in making available technologies that can then be adapted to the needs of the providers. Technologies for the detection of known CSAM have been available free of charge for years and have proven their reliability.

SMEs offering hosting services are particularly vulnerable to exploitation through illegal activities, including CSA, not least since they tend to have limited capacity to deploy state-of-the-art technological solutions to detect CSAM or specialised staff. Therefore, while they should not be exempted from any rules and obligations, it is of particular importance to ensure that measures are proportionate and do not place an undue burden on them. The free availability of **reliable databases** of known CSAM indicators as well as **detection tools** (made available by the Centre) are important in this regard. Even though companies may have unequal resources to integrate technologies for the detection of CSAM into their products, this negative effect is outweighed by the fact that excluding them from this obligation would create a safe space for child sexual abuse and therefore defeat the purpose of the proposal. To further mitigate the economic impact on smaller companies, the verification of the illegality of the reported material could be left to the expertise of the EU Centre, in cooperation with the national authorities and the network of hotlines where needed and appropriate, which would inform the provider whether the material did in fact constitute CSAM. Therefore, these service providers would not be forced to invest in additional human resources for confirmation of suspected CSAM.

The expected **increase in reports** from service providers would result in significant additional costs to public authorities, in particular law enforcement and judicial authorities, arising from the corresponding increase in investigations and prosecutions. However, this financial impact is expected to be outweighed by the positive economic impact on victim support measures and survivor quality of life and productivity.

A positive effect on the **Single Market** could result from additional legal clarity and certainty, thus limiting compliance costs. Furthermore, both the public and the private sector would benefit from a common framework creating more legal certainty and mutual trust between the public and the private sector.

6.1.2.4. Option D: option C + **mandatory detection** of **new** CSAM

The impacts of this option are those outlined for option C plus those derived from the obligation to also detect **new material.** For both the public and the private sector, administrative and compliance costs would arise from implementing new legislation. However, all of the legislative options could reduce the fragmentation of the **Internal Market** and reduce compliance costs on the long term.

The expansion to new material could further **increase the workload of law enforcement**, compared to the previous option. While the overall number of new materials detected is expected to be lower than that of known CSAM, it will likely still be significant, considering that the cases require urgent and detailed attention, given the greater likelihood of ongoing abuse and the need for victim identification. Therefore, this increase in the workload will be accompanied by additional costs to respond to reports, costs related to starting investigations as well as the criminal justice process.

As in option C, **service providers** could encounter additional costs related to the integration and maintenance of detection technology and follow-up requests from public authorities, among others. Expanding the safety policy to new CSAM might require service providers to invest in adapting the available technologies to their individual products and possibly in recruiting trained staff to verify new material before reporting it. This could affect smaller providers in particular. To mitigate this effect, technologies would be made available free of charge. In addition, in the case of SMEs the human review and verification would be left to the expertise of the EU Centre which, in cooperation with national authorities and the network

of hotlines where needed and appropriate, would inform the provider whether the material constituted CSAM.

6.1.2.5. Option E: option D + **mandatory detection** of **grooming**

The impacts of this option are those outlined for option D plus those derived from the obligation to also detect **grooming.**

Expanding the obligation to detection of grooming would require relevant **service providers** to invest in integrating additional tools to detect this type of abuse. These costs could be mitigated by making available technologies free of charge via the EU Centre, limiting service providers' expenses to the integration of such tools into their services, and by relying on the EU Centre for the confirmation of cases identified as suspected grooming. By contrast, staffing costs for the Centre would increase as such cases require immediate reaction in order to ensure the protection of victims. Where the relevant service providers choose to rely on the Centre for verification before taking action, swift turnaround would have to be ensured in order to inform the provider about the need to intervene in an interaction and to protect a child.

Law enforcement would incur higher costs related to processing reports, compared to option D. The number of additional reports is expected to be lower compared to known CSAM, but as for new CSAM, swift action is required to protect the victim. The same considerations on administrative costs for the implementation of legislation as set out above apply. The positive economic impact when it comes to victim support and quality of life would increase, as the number of children that do not fall victim to hands-on child sexual abuse because of the timely detection of grooming would increase. This could potentially reduce the impact on victim support systems, compared to the previous options, as well as having a decisive impact on the quality of life and future productivity of the children.

Stakeholders' views on economic impacts

Service providers and business associations expressed in the open public consultation and the inception impact assessment their concerns regarding the economic impact for SMEs of possible legal obligations and that a 'one-size-fits-all' solution should be avoided. They also pointed out that the costs of deploying and maintaining technical solutions should not be underestimated.

Hotlines and public authorities indicated in the open public consultation and in the targeted consultations that increased reporting could result in increased costs for investigating, prosecuting, and managing offenders, and in assistance and support to victims.

6.1.3. Fundamental rights impact

According to Article 52(1) of the Charter of Fundamental Rights, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The objective pursued by the envisaged proposal, i.e. preventing and combating CSA, which is a particularly serious crime[195], constitutes an **objective of general interest** within the meaning of Article 52(1) of the Charter[196]. In addition, the proposal seeks to protect the rights

[195] CSAM is also the only type of illegal content whose mere possession is illegal.
[196] Cf. e.g. CJEU, *Digital Rights Ireland,* Joined Cases C- -293/12 and C-594/12, para. 42.

of others, namely of **children**. It concerns in particular their fundamental rights to human dignity and to the integrity of the person, the prohibition of inhuman or degrading treatment, as well as the rights of the child[197]. It takes into account the fact that in all actions relating to children, whether taken by public authorities or private institutions, the **child's best interests** must be **a primary consideration.** Furthermore, the types of CSA at issue here – notably, the exchange of photos or videos depicting the abuse – can also affect the children's rights to respect for private and family life and to protection of personal data[198]. In connection to combating criminal offences against minors the European Court of Justice has noted that at least some of the fundamental rights mentioned can give rise to positive obligations of the relevant public authorities, requiring them to adopt legal measures to protect the rights in question[199].

At the same time, the envisaged measures affect, in the first place, the exercise of the fundamental rights of the **users** of the services at issue. Those rights include, in particular, the fundamental rights to respect for privacy (including confidentiality of communications, as part of the broader right to respect for private and family life), to protection of personal data and to freedom of expression and information[200]. Whilst of great importance, none of these rights is absolute and they must be considered in relation to their function in society[201]. As indicated above Article 52(1) of the Charter allows limitations to be placed on the exercise of those rights, subject to the conditions set out in that provision.

More specifically, the measures aim to achieve the aforementioned objective by regulating both **'public-facing' and 'private'** services, including interpersonal communication services, which results in varying levels of intrusiveness regarding the fundamental rights of users. In the case of content that is accessible to the public, whilst there is an intrusion, the impact especially on the right to privacy is generally smaller given the role of these services as 'virtual public spaces' for expression and economic transactions. The impact on the right to privacy in relation to private communications will generally be greater. Such impact, where necessary to achieve the aforementioned objective, must be **necessary** and **proportionate** and be moderated by appropriate **safeguards**. The safeguards have to be differentiated and balanced in order to adapt inter alia to the **varying level of intrusiveness** depending on the nature of the communications services at issue.

Furthermore, the potential or actual removal of users' content, in particular erroneous removal (on the mistaken assumption that it concerns CSAM), can potentially have a **significant impact** on users' fundamental rights, especially to freedom of expression and information where content is removed erroneously. Such impact can depend inter alia on the service provider's position in the Internet 'stack'. Services lower in the Internet stack include those providing cloud infrastructure, web hosting, or content distribution network services. At the same time, content involving CSA that is left unremoved can have a significant negative impact on the aforementioned fundamental rights of the children, perpetuating harm for children and for society at large. Other factors to be taken into account in this regard include the nature of the user content in question (text, photos, videos), the accuracy of the technology concerned, as well as the 'absolute' nature of the prohibition to exchange CSAM (which is in principle not subject to any exceptions and is not context-sensitive).

---

197 Art. 1, 3, 4 and 24 of the Charter, respectively.
198 Art. 7 and 8 of the Charter, respectively.
199 See in particular CJEU, *La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18, para. 126.
200 Art. 7, 8 and 11 of the Charter, respectively.
201 Cf. e.g. CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, para. 120.

In addition, the **freedom to conduct a business** of the providers covered by the proposal comes into play as well[202]. Broadly speaking, this fundamental right precludes economic operators from being made subject to excessive burdens. It includes the freedom to choose with whom to do business and the freedom of contract. However, this right is not absolute either; it allows for a broad range of interventions that may limit the exercise of economic activities in the public interest[203].

The need to **strike a fair balance** between **all of the fundamental rights** at issue played an important role in the consideration of the various options. The initiative may not affect the essence of, or affect in an unjustified and disproportionate manner, the abovementioned fundamental rights. The options were pre-selected accordingly, and the main differences between the options relate to the extent of their effectiveness in safeguarding and balancing the various fundamental rights, considering their various degrees of interference, and the ability of the options to offer a more adequate response in light of both the current and the evolving risks emerging in a highly dynamic digital environment.

6.1.3.1. Option A: **practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims,** and establishing an **EU Centre** on **prevention and assistance to victims**

Compared to the baseline scenario, a limited positive impact on fundamental rights may be expected with respect to better coordination of efforts on prevention and assistance to victims of child sexual abuse with the support and facilitation of a newly established EU Centre, and on enhancing the voluntary detection, removal and reporting of child sexual abuse online.

A very limited impact on fundamental rights may be expected with respect to the **cooperation** between private and public authorities. Practical measures would ensure confidentiality of data sets, which may have a positive effect on the protection of privacy and personal data compared to the baseline scenario.

This option would furthermore increase **transparency** and **accountability** and would contribute to ensuring sound administration. There would be no change with regard to legal clarity and only a moderate impact on individuals' fundamental rights. This option would maintain the current framework of voluntary measures to address CSA and of cooperation with service providers. The rights and obligations of service providers would not be substantially affected.

6.1.3.2. Option B: option A + legislation 1) **specifying the conditions** for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal**.

Measures need to be **effective, necessary and proportionate** to tackle the crimes at issue and to protect the fundamental rights of children, including to give effect to the State's obligation to provide for the protection of children's rights and well-being, as a vulnerable group requiring particular care, and the effective application of its laws. In line with what was said above, these rights and interests need to be balanced against the following rights in particular:

Users' rights: when data is processed for the purposes of detection, this affects users' rights to freedom of expression and information, to the protection of personal data, and, where applicable depending on the type of service, to the confidentiality of their communications. While the rights to freedom of expression and information do not extend to protecting illegal

[202] Art. 16 of the Charter.
[203] Cf. e.g. CJEU, *Sky Österreich*, Case C-283/11, para. 45-46.

activities aimed at the destruction of any of the basic fundamental rights and freedoms, the detection would also need to check legal materials and exchanges for the presence of CSAM. As a result, a **strong justification** and **strong safeguards** would be needed to ensure an appropriate balance of the different fundamental rights. The **justification** consists essentially in the particularly serious crimes that the envisaged measures aim to prevent and combat and the protection of children that it aims to ensure. As described in section 5.2.3., the **safeguards** could include requiring service providers to use technologies and procedures that ensure accuracy, transparency and accountability, including supervision by designated authorities. In addition, the database of child sexual abuse indicators provided by the EU Centre would ensure a reliable basis for determining which content is illegal. The transparency and accountability that the Centre helps ensure could also help ensure that there are no erroneous takedowns or abuse of the search tools to detect legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse).

For interpersonal communications services, the users' fundamental right to privacy of communications are also concerned in particular. Therefore, supplementary safeguards would be required, including targeting the voluntary detection of new material and grooming to services where children may be at high risk, and providing clear information to users, as well as possible information once suspected abuse has been detected, including possibilities for redress. An additional safeguard lies in the anonymised processing by technologies[204], which ensures that the impact on the fundamental rights of users whose communications are processed would remain within reasonable limits and do not go beyond what is necessary, since no personal data deriving from their communications would be reviewed unless there is a justified suspicion of child sexual abuse (these technologies simply detect content like a virus scanner or spam filter, taking no records and not 'understanding' the substance of the communication, e.g. they answer the question 'does this image contain CSA **patterns**?' rather than 'what is this image about?').

Service providers' rights: This option would have no impact on the rights of service providers who choose to take no action to proactively detect child sexual abuse involving their services. On the other hand, service providers who choose to do so would be subject to new requirements that have not applied previously, in addition to those arising from the DSA proposal, such as requirements on the reliability and accuracy of technologies and on reporting and removal. Such requirements however are important safeguards for the fundamental rights of users.

Regardless of whether service providers decide to take voluntary action to detect CSA, they would be subject to reporting and removal obligations in case they become aware of the existence of CSA online in their services. These obligations impact service providers' rights but are necessary to safeguard the fundamental rights of victims.

As an additional important safeguard, the **EU Centre** would help improve **transparency and accountability**. The obligation to report would ensure that all instances of reported child sexual abuse online are independently verified, that action is taken to identify and rescue children, and that offenders are investigated. In addition, its existence would facilitate reporting to a Centre in the EU, thus limiting international transfers of personal data of EU citizens. By facilitating Member States' action on prevention and supporting victims in

[204] For example hashing technologies automatically convert images into a "hash", a code describing the image. This code cannot be converted back into an image and does not contain any personal data. The company then compares the hash of the image to a database of hashes of known CSAM. Where the hash of the user's image matches a hash in the database, the image is flagged as potential CSAM. See annex 8, section 1.

removing CSAM, the Centre would have a significant positive impact on the fundamental rights of victims and children who may become victims. The Centre itself would also be subject to safeguards as described in section 5.2.3. to ensure that it carries out its responsibilities fully and in a transparent way.

On the whole, provided appropriate limits and safeguards are ensured, this option would thus fairly balance the various rights at stake.

6.1.3.3. Option C: option B + **mandatory detection** of **known** CSAM

The rights to be balanced are the same as in the previous option; the difference lies in the greater impact on rights resulting from a) the mandatory nature of the detection of known CSAM and b) its application potentially regardless of the technology used in the online exchanges.

This option, because of the expanded and more effective action against CSAM, would have a **significantly positive impact on fundamental rights of victims** whose images are circulating on the Internet, in particular on their right to the respect for private life, and to the rights as children.

At the same time, the mandatory nature of the detection has a **notable impact on providers' freedom to conduct their business**. This can only be justified in view of the fundamental importance of tackling the particularly serious crimes at issue and more effective protection of children. Especially in the context of interpersonal communications, providers are **the only ones** that have visibility on the abuse taking place. Given that up to 80% of investigations in some Member States are possible only because of reports from providers, such a measure is objectively necessary[205]. In addition, providers would have access to free and verified detection tools. The obligation to detect known CSAM would **level the playing field** and ensure the detection thereof where it is currently missing, with all the necessary **safeguards**. It would be targeted, risk-based, limited in time and would not impose an undue burden on providers.

In addition, **users' rights** (in particular freedom of expression, privacy and data protection) are concerned to a greater extent than under the previous option. The availability of reliable and verified tools could ensure that the impact on their rights does not go beyond what is strictly necessary, by limiting the interference and reducing the risk of false positives and the possibility of misuse. In particular, there would be no human interaction with interpersonal communications of users beyond the communications that have been automatically identified as containing CSAM.

On the whole, provided appropriate limits and safeguards are ensured, this option would thus fairly balance the various rights at stake.

Box 19: risk of misuse of tools to detect CSA online for other purposes

There is a risk that the technologies intended to detect CSA online are repurposed and misused for other purposes. This risk is common across technologies and across technical fields, including other technologies used in online services (e.g. the GPS or the camera of a mobile phone, which could be misused for surveillance). In fact, the underlying technologies behind the most common tools to detect CSA online are in themselves applications of

[205] While the prohibition to impose an obligation of general monitoring or active fact-finding does not rank in itself as a fundamental right, it serves as a safeguard to facilitate the appropriate balancing of rights and interests. As set out in more detail above in section 5.2.3, this obligation would be complied with.

technologies that were not originally developed for the exclusive purpose of detecting CSA online. For example, hashing is an application of digital fingerprinting, which was already being used to detect malware when tools like PhotoDNA were first developed. Likewise, AI, the underlying technology to detect new CSAM and grooming, was not originally developed to detect CSA online. The possibility of repurposing a technology (and therefore the risk of misuse) exists since the technology is **first** developed. In the case of the tools to detect CSA online, these have existed for over a decade (e.g. PhotoDNA) and there is so far no evidence of that risk having materialised; the tools have been made available under a licensing agreement limiting their use to the detection of child sexual abuse content, which appears to have been respected. The legislation would include safeguards on purpose limitation, the way they are deployed, and oversight by competent authorities and the EU Centre to keep the risk of misuse to the absolute minimum.

6.1.3.4. Option D: option C + **mandatory detection** of **new** CSAM

The rights to be balanced are the same as in the previous option; the difference lies in the greater impact on rights resulting from the mandatory detection of new CSAM.

This option would represent a higher impact on providers' freedom to conduct a business and more interference into users' right to privacy, personal data protection and freedom of expression. However, there is corresponding increase in the types of CSA that are tackled and, thus, to the achievement of the objective of combatting the particularly serious crimes at issue and protecting children. Moreover, stricter safeguards, remedies and transparency and accountability measures would be provided for to safeguard users' rights.

Given the similar nature of the materials to be detected and the reliance on verified indicators to be provided by the EU Centre, the **detection** of new material would in principle have a **comparable level of intrusiveness** as the detection of known CSAM. However, given that accuracy levels of current tools, while still being well above 90%, are lower than for the detection of known CSAM, human confirmation is essential. This would add to the service providers' burdens and increase intrusiveness, but is deemed necessary to avoid errors and the negative consequences that such errors might have, including for users' rights. The need to rely on human confirmation could decrease as the technology develops, partly as a consequence of the obligations to detect new CSAM in this option. In addition, strict requirements and safeguards would apply, including on the reliability of indicators and independent supervision, and reliable detection tools made available free of charge.

Similarly to Option C, the identification of the specific providers in scope would be done through detection orders issued by Member States' national authorities. This ensures a case-by-case, risk-based and time-limited approach, thus contributing to the proportionality of the approach. For the detection of new CSAM a specific, **higher threshold would apply** (as compared to detection orders for known CSAM), i.e. only **services at a high and objective risk of being misused for the exchange and dissemination of new CSAM** would be subject to a detection obligation.

In light of the new nature of most previously undetected CSAM, this option would have **a positive impact on victims of ongoing abuse** and would significantly enhance the possibility of safeguarding victims from additional abuse. In addition, the early detection and confirmation of new CSAM and the swift addition thereof to the database of known CSAM can help limit the spreading of CSAM across service providers.

Overall, the measures in this option would therefore fairly balance the affected fundamental rights while having a significantly greater positive effect on the rights of victims.

6.1.3.5. Option E: option D + **mandatory detection** of **grooming**

The impacts of this option are the same as in Option D, with the **important difference** of the additional impact caused by requiring service providers to also detect grooming. The introduction of this obligation would have a higher impact on fundamental rights, which would be balanced by **stricter personal data protection and privacy safeguards while providing redress, accountability and transparency**.

Detecting grooming would have **a positive impact** on the fundamental rights of potential victims by contributing to the prevention of abuse. At the same time, the detection process would be the **most intrusive one** for users (compared to the detection of known and new CSAM) since it would involve searching text, including in interpersonal communications, as the most important vector for grooming. On the one hand, such searches have to be considered as necessary to combat grooming since the service provider is the only entity able to detect it. Automatic detection tools have acquired a high degree of accuracy[206], and indicators are becoming more reliable with time as the algorithms learn, following human review. On the other hand, the detection of patterns in text-based communications may be more invasive into users' rights than the analysis of an image or a video to detect CSAM, given the difference in the types of communications at issue and the mandatory human review of the online exchanges flagged as possible grooming by the tool.

This obligation **would be restricted to only certain specific service providers** (identified, on a case-by-case basis, through the detection orders of Member States' national authorities), which are at **high risk of being misused for grooming**, which would further reduce the fundamental rights impact only to the users of those services and the providers concerned. This approach would contribute to ensure the required level of proportionality.

In this option, detection obligations would apply to the three main types of CSA online (known CSAM, new CSAM and grooming). Compared to voluntary detection, which leaves to private parties the decision of whether to detect, under this option the legislator is the one taking the decision on whether to detect all three types, given the particularly serious objective of public interest at stake, setting out the conditions and safeguards under which that detection should take place.

Overall, provided appropriate limits and safeguards are ensured, the measures in this option would therefore fairly balance the affected fundamental rights while having a significantly greater positive effect on the rights of victims.

6.1.4. UN SDGs impact

6.1.4.1. Option A: **practical measures** to enhance **prevention, detection, reporting and removal, and assistance to victims,** and establishing an **EU Centre** on **prevention and assistance to victims**

Enhancing voluntary detection, removal and reporting of online CSA and the creation of the EU Centre on prevention and assistance would to some extent contribute to relevant SDGs. Notably, limiting the likelihood of girls and children in general falling victims to CSA would positively impact SDG 5.2 (eliminate all forms of violence against women girls, as a majority of CSA victims are girls) and SDG 16.2 (end abuse, exploitation, trafficking and all forms of

[206] For example, Microsoft reports that the accuracy of its grooming detection tool is **88%**, see annex 8.

violence against children). This option would also help to minimise the short and long-term negative health consequences of CSA and support mental health for victims and offenders or people who fear that they might offend (SGD 3: health and well-being), and address SDG 4 (education) e.g. through prevention campaigns to raise awareness of CSA online risks. This option would also affect, to a lesser extent, SDG 1 on poverty (e.g. by supporting research on long-term economic effect of CSA).

However, the overall impact of this option would be limited, as the actions would remain fragmented, and the overall reduction of the circulating CSAM would be limited.

6.1.4.2. Option B: option A + legislation 1) **specifying the conditions** for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal**

This option would clarify the legal basis for service providers' voluntary detection of CSA online, which, along with the expansion of the EU Centre to a broader **facilitator** role covering also detection, reporting and removal of CSA online, would contribute to a reduction of the prevalence of CSA and consequently a reduction of victimisation of girls (SDG 5.2), and the sexual exploitation of children in general (SDG 16.2).

This option would also address to some extent SDG 3 on health and well-being, and SDG 4 on education, similarly to option A. It would also contribute to SDG 9 (industry, innovation and infrastructure), supporting service provider's efforts to develop technology to fight CSA online.

6.1.4.3. Option C: option B + **mandatory detection** of **known** CSAM

This option would have a positive impact on the same SDGs as option B, but stronger. The obligation to detect is expected to significantly reduce the number of CSAM available online, which would lead to a more positive impact on **all SGDs** described in option B, in particular SDG 5.2, and SDG 16.2.

6.1.4.4. Option D: option C + **mandatory detection** of **new** CSAM

The impacts of this option would be the same as option C, plus those of establishing a legal obligation for mandatory detection of new CSAM. The obligation to detect new CSAM would further reduce the number of CSAM available, positively impacting **all SGDs** described in option B.

6.1.4.5. Option E: option D + **mandatory detection** of **grooming**

The impacts of this option would be the same as option D, plus those of establishing a legal obligation for mandatory detection of grooming. The obligation to detect grooming, with its positive effects on preventing imminent crimes (and stopping ongoing ones) could lower the prevalence of CSA, positively impacting **all SGDs** described in option B.

6.2. Quantitative assessment

The quantification of the costs and benefits of the policy measures/policy options is limited by the **lack of data**, in particular on the level of abuse on services which do not currently make significant numbers of reports, as it is unclear whether this indicates a lower level of abuse on those services, or less effective efforts to detect and report such abuse. This requires the use of a number of **assumptions**, described in detail along with the rest of the methodology used, in annex 4, sections 3-4. Given these limitations, the estimates in this section provide an idea of

the **order of magnitude** of costs and benefits and therefore should not be taken as exact forecasts.

6.2.1. Costs

All the policy options under consideration would result in costs for public authorities, service providers, and the Centre. Each policy option includes measures relating to prevention, assistance to victims, and detection, reporting and removal of online child sexual abuse.

In the area of **prevention**, costs would be incurred by the Commission as a result of the practical measures in Option A, under which the **Commission** would have responsibility for managing the Centre as a knowledge hub without legal personality. Under all other options, costs related to prevention measures would be borne by the **Centre** itself.

Costs in the area of **assistance to victims** would similarly by borne by either the **Commission or the Centre**, depending on the option chosen. In addition, measures to improve prevention and assistance to victims would likely give rise to costs for Member States.

Measures relating to the **detection, reporting and removal of online CSA** would entail administrative costs for **service providers and public authorities** under all options. These relate to the expense for service providers to implement measures to detect, report and remove online CSA, whether on a voluntary or mandatory basis, as well as the cost to both service providers and public authorities of processing each report. Under Options B to E, the Centre would also incur costs relating to the handling of reports, as well as costs for the creation and maintenance of an EU database of indicators of online child sexual abuse.

The cost model built to estimate the above costs first determined the composition of an average report today, based on the total amount of known and new CSAM files and grooming reports made in 2020. Then it estimated the cost of this average report, based on the estimated time that service providers and public authorities require for processing and following up on it (including investigations). It also estimated the number of reports in the coming years under the baseline scenario under **voluntary detection**, assuming that the number of reports would continue to grow in line with trends over recent years. It also assumed that the level of abuse detected and reported by Facebook, which is the top provider of reports to NCMEC, is indicative of the level of abuse that could potentially be detected and reported by other providers under **mandatory detection**. Finally, the model estimated the costs of each policy measure by estimating how the policy measure would change the composition of the average report and/or the number of reports compared to the baseline.

The estimated costs of each measure and option are presented in table 3 and table Table4, below.

Table 3: cost estimates for the retained policy measures (EUR millions)

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0,4	€0,2	€3,5	€2,8
2	€0,0	€0,0	€10,3	€0,0
3	€5,0	€0,0	€25,7	€0,0
4	€0,0	€137,7	€11,1	€6,9
5	€0,0	€20,4	€3,3	€1,7
6	€0,0	€352,2	€503,6	€459,4
7	€0,0	€604,4	€250,1	€520,5

8	€0,0	€618,0	€28,2	€471,9

Table 4: one-off and continuous costs estimates for the policy options (EUR millions)

POLICY OPTIONS	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
A	€0,4	€0,2	€13,9	€2,8
B	€5,4	€158,4	€43,6	€11,4
C	€5,4	€466,9	€547,3	€470,9
D	€5,4	€1.025,0	€797,4	€991,3
E	€5,4	€1.595,3	€825,6	€1.463,3

6.2.2. Benefits

The main quantitative benefits derive from savings as a result of **reduction of CSA** associated costs, i.e. savings relating to offenders (e.g. criminal proceedings), savings relating to victims (e.g. short and long-term assistance), and savings relating to society at large (e.g. productivity losses).

To estimate the benefits the first step is therefore to determine the total CSA costs in the EU. As indicated in section 5.1 on the baseline, the estimated annual costs of CSA in the EU are **EUR 13.8 billion**.

Box 20: estimation of annual costs of CSA in the EU

No studies that have estimated the total costs of CSA in the EU, or in a Member State are known to be published[207].

Letourneau et al. estimated the total annual costs of CSA in the US, adjusted to the reference year 2015, in a paper that appeared in 2018 in the **peer-reviewed** journal Child Abuse & Neglect[208]. The paper estimated total costs including health care costs, productivity losses, child welfare costs, violence/crime costs, and special education costs, based on secondary data drawn from papers published in **peer-reviewed** journals. The paper indicates that its estimates of annual losses of USD 11 billion are **conservative and minimum**, since they could not include the economic impact of nonfatal CSA on male victims due to lack of data, and they relied on cases reported to child protection agencies, whereas it is widely recognised that a substantial proportion of CSA cases never comes to attention of child protection agencies[209].

For comparison, the other known study[210] on CSA costs in the US (not peer-reviewed) estimated the annual costs in USD 23 billion. And the only other known peer-reviewed paper (in addition to Letourneau et al's) on CSA costs estimated the annual costs in Canada in approximately CAN $3.70 billion[211], with a population less than 10% that of the EU.

[207] The lack of EU-specific studies is an important gap in knowledge in the fight against CSA in the EU. Such research could be facilitated through the prevention and assistance to victims functions of the Centre.

[208] Letourneau et al., The economic burden of child sexual abuse in the United States, May 2018

[209] IOM, NRC, Child maltreatment research, policy, and practice for the next decade: Workshop summary, The National Academies Press, Washington, DC (2012).

[210] T.R. Miller, M.A. Cohen, B. Wiersema, Victim costs and consequences: a new look, 1996.

[211] O. Hankivsky, D.A. Draker, The economic costs of child sexual abuse in Canada: a preliminary analysis, Journal of Health & Social Policy, 17 (2) (2003), pp. 1-33.

Although Letorneau et al's paper concerns the US, studies on the economic cost of violence against children (including child sexual abuse) suggest that costs are comparable among high-income countries[212]. Therefore, the **conservative** estimates provided in the above-mentioned paper are assumed to be applicable in the EU context, when adjusted to take account of the larger population in the EU in 2021 compared to that of the US, the inflation rate 2015-2021 and the exchange rate USD-EUR in April 2021, resulting in a total of EUR 13.8 billion of annual CSA costs in the EU.

The quantitative benefits originate mainly from two sources:

- savings from CSA crimes prevented: these result not only from the options that explicitly cover prevention but also from those that cause an increase in the number of reports (e.g. those imposing detection and reporting obligations on service providers). The increase in reports is likely to lead to an increase in victims rescued from ongoing and/or imminent abuse as well as to an increase in arrests, which in turn could lead to prevention of future crimes by those offenders. It could also lead to an increase in removal of CSAM, with the positive effects on prevention that it entails (see box 1). In addition, the prosecuted offenders would have (improved) access to prevention programmes during and after criminal proceedings (including during and after prison), which could decrease reoffending. Moreover, the increase in reports could also have a deterrence effect, and thereby prevent additional offences;
- savings from better assistance of victims: these would result from a better mitigation of the negative effects of these crimes on victims, e.g. by facilitating Member States' action in this area through the exchange of best practices and research, and supporting the takedown of images and videos (including at the victims' request).

It is not possible to determine exactly what would be the benefits caused by each of these two sources or each policy measure, such as the obligations on service providers or the Centre. In addition, it is not possible to forecast with certitude what would be the exact benefits of each policy measure. For example, the reduction of CSA due to prevention would depend to large extent on the investments and efforts from Member States and the EU, which the policy options considered in this initiative could only help facilitate.

Considering the qualitative considerations above, it would be safe to estimate that the quantitative benefits could be up to 50% of the annual costs of CSA in the EU (remembering that the amount of EUR 13.8 billion was a conservative estimate).

The calculation of benefits for each of the options will take an even more conservative approach and assume that the benefits would be in the middle of that range, i.e. a maximum of 25% of the total annual costs. This calculation also assumes that there is a direct correlation between the factor that can be best quantified, the increase in reports, and the estimated savings. This is of course an approximation, as the savings could also derive from other components not linked to the increase in reporting, as explained above, but it facilitates the comparison of options. The model therefore assumed a cost decrease of 25% for option E (highest number of reports) and applied the same ratio of increase in reporting vs decrease in costs from option E to the other options.

[212] See, for example Ferrara, P. et al., The Economic Burden of Child Maltreatment in High Income Countries, December 2015.

Table 5: estimated benefits for the policy options (EUR million)

POLICY OPTIONS	Estimated number of reports	Estimated increase in reporting compared to the baseline	Estimated cost reduction	Benefits (millions per year)
Baseline	1.939.556	-	-	-
A	2.133.584	10%	0,7%	97,3€
B	2.385.726	23%	1,6%	223,8€
C	7.521.652	288%	20,3%	2.800,3 €
D	8.691.029	348%	24,6%	3.386,9 €
E	8.812.811	354%	25,0%	3.448,0 €

See **annex 4, sections 3 and 4** for further details on the model, the assumptions and the calculations.

7. HOW DO THE OPTIONS COMPARE?

7.1. Qualitative comparison

7.1.1. Criteria for the comparison

The following criteria are used in assessing how the five options would potentially perform, compared to the baseline:

- **Effectiveness** in achieving the specific objectives.
- **Efficiency**, i.e. cost-benefit assessment of each policy option in achieving the specific objectives.
- **Coherence** with all relevant policy instruments in the fight against CSA:
    a. Legislation:
        i. horizontal instruments (GDPR, ePrivacy Directive and its proposed revision, e-Commerce Directive and the proposed Digital Services Act, Victims' Rights Directive);
        ii. sector-specific legislation (CSA Directive, Interim Regulation, Europol Regulation and its proposed revision);
    b. Coordination: EU level cooperation in investigations, prevention and assistance to victims, as well as multi-stakeholder cooperation at EU and global level;
    c. Funding.
- **Proportionality**, i.e. whether the options go beyond what is a necessary intervention at EU level in achieving the objectives.

7.1.2. Summary of the comparison

Table 6 below summarises the qualitative scores for each main assessment criteria and each option. The options are compared below through listing positive (+), negative (-) and 'no-change' (~) impacts compared to the baseline (> indicates higher costs compared to the baseline).

The detailed comparative assessment of all options can be found in annex 4, section 2:

Table 6: summary of the comparison of policy options

	Effectiveness	Efficiency		Coherence			Proportionality
		Costs	***Benefits***	***Leg.***	***Coord.***	***Fund.***	
Baseline	~	~	~	~	~	~	~
Option A	+	>	+	+	+	+	+
Option B	++	>>	++	+	++	+	+
Option C	+++	>>>	+++	+	+++	+	+
Option D	++++	>>>>	++++	+	+++	+	+
Option E	+++++	>>>>>	+++++	+	+++	+	+

7.1.3. Effectiveness

The scores on effectiveness indicate the extent to which the impacts screened in section 6 contribute to the achievement of the specific objectives.

1. Ensure the effective detection, removal and reporting of online child sexual abuse where they are currently missing

While options A and B could improve detection, removal and reporting of online child sexual abuse, their effectiveness is significantly limited by their reliance on voluntary action by providers when it comes to detection, which has proven to be insufficient. Under option A, as under the baseline, many of these activities would be prohibited following the expiry of the Interim Regulation.

Options C to E are the only options which would ensure the effective detection and reporting of online CSA. In particular, Option E would have the highest effectiveness as it would ensure that all relevant online service providers detect known and new CSAM, and grooming.

Whereas option C imposes obligations to detect only known CSAM, options D and E, impose additional, cumulative obligations to detect new CSAM and grooming respectively. As described in Section 6.1.1, the detection of new CSAM and grooming, by their nature, provide greater added value in terms of the ability to identify and rescue children from ongoing or imminent abuse. As such, the effectiveness under options D and E is higher than in option C. The obligations to detect, and report known and new CSAM and grooming are a significant step forward. Reliable tools for the detection of CSA online are already freely available and in use by a number of service providers. Extending their deployment to all relevant online services could greatly contribute to virtually eliminate the dissemination of known CSAM on such services and significantly reduce the dissemination of new CSAM, and the instances of grooming. The Centre would facilitate the detection, reporting and removal process, including by making available technology and possibly contributing to their developments through its technical expertise[213].

[213] Researchers have acknowledged the need to continue developing technical tools to detect, report and remove CSA online. See for examples, Insoll T, Ovaska A & Vaaranen-Valkonen N, (Protect Children), CSAM Users in the Dark Web: Protecting Children Through Prevention, 2021.

2. Improve legal certainty, transparency and accountability and ensure protection of fundamental rights

Option A, which consists of non-legislative measures, offers the least improvement in terms of legal certainty, protection of fundamental rights, transparency and accountability. Any such improvements under Option A would be largely limited to legal advice and jurisprudence and the establishment of best practices to be adhered to on a voluntary basis.

Options B to E could all offer significant improvements in these areas. Under each of these options, the conditions for voluntary detection would be clarified and mandatory measures to detect, report and remove CSA online would be established, ensuring improved legal certainty for all stakeholders. In addition, each of these options would establish robust safeguards and accountability mechanisms to ensure strong protection of fundamental rights. These would include notably the designation of a competent national authorities to assess the measures implemented by relevant online service providers, impose detection and removal orders, and impose sanctions on providers that do not meet their obligations. These options would also establish transparency obligations for both service providers and the authorities designated to receive reports from and supervise providers, as well as redress mechanisms for users, among other safeguards.

Both the baseline scenario and option A would not address the current challenges and the impact on children's fundamental rights would likely worsen with time.

Option B would increase legal certainty for detecting CSA voluntarily and would also create an obligation to report once a provider becomes aware and remove CSAM, once confirmed to be illegal. In addition, the activities of the EU Centre would have a significant positive impact on the fundamental rights of victims and children who may become victims. The necessary safeguards would also be provided in order to balance the interference with the rights of the users and providers. However, the detection of CSA would remain voluntary, which would not ensure a consistent protection for children who are or might become victims, while there will still be an impact of privacy and data protection rights of all users. In sum, this option would have a certain negative impact on fundamental rights, particularly those of children.

Options C to E would render the detection of CSA mandatory, and, especially since the systems used for detection can affect relevant fundamental rights would include comprehensive safeguards. Furthermore, appropriate checks and balances are also to be set up, notably through sanctioning mechanisms and reporting and transparency requirements, and supervision by the competent national authorities, supported where relevant in the technical aspects by the EU Centre to prevent and counter child sexual abuse. These options would have overall small positive (Option C), significant positive (Option D) and significant positive (Option E) impacts on fundamental rights, particularly those of children.

The fundamental rights most clearly touched upon by the intervention are the following:

- Rights to human dignity and integrity of the person, prohibition of inhuman and degrading treatment and rights of the child (Articles 1, 3, 4 and 24 of the Charter).

All five options would have a positive impact in protecting the safety and rights of children. Consistent with the analysis in section 6.1.3 the positive impact is strengthened with each subsequent option. Given the seriousness of the crimes at stake and of the impact on children, being vulnerable persons entitled to protection by the public authorities, the objective pursued by the envisaged measures is capable of justifying a significant interference with the fundamental rights of other parties involved (service

providers, users), provided that the interference respects the essence of those rights and remains limited to what is necessary.

- Rights to respect for private and family life, protection of personal data, and freedom of expression and information (Articles 7, 8 and 11 of the Charter).

Each of the options would have an impact on privacy and the protection of personal data, with regard to both the users of relevant online services and victims or potential victims of child sexual abuse. All options take into account the need to balance these impacts by including strong safeguards for voluntary/mandatory detection, reporting and removal of online CSA.

Evidently, the obligations imposed by Options C, D and E would have the greatest impact on overall users' rights, especially those to privacy and on personal data protection, due to the data to be processed in the detection and the progressively increasing need for human review with each option. Furthermore, errors in the detection process could have additional negative consequences for users' rights, such as erroneous decisions to remove users' content, or limit access, which would impact their freedom of expression and information. At the same time, the scope for erroneous decisions is likely to be limited, especially when adequate safeguards are provided for, bearing in mind the 'absolute' (non-context-specific) nature of the prohibition of distributing CSAM. That holds in particular in respect of Options C and (to a somewhat lesser extent) Option D, considering the accuracy of the technologies which would need to be used.

On the other hand, the progressively increasing detection and number of reports of online child sexual abuse expected under each option would result in corresponding improvements to the rights of victims (and potential victims) to privacy and personal data. In particular, options C, D and E would contribute significantly to safeguarding rights of victims, while robust safeguards would ensure proportionality and limit interference to what is strictly necessary.

- Freedom to conduct a business (Article 16 of the Charter).

Another important element of the overall balance that has to be struck is the balance between facilitating or mandating action against CSA online and the protection of providers' freedom to conduct a business.

The options considered in the impact assessment take into account the need to ensure that any impact upon these rights and freedoms would be strictly limited to what is necessary and proportionate, whilst leaving the essence of the freedom to conduct a business unaffected. While Options A and B would not directly or significantly affect the freedom to conduct a business, Options C, D and E would entail an interference with this freedom, while however minimising negative effects on this right by ensuring a level playing field for all providers offering services in the Union, regardless of their size or location. The interference with this right will be further mitigated by the strong support offered by the Centre, the availability of the necessary technology at no or limited costs, as well as the benefits associated with operating under a clear and uniform legal framework.

3. Reduce the proliferation and effects of CSA through harmonisation of rules and increased coordination of efforts

The non-legislative measures of Option A are less effective than the rest of the options, which includes the creation of the EU Centre to support prevention and assistance to victims, as well as detection, reporting and removal of CSA online. Practical measures can only lead to

limited improvements, and cannot replace a Centre as reference entity in the EU and a facilitator on all the aspects of the fight against child sexual abuse.

7.1.4. Efficiency

Except for the baseline, all options would generate some additional administrative costs for public authorities as a result of the anticipated increase in reporting of CSA. Options C to E would lead to significant cost increases for public authorities due to the significant increase in the volume of reports of online CSA expected to arise from the obligations imposed on service providers under those options.

For service providers, all options will generate administrative and other costs, and may also result in savings when processes become more efficient. The extent of additional costs to service providers will, in part, depend upon the nature and size of their services, which is expected to affect both the volume of data to be processed for the purposes of detection and reporting, and the cost of integrating the relevant technologies.

Given the cumulative nature of the options, the costs also increase with each option, driven in particular by the increased detection obligations. These will entail a progressive increase in reports and therefore increased costs for both service providers and public authorities. On the other hand, these increased obligations would also lead to increased benefits derived from savings as a result of **reduction of CSA** associated costs, i.e. savings relating to offenders (e.g. criminal proceedings), savings relating to victims (e.g. short and long-term assistance), and savings relating to society at large (e.g. productivity losses).

7.1.5. Coherence

a) Legislation

Horizontal instruments

- *GDPR*

The proposed measures in Options B to E build on the GDPR. At the moment, various grounds for processing set out in the GDPR are invoked by service providers to carry out the processing of personal data inherent in voluntary detection and reporting of CSA online. Options B to D would specify the conditions for mandatory and voluntary detection, providing greater legal certainty for those activities.

Insofar as mandatory detection activities involving processing of personal data are concerned, options C to E would build on the GDPR's Article 6(1)(c), which provides a legal basis for the processing of personal data to comply with a legal obligation.

- *ePrivacy Directive and its proposed revision*

The proposed measures in Options B to E would include service providers that offer interpersonal electronic communications services and hence are subject to the provisions of the ePrivacy Directive and its proposed revision currently in negotiations. These measures presuppose the need for a derogation from the relevant provisions of that Directive (akin to the Interim Regulation already in force, but then without limit in time and covering, where relevant, also mandatory detection) and would provide specific conditions for the processing of certain types of data otherwise subject to the ePrivacy framework.

- *e-Commerce Directive*

The e-Commerce Directive prohibits Member States from imposing general monitoring obligations and from actively seeking facts or circumstances indicating illegal activity. The

DSA proposal confirms and restates this principle. The legislative proposal will include the necessary elements (including on objectives pursued, type of material, scope and nature of obligation, risk-based approach, limitation in time, assistance, safeguard and supervision) to ensure respect for the appropriate balancing of fundamental rights enshrined in this principle.

- *The proposed Digital Services Act*

Options B to E would build on the DSA's horizontal framework, setting out a more specific framework where needed for the particular case of combating CSA online, akin to sectoral legislation such as the Terrorist Content Online Regulation, relying on the baseline provided by the DSA where possible. As regards the prohibition of general monitoring and active fact-finding obligations (which is also provided for in the DSA proposal), see the above point on the eCommerce Directive.

- *Victims' Rights Directive*

Options A to E would strengthen – to an increasing extent – support to victims, in coherence with the Victims' Rights Directive as a horizontal instrument to improve victims' access to their rights. Options B to E would establish an EU Centre that would carry out, in addition to its principal tasks, certain tasks relating to prevention and assistance to victims, and would thus ensure greater facilitation of the cooperation with Member States and exchange of best practices, with regards to CSA victims. These options would also include measures to enhance the practical implementation of victims' rights to stop images and videos related to their abuse from circulating and hence give fuller impact to these rights.

Sector-specific legislation

- *CSA Directive*

The CSA Directive is a criminal law instrument, which none of the policy options considered would contradict. In fact, strengthening prevention, detection, reporting and victim support should positively influence the implementation of the Directive and cooperation between Member States.

- *Interim Regulation*

Option A would contribute through non-legislative measures to the voluntary efforts by online service providers under the Interim Regulation. Once the Interim Regulation expires on 3 August 2024, there would not be another legal instrument to replace it under this option.

Options B to E specify the conditions for voluntary detection, reporting and removal of CSA online and options C to E define obligations to detect CSA online. These options would provide a long-term regulatory framework that would build on the Interim Regulation (including its safeguards) and replace it.

- *Europol Regulation and its proposed revision*

Under options B to E, the EU Centre would be the recipient of the reports by service providers, will review them and eventually forwarded them to Europol for action. The processing and follow up of these reports by Europol would be governed by the Europol Regulation and then by its proposed revision. This proposed revision could strengthen the fight against CSA by e.g. effectively supporting Member States and their investigations with the analysis of large and complex datasets, addressing the big data challenge for law enforcement authorities. The Centre would contribute to ensure that the data that Europol services from service providers is actionable and usable for law enforcement authorities.

b) Coordination

- *EU level cooperation in investigations, prevention and assistance to victims*

Option A would facilitate to a limited extent cooperation in investigations, prevention and assistance to victims. This cooperation would be higher in the case of options B to E, thanks to the Centre, whose main purpose is to serve as a **facilitator** of efforts, including thorough increased cooperation in those three areas.

- *Multi-stakeholder cooperation at EU and global level*

Likewise, the Centre in options B to E would also facilitate multi-stakeholder cooperation at EU and global level, in particular by facilitating the exchange of best practices on prevention and assistance to victims.

Under options C to E, the obligations to detect CSA online would likely entail an increase in the number of reports in other jurisdictions, in particular the US. While these obligations would apply only to services offered in the EU, the cross-border nature of these crimes means that a significant number of reports will relate to activities which involve third countries (for example, a report of grooming where the suspect and victim are located in different jurisdictions). In addition, while technology to detect known CSAM is widely used by many providers, technologies for the detection of new CSAM and grooming are less widely-deployed. It is expected that obligations to use such technologies in the EU could lead to increased voluntary use of the same technologies in relation to third countries, particularly as their distribution would be facilitated by the centre to the relevant service providers offering their services in the EU (without imposing restrictions on use outside of the EU). The amount of CSAM detected globally would increase, and with it the possibilities to stop its circulation and prevent future abuses globally. The number of cross-border investigations and opportunities to cooperate internationally, within the EU and globally, would increase.

Box 21: risk of duplication of reporting to the EU Centre and NCMEC

Mandatory reporting of CSA online to the EU Centre could lead to duplicating obligations for US service providers to make reports both in the EU and in the US. Some stakeholders have suggested that, in order to avoid duplication of reporting, any obligation to report to an EU organisation should include an exemption for providers that already report to NCMEC. This exemption would have several negative consequences, notably:

- delays for European law enforcement authorities to receive the reports due to exclusive reporting to NCMEC and losing the ability to 'de-conflict' reports by discovering reports having the same or similar content by cross-referencing the reports received by NCMEC, the EU Centre and Europol;
- unequal conditions and safeguards relating to the reporting obligations, since those existing under US law and those to be established under the present initiative would differ; and
- the processing of large volumes of EU user data outside the EU, by an entity not bound by EU law.

Such an exemption would therefore have a negative impact on the protection of fundamental rights, another specific objective of the initiative, and potentially lead to negative effects on international relations. Where possible within the limits sets by the applicable legislation, the implementation of technical solutions to report could help ensure that there is no confusion or unnecessary duplication of reports received by law enforcement agencies in the EU (e.g. by simply adding a tag in the report indicating whether it has been sent to the US or the EU).

In any event, the obligations under EU law would remain limited to the relevant services offered in the EU. Therefore, those obligations would not extend to services offered elsewhere.

c) Funding

The Centre under options B to E would serve as a **facilitator** of efforts, possibly including thorough signposting funding opportunities at EU and national level and maintaining an overview of past projects, to avoid duplication of efforts and ensure the most effective use of funds. The Centre would also facilitate research on prevention and assistance to victims, possibly by managing its own research funding.

7.1.6. Proportionality

The five options follow the same principle of proportionality and necessity of an intervention at EU level: a fragmented approach across Member States is unable to ensure an appropriate level of protection to children across the Union, and the protection of fundamental rights of all online users. Whereas the level of effectiveness of the options is different, as they contain different measures and impose different obligations, all are proportionate, as none goes beyond what is a necessary intervention at EU level to achieve the specific objectives. In addition, the conditions of application and safeguards for each option are conceived according to match its level of intrusion.

7.2. Quantitative comparison

7.2.1. Overall costs

For the purpose of comparing the options and calculating overall costs, the total combined cost (not discounted) to service providers and public authorities over a period of 10 years (2021-2030) was considered. The cost over this period was obtained by combining the one-off costs of the relevant policy measures with the sum of the annual costs for ten years. These include all costs directly arising from the measures as described in Annex 4, section 3, such as costs for the establishment of the Centre, implementation of technical measures for detection and reporting of CSA online, development of tools, processing of reports, etc.

The one-off and annual costs associated with each policy option are set out in detail in Annex 4, section 4.

Over 10 years, the total of costs per option is the following:

Table 7: comparative costs of the policy options over 10 years (EUR billions)

	A	B	C	D	E
Total costs (EUR billions)	0.17	0.71	10.65	18.92	24.49

7.2.1. Overall benefits

The table below compares the estimated costs and benefits for the different options over ten years:

Table 8: comparative quantitative assessment of the policy options over 10 years (EUR billions)

	A	B	C	D	E
Overall costs	0.17	0.71	10.65	18.92	24.49
Overall benefits	0.97	2.24	28.00	33.87	34.48
Total (net benefits)	**0,81**	**1,52**	**17,35**	**14,95**	**9,99**

The overall benefits (not discounted) assumes a decrease of 25% in the total CSA costs per year. Annex 4 contains a sensitive analysis on the % decrease in total CSA costs to determine the minimum values at which each of the options would produce net quantitative benefits. Table 9 summarises these results:

Table 9: minimum % decrease in total annual CSA costs to generate net benefits in each policy option

A	0,13%
B	0,6%
C	8%
D	14%
E	18%

8. PREFERRED OPTION

On the basis of the assessment, the **preferred option is E**, which notably includes:

- the creation of the **EU Centre** in the form of a **decentralised EU agency**;
- **mandatory detection** of **known and new CSAM and grooming, based on detection orders**;
- an **obligation to report** possible CSA online to the EU Centre; and
- an **obligation to remove** CSA online, once confirmed as illegal.

The preferred option is the one that most effectively address the problem drivers as well as the associated costs and impacts in other areas such as fundamental rights, and achieves the objectives of the initiative. While some of the other options that are more economically convenient, the degree to which they would be less effective outweighs financial savings. However, it should be noted that the report aims to make a recommendation for the preferred option, and the final policy choice is left to the political decision maker.

The annual estimated costs of Option E, based upon the analysis in Section 6.2.1, are summarised in Table 10, below. As noted in that section, the costs were estimated primarily for the purposes of comparing the policy options. The estimates provide an idea of the order of magnitude of costs and benefits and therefore should not be taken as exact forecasts.

Table 10: annual costs of the preferred option E (EUR millions)

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0,4	€0,2	€3,5	€2,8
3	€5,0	€0,0	€25,7	€0,0
4[214]	€0.0	€0,0	€11,1	€6,9
5	€0,0	€20,4	€3,3	€1,7
6	€0,0	€352,2	€503,6	€459,4
7	€0,0	€604,4	€250,1	€520,5
8	€0,0	€618,0	€28,2	€471,9
Total	**€5,4**	**€1.595,3**	**€825,6**	**€1.463,3**

8.1. Main advantages

Effectively achieves the general and specific objectives: Option E would bring strong improvements in **identification, protection and support of victims** of child sexual abuse, would ensure **effective prevention** and would **facilitate investigations**. In particular:

- The **Centre** would **facilitate** and support coordination of efforts of all relevant actors**,** which would in turn reduce the **proliferation and effects** of CSA. This includes carrying out certain tasks entailing **support for victims**, which could rely on the Centre to **assist them in requesting removal of known CSAM** depicting them.
    - ⇨ The **Centre** would help boost efforts (and their effectiveness) in the **overall** fight against child sexual abuse in the EU, focusing on CSA **online** but leading in that manner **also to concrete results offline.**
- The **legislative provisions**, in particular the **obligations to detect known and new CSAM and grooming**, combined with the support of the Centre on detection, reporting and removal efforts, would ensure the effective detection, removal and reporting of online CSA where they are currently missing.
- The **safeguards** to be included in the **legislation**, combined with the **Centre**'s support to help ensure **transparency and accountability** in the detection, reporting and removal by online service providers, would improve overall **legal certainty, protection of fundamental rights, transparency and accountability**.
    - ⇨ The **Centre** is a **fundamental component of the legislation**. It serves as a **key safeguard** in the detection, reporting and removal process**.**
- **The establishment** of clear and uniform legal requirements at EU level, to the exclusion of diverging national rules on the issues covered, would **improve the functioning of the internal market** to the benefit of both providers and users. The present initiative will join other sector-specific initiatives like the terrorist content online regulation and the Copyright directives in providing more specific and stricter rules to address certain types of illegal content and activities.

Respects subsidiarity and proportionality

Subsidiarity: option E offers the **highest added value of EU action** described in section 3.3. In particular, it **reduces legal fragmentation** through the EU level legislation, and through

[214] Adjusted to exclude one-off costs of measure 4 on voluntary detection, which would be covered by those of measures 6, 7 and 8 on mandatory detection.

the **Centre** it facilitates Member States' action, enables the exchange of best practices and reduces dependence and increases cooperation with third countries.

Proportionality: option E does not go beyond what is necessary to achieve the general and specific objectives identified for EU intervention. In particular, the necessary measures would be taken to ensure **respect for the fair balance principle underlying the prohibition to impose general monitoring or active fact-finding obligations.** Also, the legislation in this option would have the legitimate purpose of more effectively tackling CSA online, including better protection of victims through more effective detection, reporting and removal, with the necessary **limits and safeguards** to ensure a fair balance and proportionality.

Protects fundamental rights: All options have to strike a fair balance between different fundamental rights. Of the available options, option E protects **fundamental rights** to human dignity and to the integrity of the person, the prohibition of inhuman or degrading treatment, and the **rights of the child**, among others, by boosting efforts to better prevent and protect children from sexual abuse and better support victims. In addition, option E also limits the impact on **fundamental rights of users** of the online services concerned, notably to the respect for private and family life, protection of personal data, and freedom of expression, among others, to the strictly necessary minimum, through the necessary **limits and safeguards** in the legislation, including the functions of the **Centre**. These conditions also ensure increasing standards over time as technology evolves, by ensuring that tools correspond to the state of the art. In particular, given the importance of the objective and the interference with the rights of users inherent in proactive detection, the decision on the limits and safeguards to detect CSA should be the legislator's, not the service provider's.

8.2. Main disadvantages

Implies more extensive implementation efforts and higher costs: the implementation efforts of the legislation imposing such obligations on service providers, and setting up the Centre, would likely require more time and effort and hence be more expensive than a less comprehensive instrument. The establishment of the Centre as a decentralised EU **agency** requires **higher initial and running costs** than if the Centre were established as part of an existing entity. **Service providers** will incur costs to comply with the legislation. **Public authorities** will also incur increased costs, notably to deal with the likely increase in child sexual abuse cases detected.

8.3. Trade-Offs

Better detection, reporting, prevention and victims' assistance imply new efforts and costs
To achieve the general objective, the initiative proposes a **new legislative framework** for online service providers, which includes the creation of a **Centre** to facilitate **existing and new efforts**. Whereas the proposal would seek to **minimise disruption**, building as much as possible on ongoing efforts, it is clear that **additional human, technical, and financial efforts are required** to improve prevention, support of victims, and the detection, reporting and removal mechanisms. The new efforts will likely lead to an **increase of detected cases**, at least in the near future, before prevention efforts decrease the prevalence of the crimes.

Although option C would have the highest net economic benefit, the overall benefits for option C are still expected to be significantly lower than under option E. In addition, as set out in the qualitative comparison in section 7.1, option E appears as the best one in terms of overall qualitative scores, driven by higher effectiveness. Specifically, the detection of grooming included in option E adds a significant prevention aspect to this option, which

determines its highest score on effectiveness compared to the other options. Child sexual abuse material depicts scenes of crimes **already committed**, and, whereas its detection contains an important prevention aspect as described in box 1, the detection of grooming focuses on **preventing** crimes such as hands-on abuse or sexual extortion. This avoids the short-term and long-term consequences for victims, all of which cannot be numerically quantified.

Improved detection and reporting imply a comprehensive set of conditions and safeguards

Mandatory detection of known and new CSAM and grooming has an **impact on fundamental rights of all users**, in particular considering that online service providers would be processing **personal data**, in both **public and non-public** (interpersonal) communications. This is a **sensitive issue** that requires appropriate consideration to ensure that the **conditions and safeguards** put in place protect the fundamental rights of all users. Likewise, the relationship with other acts of EU law (especially e-Commerce Directive/DSA and the EU data protection acquis) is a point of particular attention. This will likely require **substantial time to prepare** (until the legislative proposal becomes EU law) **and implement**.

8.4. Application of the 'one in, one out' approach

The 'one in, one out' approach refers to the principle whereby each legislative proposal creating new burdens should relieve people and businesses of an equivalent existing burden at EU level in the same policy area.

The preferred option for this initiative entails direct **adjustment costs** for businesses (service providers) and administrations. These are costs of complying with and adjusting their operating processes to the requirements of the proposed legislation. Examples of adjustment costs for service providers include the human and technical resources to comply with the obligations to detect, report and remove CSA online. The preferred option will also generate direct adjustment costs for administrations (notably law enforcement), due to the increased workload to deal with the increase of CSA reports.

The preferred option also creates **administrative costs** for service providers and administrations. These are costs that result of administrative activities performed to comply with the administrative obligations included in the proposed legislation. They concern costs for providing information, notably on the preparation of annual transparency reports.

On the other hand, the proposed legislation will **replace one existing legislative instrument**: the Interim Regulation. This would generate savings on administrative costs for service providers and public authorities. See Annexes 3 and 4 for additional details.

Furthermore, the initiative is expected to generate significant **cost savings to society**, derived from a reduction in CSA crimes (e.g. reduction in productivity losses, see section 6.2.2).

Also, the **EU Centre** will **facilitate** action of Member States and service providers in preventing and combating CSA, and support victims. This will generate **cost savings**, by, e.g. helping **avoid duplication of efforts** and facilitating a more effective and efficient use of resources.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

The actual impacts of the preferred option, i.e. the actual progress in the fight against child sexual abuse offline and online, will be monitored and evaluated against the three **specific objectives**. The **indicators** would **build on** those of the **Interim Regulation** to **minimise disruption** and costs.

The specific objectives basically aim to improve **what is being done** (specific objectives 1 and 3), and **how it is being done** (specific objective 2). The specific objectives have corresponding **operational objectives,** which would be monitored using various **data sources** through **indicators**, which different actors would be **responsible** for collecting and sharing.

Table 11: monitoring of general, specific and operational objectives

General objective	**Specific objectives**	**Operational objectives**	**Indicators - *data sources***	**Who is responsible for collection - *output***	
Improve the functioning of the Internal Market by introducing **clear, uniform and balanced EU rules** to **prevent** and **combat** child sexual abuse	Improve the **what**": 1. Ensure the effective detection, removal and reporting of online child sexual abuse where they are currently missing 3. Reduce the proliferation and effects of child sexual abuse through harmonisation of rules and increased coordination of efforts	Prevention: • reduce CSA prevalence • reduce **duplication and blind spots** of Member States' efforts Assistance to victims: • provide the required assistance • reduce **duplication and blind spots** of Member States' efforts Detection and reporting: • detect, report and remove **all CSAM, known and new**, distributed online • increase detection and reporting of **grooming**	Prevention: • **prevalence rate** in Member States - *surveys* • **number, type and evaluation results** (including best practices and lessons learned) of prevention programmes - *public authorities in Member States* Assistance to victims: • **number** of victims assisted and **level of satisfaction** of victims with the assistance provided - *surveys to survivors* • **number, type and evaluation results** (including best practices and lessons learned) of victims assistance programmes - *public authorities in Member States* Detection and reporting: • number of reports by Member State, source (company, hotline, public), type of online service, and type of CSA online (i.e. number of images and videos, including unique/not unique and known/new, and grooming) – *EU Centre* • **feedback on reports**: if no action taken **why**, if action taken **outcome** (**number of victims identified/rescued, number of offenders convicted**, and (anonymised and short) description of the case) – *public authorities in Member States*	**EU Centre** – ***annual report*** to the public and the Commission (extended version)	**Commission** – ***implementation report*** every **5 years** – ***evaluation*** every **5 years**, using as sources the annual reports from the EU Centre and from providers, among others
	Improve the **how**": 2. Improve legal certainty, transparency and accountability and ensure protection of fundamental rights	• **Make clear** all relevant aspects of the **detection, reporting and removal process** by online service providers	• **technologies used,** including **error rates**, measures to limit the error rates, and, if the technologies are new, **measures taken to comply with written advice** of competent authorities – *service providers*	**Service providers** – ***annual report*** to supervisory authorities, the EU Centre and the Commission	

Annexes

ANNEX 1: PROCEDURAL INFORMATION

- **Lead DG, Decide Planning/CWP references**

This Staff Working Paper was prepared by the Directorate-General for Migration and Home Affairs (**HOME**).

The Decide reference of this initiative is **PLAN/2020/8915**.

This initiative appears in the 2021 **Commission Work Programme** under action 35, 'Follow-up to the EU security strategy': Legislation to effectively tackle child sexual abuse online (legislative, incl. impact assessment, Article 114 TFEU, Q2 2021).

- **Organisation and timing**

Organisation

The **Security Union Inter-Service Group** (ISG), chaired by the Secretary-General of the Commission, was consulted **at all stages** of the process to prepare the impact assessment, including the inception impact assessment, consultation strategy, questionnaire for the public consultation and the various drafts of the impact assessment.

The ISG included the following Commission services: DG EMPL (DG Employment, Social Affairs and Inclusion), DG GROW (DG Internal Market, Industry, Entrepreneurship and SME), DG RTD (DG Research and Innovation), SJ (Legal Service), DG SANTE (DG for Health and Food Safety), DG TRADE, DG CNECT (DG Communications Networks, Content and Technology); DG EAC (DG Education and Culture); DG JUST (DG Justice and Consumers); DG NEAR (DG Neighbourhood and Enlargement Negotiations); ESTAT (Eurostat); DG DEFIS (DG Defence Industry and Space); DIGIT (Informatics); DG ECHO (DG Humanitarian Aid and Civil Protection); DG ENER (DG Energy); DG ENV (DG Environment); DG FISMA (DG Financial Stability, Financial Services and Capital Markets Union); FPI (Service for Foreign Policy Instruments); IDEA (Inspire, Debate, Engage and Accelerate Action); JRC (Joint Research Centre); DG MARE (DG Maritime Affairs and Fisheries); DG MOVE (Mobility and Transport); DG TAXUD (Taxation and Customs Union); DG REFORM (DG Structural Reform Support); OLAF (European Anti-Fraud Office); DG INTPA (DG International Partnerships); CERT-EU (Computer Emergency Response Team for the EU Institutions, bodies and agencies); DG BUDG (DG Budget) and DG REGIO (DG Regional Policy). It also included the EEAS (European External Action Service).

The **last meeting of the ISG**, chaired by the Secretariat-General, was held on **17 January 2022**.

Timing - chronology of the IA

This initiative was first announced in the **July 2020 EU strategy for a more effective fight against child sexual abuse**[215], where the Commission notably committed to:

[215] EU strategy for a more effective fight against child sexual abuse, COM(2020)607 final.

- propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect child sexual abuse on their services and to report any such abuse to relevant public authorities; and
- work towards the possible creation of a European centre to prevent and counter child sexual abuse to enable a comprehensive and effective EU response against child sexual abuse online and offline, based on a thorough study and impact assessment.

The strategy also announced the proposal for the necessary legislation to ensure that providers of electronic communications services could continue their current voluntary practices to detect in their systems child sexual abuse after December 2020. The Commission proposed this legislation ("**the Interim Regulation**") in September 2020[216], and on 29 April 2021 there was a political agreement between the European Parliament and the Council on the text, which was then adopted by the two institutions in July 2020[217].

The present initiative, once adopted, would replace this Interim Regulation, among other purposes.

The Commission published an **inception impact assessment**[218] on 3 December 2020. The feedback period ran until 30 December 2020. A **public consultation** was launched on 11 February 2021, and stakeholders and citizens had the opportunity to express their views through an online questionnaire until 15 April 2021.

While work on various aspects of the measures considered has been going on for several years, the drafting of the impact assessment itself started in October 2020 and continued until February 2022, after incorporating the feedback from the Regulatory Scrutiny Board.

- **Consultation of the Regulatory Scrutiny Board**

The Regulatory Scrutiny Board received the draft version of the present impact assessment report on 25 May 2021. It issued an impact assessment quality checklist on 11 June 2021.

The Regulatory Scrutiny Board issued a first negative opinion on 17 June 2021 on the draft impact assessment report. To address the feedback given by the Regulatory Scrutiny Board, the following changes were made in the report and its annexes:

---

216 Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse of 10 September 2020, COM/2020/568 final.

217 Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, OJ L 274, 30.7.2021, p. 41–51

218 Inception Impact Assessment, 3 December 2020.

Board's comments	How they were incorporated in the report and annexes
1. The internal market dimension and the necessity for EU action in the area of prevention and victim support is not always clear	Changes were made throughout the report, in particular in sections 1, 2 and 3, in particular to highlight that the central focus of the legislation to is to harmonise rules for online service providers
2. The report does not fully describe all the available policy choices and leaves a number of questions open. It does not discuss in a transparent and balanced manner the alternative implementation forms for a European centre	Addition of a dedicated section (5.2.2.1) discussing the implementation choices for the EU centre.
3. The report does not clearly establish how safeguards will ensure fundamental rights, in particular regarding technologies to detect CSA in encrypted communications	Section 5 in particular was reviewed to detail the safeguards that could apply (see description of options). Section 6 was updated accordingly, including the analysis on fundamental rights.
4. The comparison of policy options does not comply with the standard assessment criteria and is not based on a clear and consistent ranking methodology	Section 7 was reviewed to notably include coherence as a comparison criterion, and a revised ranking methodology.

The Regulatory Scrutiny Board issued a second and final positive opinion on 17 June 2021 on the draft impact assessment report. To address the feedback given by the Regulatory Scrutiny Board, the following changes were made in the report and its annexes:

Board's comments	How they were incorporated in the report and annexes
1. The role of the EU centre and associated costs are not sufficiently described. The implementation options for the EU centre are not presented in a sufficiently open, complete and balanced manner	Additional descriptions of the role of the Centre on prevention and assistance to victims added to Section 5.2.1. Additional clarifications on the role of the Centre added in sections 5.2.2., 5.2.3., 5.2.4., and 5.2.5. Section 5.2.2. was restructured to present and analyse the options in an open, complete and balanced manner.
2. The report is not sufficiently clear on how the options that include the detection of new child sexual abuse material or grooming would respect the prohibition of general monitoring obligations	Further clarifications added in sections 5.2. and 5.2.3.
3. The efficiency and proportionality of the preferred option is not sufficiently demonstrated	Further clarifications added in section 8.3., in particular in relation to the importance and added value of grooming detection.
4. The scope and quantification of the cost and cost savings for the 'one in, one out' purposes are not clear	Clarifications added in section 8.4., in particular in relation to the costs and savings included in the quantification for one in, one out purposes.

- **Evidence, sources and quality**

When drafting the impact assessment report and annexes, particular attention has been given to properly reference all the **sources and** review their **quality**.

The calculations of **costs and benefits** were limited by the **lack of data**. The Commission made significant efforts to collect data, or at least estimates, from public authorities and service providers through targeted surveys. Where this information was not available, assumptions were made in the model to calculate costs, which were discussed with experts from Member States and service providers.

The **evidence base** includes in particular:

- **external studies prepared at the request of the European Commission**

- ICF et al. Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues, 2021
- ICF et al. Study on framework of best practices to tackle child sexual abuse material online, 2020.
- ICF, Grimaldi, Overview of the legal framework of notice-and-action procedures in Member States, SMART 2016/0039, 2018.

- **selective list of relevant case law:**

Court of Justice of the European Union:

- C-236/08 to C-238/08, Google France SARL and Google Inc. v Louis Vuitton Malletier SA, ECLI:EU:C:2010:159.C380/03.
- C-324/09, L'Oréal v eBay, ECLI:EU:C:2011:474.
- C-70/10, Scarlet Extended SA v SABAM, ECLI:EU:C:2011:771.
- C-360/10, SABAM v Netlog NV, ECLI:EU:C:2012:85.
- C-314/12, UPC Telekabel Wien, EU:C:2014:192.
- C-484/14, McFadden, ECLI:EU:C:2016:689.
- C-18/18, Glawischnig-Piesczek v Facebook Ireland, ECLI:EU:C:2019:821.

European Court of Human Rights:

- Application no. 2872/02, K.U. v. Finland, judgment of 2 December 2008.
- Application no. 5786/08, Söderman v. Sweden, judgment of 12 November 2013.
- Application no. 24683/14, ROJ TV A/S against Denmark, decision of 24 May 2018.
- Application no. 56867/15, Buturugă against Romania, judgment of 11 February 2020.

Decisions of national courts:

- Antwerp Civil Court, A&M, judgment n.2010/5-6 of 3 December 2009.
- OLG Karlsruhe, judgment 6 U 2/15 of 14 December 2016.
- Rome Court of Appeal, RTI v TMFT Enterprises LLC, judgment 8437/2016 of 27 April 2016.
- Austrian Supreme Court, (Oberster Gerichtshof), decision 6 Ob 178/04a of 21 December 2006.
- Turin Court of First Instance, Delta TV v Google and YouTube, judgment No 1928, RG 38113/2013 of 7 April 2017.

- **Selective Bibliography**

- Carnegie Endowment for International Peace, *Moving the Encryption Policy Conversation Forward,* Encryption Working Group, September 2019.
- De Jong, R., Child Sexual Abuse and Family Outcomes, *Crime Science,* 2 November 2015.

- Di Roia, R., Beslay, L., 'Fighting child sexual abuse-Prevention policies for offenders, *Publication Office of the EU,* 3 October 2018.
- Fargo, J., Pathways to Adult Sexual Revictimization: Direct and Indirect Behavioural Risk Factors across the Lifespan, *Journal of Interpersonal Violence,* 16 October 2008.
- Farid, H., Reining in online abuses, *Technology and Innovation,* Vol.19, p. 593-599, 2018.
- Floridi, L., & Taddeo, M. (2017). The Responsibilities of Online Service Providers, 2017.
- Gewirtz-Meydan, A., Finkelhor, D., Sexual Abuse and Assault in a Large National Sample of Children and Adolescents, *Child Maltreatment,* 16 September 2019.
- Kuhle, L., et al., Child Sexual Abuse and the Use of Child Sexual Abuse Images, 9 March 2021.
- Letourneau, E., The Economic Burden of Child Sexual Abuse in the United States, *Child Abuse & Neglect*, Vol. 79, May 2018.
- Madiega, T. (2020). Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act. *European Parliamentary Research Service,* PE 649.404, May 2020.
- Martin E, Silverstone P: How much child sexual abuse is "below the surface", and can we help adults identify it early, *Front Psychiatry,* May 2013.
- Noemí Pereda et al., 'The prevalence of child sexual abuse in community and student samples: A meta-analysis', *Clinical Psychology Review*, Vol. 29, Issue 4 (2009).
- Rosenzweig, P. (2020). The Law and Policy of Client-Side Scanning, *Lawfare*, 20 August 2020.
- Ruzicka, A., Assini-Meytin, L., Schaeffer, C., Bradshaw, C., & Letourneau, E., Responsible Behavior with Younger Children: Examining the Feasibility of a Classroom-Based Program to Prevent Child Sexual Abuse Perpetration by Adolescents, *Journal of Child Sexual Abuse,* 8 February 2021.
- Scherrer, A., Ballegooij, W., Combating sexual abuse of children Directive 2011/93/EU, European Implementation Assessment, *European Parliamentary Research Service,* PE 598.614, April 2017.
- Schwemer, S.F. (2018). On domain registries and unlawful website content. *International Journal of Law and Information Technology,* Vol. 26, Issue 4, 12 October 2018.
- Sluijs, J. et al. (2012). Cloud Computing in the EU Policy Sphere, 2011.

- Smith M. (2020), Enforcement and cooperation between Member States - E-Commerce and the future Digital Services Act, Study for IMCO committee, PE 648.780, April 2020.
- Stalla-Bourdillon, S. (2017). Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well. In The Responsibilities of Online Service Providers, 1 July 2016.
- Truyens, M., & van Eecke, P. (2016), Liability of Domain Name Registries: Don't Shoot the Messenger, *Computer Law & Security Review*, Vol.32, Issue 2, 19 January 2016.
- Urban, J., et al., Notice and Takedown in Everyday Practice, *UC Berkeley Public Law Research Paper No.2755628,* 22 March 2017.
- Van Hoboken, J., et al., Hosting intermediary services and illegal content online: An analysis of the scope of Article 14 ECD in light of developments in the online service landscape, final report prepared for the European Commission, *Publications Office of the EU*, 29 January 2019.
- Wagner B., Rozgonyi K. et al., Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act, January 2020.
- Wilman, F., The responsibility of online intermediaries for illegal user content in the EU and in the US, 20 November 2020.

- **Related Impact Assessments**

Impact Assessment accompanying the Proposal on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, SWD(2020) 348 final, 15 December 2020.

Impact Assessment accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, SWD(2020) 543 final, 9 December 2020.

Targeted subsitute Impact Assessment on the Commission proposal on the temporary derogation from the e-privacy Directive for the purpose of fighting online child sexual abuse, *European Parliamentary Research Service,* PE 662.598, February 2021.

Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, SWD(2018) 408 final, 12 September 2018.

Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal

representatives for the purpose of gathering evidence in criminal proceeding, SWD(2018) 118 final, 17 April 2018.

Additional external expertise was gathered through the stakeholder consultation, as explained in detail in Annex 2.

ANNEX 2: STAKEHOLDER CONSULTATION

This annex is the synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

1) Consultation strategy

In order to ensure that the general public interest of the EU is properly considered in the Commission's approach to the fight against child sexual abuse, the Commission has consulted as widely as possible. The consultation aimed to enable an evidence-based preparation of the future Commission initiative for a more effective fight against child sexual abuse with the help of stakeholders and had four main objectives:

- to identify current best practice, as well as challenges and gaps, and the relevant needs of all stakeholders;
- to identify ways forward that would best address those needs;
- to ensure that stakeholders (including citizens and those who would be directly affected by this initiative), can provide their views and input on the possible options for the way forward; and
- to improve the overall evidence base underpinning the initiative.

To do this, the Commission services identified relevant stakeholders and consulted them throughout the development of its draft proposal. The Commission services sought views from a wide range of subject matter experts, service providers, business associations, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to the issue of child sexual abuse and possible initiatives to prevent and combat it. These included in particular the responsibilities of relevant online service providers and possible requirements to detect and report child sexual abuse online and to report that material to public authorities, as well as the possible creation of a European centre to prevent and counter child sexual abuse.

During the consultation process, the Commission services applied a variety of methods and forms of consultation. They included:

- the consultation on the Inception Impact Assessment and the Open Public Consultation, which sought views from all interested parties;
- targeted stakeholder consultation by way of dedicated questionnaires;
- a series of workshops, conferences, expert groups, as well as bilateral meetings;
- inviting position papers and analytical papers from organizations, industry representatives, civil society and academia.

Taking into account the technicalities and specificities of the subject, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

2) The consultation was structured as follows:

1. **Who** – stakeholders consulted:
   - citizens;
   - service providers:

- individual companies;
- professional and business associations;
- public authorities from Member States and relevant non-EU countries:
- Ministry of Justice officials;
- Ministry of Interior officials;
- law enforcement representatives;
- legal practitioners (lawyers, prosecutors, judges);
- non-governmental organisations (NGOs);
- inter-governmental organisations (IGOs);
- EU institutions and agencies; and
- academia.

2. **How** – methods and tools used:

Surveys:

- **Open public consultations:**
  - Survey, open to feedback from **any interested party**, from 11 February 2021 to 15 April 2021; included a link to the Commission website on the fight against child sexual abuse[219] to provide further information and context.
  - **Consultation on the Inception Impact Assessment**, open to feedback from any interested party from 2 December to 30 December 2020.
- **Targeted** surveys:
  - Survey for **law enforcement authorities** in Member States to collect information regarding the origin, quality and use of reports of child sexual abuse online that law enforcement authorities receive.
  - Survey for **law enforcement authorities** in Member States to collect information regarding the costs associated with reports of child sexual abuse online received by law enforcement authorities (LEAs); how the quality of reports can be improved; and the impact of encryption on investigations.

Meetings[220]:

- Expert group meetings and bilateral meetings organised by the Commission;
- **Participation in** conferences and workshops organised by third parties.

In total, the dedicated **consultation activities** lasted **two years**, from **February 2020 to January 2022.**

The consultation was designed to follow the same logical sequence of the impact assessment, starting with the problem definition and allowing for a **gradual development** of the possible options and scenarios and their impacts, gradually increasing the number of stakeholders involved.

[219] EU strategy for a more effective fight against child sexual abuse, COM(2020)607 final.
[220] For a list of meetings and conferences, please see Section 3 below.

3. **What** – the consultation gathered feedback on the **problem definition, options and impacts** of these options, focused on the legislation to tackle child sexual abuse online effectively and the possible creation of a European centre to prevent and counter child sexual abuse. The diversity of perspectives proved valuable in supporting the Commission to ensure that its proposal addresses the needs, and takes account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary and indispensable data, facts and views, on the relevance, effectiveness, efficiency, coherence and EU added value of the proposal. Taking into consideration the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys as well as meetings via video conference. The table below summarises the structure of the consultation:

Table 1: consultation strategy for a more effective fight against child sexual abuse

		HOW					
		Surveys			Meetings		Conferences
		Open public consultation	Targeted survey 1	Targeted survey 2	Group	Bilateral	
WHO	Citizens	✓					✓
	Service providers	✓			✓	✓	✓
	Public authorities	✓	✓	✓	✓	✓	✓
	Practitioners	✓			✓	✓	✓
	NGOs	✓			✓	✓	✓
	IGOs	✓			✓	✓	✓
	EU institutions and agencies	✓			✓	✓	✓
	Academia	✓					✓
		Problem definition, options and impacts	Origin, quality and use of reports	Costs and quality of reports	Problem definition, options and impacts	Problem definition, options and impacts	Problem definition, options and impacts
		WHAT					

1. Consultation activities - summary of results

The following sections present a summary of the main results of the consultation activities.

Open public consultation

The purpose of the open public consultation was to gather evidence from citizens and stakeholders and it was part of the data collection activities that the related inception impact assessment announced in December 2020.

In total, 603 responses were submitted by a diverse group of stakeholders. It was addressed to a broad range of interested stakeholders, including public authorities, EU institutions and agencies, international organisations, private companies, professional and business associations, NGOs, academics and the general public.

Most feedback was received by citizens (77.93% from EU citizens, 1.84% from non-EU citizens), NGOs (10.37%), public authorities (3.51%), companies/businesses organizations (2.68%). This was followed by others (1.84%), business associations (0.84%), academic/research institutions (0.67%), as well as consumer organisations (0.33%). Additionally, around 45 position papers were received in the context of the open public consultation.

In terms of geographical distribution, most of the respondents are located in the EU, with a majority of contributions coming from Germany (45.15%), Ireland (16.22%), Belgium (4.18%) and Italy (4.18%). Internationally, the highest share of respondents that participated were from the UK (1.84%) and the US (2.51%)[221].

Summary

Its results as far as current practices and identified gaps, legislative solutions and the possible creation of a European centre to prevent and counter child sexual abuse are concerned, can be summarized as follows:

- The public consultation revealed broad support for EU action (among all categories of respondents).
- More specifically it revealed strong support for legal certainty for all stakeholders involved in the fight against child sexual abuse online (e.g. service providers, law enforcement and child protection organisations), for future-proved legislations, for effective cooperation between stakeholders and for additional coordination and support to EU level in the fight against child sexual abuse online and offline.

What is the current situation and where are the gaps

- 54.01% of the respondents state that the new legislation should aim to enable a swift takedown of child sexual abuse material after reporting.

[221] Countries with ≤15 submissions include Austria, Bulgaria, Croatia, Cyprus, Czechia, Finland, France, Greece, Hungary, Kosovo, Luxembourg, Netherlands, Poland, Portugal, Russia, Slovenia, Spain, Sweden, Switzerland, Thailand, Venezuela, Zimbabwe.

- The new legislation should further aim to reduce the number of instances of online grooming of children, based on the feedback provided by 49.67%.
- The areas of prevention and assistance to victims of child sexual abuse should be tackled in priority according to 61.54% and 65.05% of respondents, respectively.
- Law enforcement reflected on what are the main challenges they face in their work investigating child sexual abuse cases.
- 85.71% raised their concerns with regards to the increased number of child sexual abuse material in the last decade and the lack of resources (i.e. human, technical). It was followed by concerns about the underreporting of child sexual abuse cases and difficulties accessing evidence during investigation linked to the introduction of end-to-end encryption (38.1% and 47.62%). 14.29% referred to gaps in national or/and EU laws as one of the main issues.
- NGOs cooperate with law enforcement authorities in the fight against child sexual abuse, including by forwarding reports of child sexual abuse online received from the public or from service providers. 74.19% of the respondents see a need for improvement in the cooperation.
- NGOs also cooperate with services providers. Among other things, NGOs advise them on policies to fight child sexual abuse online and they also send notice-and-takedown requests to services providers. However, based on 72.58% of the replies, there is still room for improvement.
- 9.68% of the NGOs respondents consider that 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) while 56.45% considered that the current efforts put too much emphasis on the rights of all users and not enough emphasis on victims' rights.

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

- If online service providers were to be subject to a legal obligation to detect, remove and report child sexual abuse online in their services, most of the respondents to the public consultation agreed that services providers of social media (33.11%), image hosting (29.10%), web hosting (25.75%), message boards (23.75%), video streaming (23.58%) and online gaming (21.40%) should be subject to such legal obligation.
- In addition, 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 the following services should be included: social media (38.96%), image hosting (35.79%), video streaming (30.43%), message boards (29.10%), online gaming (26.76%).
- The respondents further reflected on the types of child sexual abuse online that the possible legislation should cover as well as on the best possible ways to achieve that as follows:

Which types of child sexual abuse online should the possible legislation cover and how?	Answers	Ratio
Known child sexual abuse material (i.e. material previously confirmed as constituting child sexual abuse)		
Mandatory detection and removal	161	26.92%
Mandatory reporting	72	12.04%
Voluntary detection and removal	85	14.21%
Voluntary reporting	45	7.53%
No need to cover this in the legislation	161	26.92%
New (unknown) child sexual abuse material		
Mandatory detection and removal	120	20.07%
Mandatory reporting	87	14.55%
Voluntary detection and removal	91	15.22%
Voluntary reporting	60	10.03%
No need to cover this in the legislation	169	28.26%
Online grooming		
Mandatory detection and removal	107	17.89%
Mandatory reporting	107	17.89%
Voluntary detection and removal	84	14.05%
Voluntary reporting	61	10.20%
No need to cover this in the legislation	162	27.09%
Live – streaming of child sexual abuse		
Mandatory detection and removal	156	26.09%
Mandatory reporting	96	16.05%
Voluntary detection and removal	77	12.88%
Voluntary reporting	46	7.69%
No need to cover this in the legislation	150	25.08%

- To be able to detect, remove and report child sexual abuse online, service providers need to carry out a series of actions. The respondents to the public

consultation were asked to share their views concerning the proportionality of the following action, when subject to all necessary safeguards:

Proportionality of actions subjected to all necessary safeguards				
	Fully agree	**Partially agree**	**Partially disagree**	**Disagree**
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	30.77%	16.89%	8.36%	32.94%
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	22.07%	15.05%	13.04%	37.96%
To check whether images or videos sent in a **private communication** are copies of **known** child sexual abuse material	14.38%	6.52%	6.69%	60.20%
To assess whether the images or videos sent in a **private communication** constitute **new** child sexual abuse material	14.38%	6.52%	6.69%	60.20%
To assess whether the images or videos sent in a **private communication** constitute **new** child sexual abuse material	12.21%	6.86%	6.02%	63.38%
To assess whether the contents of a **text based communication** constitute **grooming**	13.04%	9.70%	9.03%	54.85%
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	14.55%	11.54%	8.86%	50.33%

- 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. According to the submitted replies, the legislation should put in place safeguards to ensure the following:

Safeguards to ensure the respect of fundamental rights of all users, prevent abuses, and ensure proportionality				
	Fully agree	**Partially agree**	**Partially disagree**	**Disagree**
The tools used to detect, report and remove child sexual abuse online reduce the **error rate** to the maximum extent possible	41.30%	12.21%	4.18%	13.04%
The tools used to detect, report and remove child sexual abuse online are the **least privacy intrusive**	49.50%	9.20%	1.67%	13.04%
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	48.16%	8.36%	2.51%	12.71%
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	54.52%	4.85%	1.17%	11.20%
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	51.67%	7.86%	1.84%	10.70%
The online service provider conducts a **data protection impact assessment and consults the supervisory authority**, if necessary	38.13%	10.37%	3.85%	11.87%
Online service providers are subject to the oversight of a **supervisory body** to assess their compliance with legal requirements	36.12%	10.70%	5.18%	16.22%
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	38.13%	13.71%	6.19%	11.20%
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	32.61%	14.88%	8.53%	13.55%
A clear **complaint mechanism** is available to users	61.37%	5.69%	1.00%	6.19%
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	62.37%	4.68%	1.00%	4.85%

Providers should make clear in the **Terms and Conditions** that they are taking measures to detect, report and remove child sexual abuse online	60.87%	5.18%	1.51%	5.02%

- 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, 39.97% of the respondents believe that 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. While 27.09% opposed to this.
- Concerning **criminal sanctions**, opinions were almost equally divided between those in favour of such measure (35.96%) and those against (30.43%).
- It is further noted that there is no difference between the percentage for the respondents who would agree (32.61%) and that for those who would not (32.61%), that companies that **erroneously** detect, remove or report child sexual abuse online **in good faith** should not be subject to the relevant sanctions.
- Nearly half (41.64%) of the respondents participating in the survey stressed that 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. At the same time, 22.57% of the replies were in favour of such measure.

- **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
Obligatory to ensure transparency and accountability	**46.15%**	17.39%
Voluntary: an obligation would incur an additional burden on the online service providers, especially when they are small and medium enterprises	25.92%	**31.77%**
Evaluated by an independent entity	**47.99%**	11.37%
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	**50.17%**	11.54%

In addition, transparency reports should include the following information:

Transparency reports		
	Answers	**Ratio**
Number of reports of instances of child sexual abuse online reported by type of service	290	48.49%
Number of child sexual abuse material images and videos reported by type of service	269	44.98%%

Time required to take down child sexual abuse material after it has been flagged to/by the service provider	265	44.31%
Types of data processed to detect, report and remove child sexual abuse online	285	47.66%
Legal basis for the processing to detect, report and remove child sexual abuse online	279	46.66%
Whether data are shared with any third party and on which legal basis	317	53.01%
Number of complaints made by users through the available mechanisms and the outcome of those proceedings	291	48.66%
Number and ratio of false positives (an online event is mistakenly flagged as child sexual abuse online) of the different technologies used	319	53.34%
Measures applied to remove online child sexual abuse material in line with the online service provider's policy (e.g. number of accounts blocked)	276	46.15%
Policies on retention of data processed for the detecting, reporting and removal of child sexual abuse online and data protection safeguards applied	295	49.33%

- To measure the success of the possible legislation, a series of performance indicators should be monitored. In particular:
    - Number of reports of child sexual abuse online reported by company and type of service (33.78%);
    - Number of child sexual abuse material images and videos reported by company and type of service (32.78%);
    - Time required to take down child sexual abuse material after it has been flagged to/by the service provider (34.78%);
    - Number of children identified and rescued as a result of a report, by company and type of service (44.31%);
    - Number of perpetrators investigated and prosecuted as a result of a report, by company and type of service (44.31%);
    - Number of related user complaints as a result of a report, by company and type of service (33.28%).

- Views were particularly divided over (i) the legal obligation of online service providers that offer their services within the EU, even when the providers themselves are located outside the EU, and (ii) the legal obligation of online service providers who offer encrypted services to detect, remove and report child sexual abuse online in their services.

Possible European centre to prevent and counter child sexual abuse

- 44.65 % of the respondents 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.
- This could help to address existing challenges related to law enforcement action (up to 30% of the replies), preventive measures (up to 45%) as well as in the field of assistance to victims (up to 41%).

- Concerning relevant **functions to support law enforcement action** in the fight against child sexual abuse in the EU, survey respondents supported that possible Centre could:
    - Receive reports in relation to child sexual abuse to ensure the relevance of such reports, determine jurisdiction(s), and forward them to law enforcement for action (45.82%);
    - Maintain a single EU database of known child sexual abuse material to facilitate its detection in companies' systems (39.96%);
    - Coordinate and facilitate the takedown of child sexual abuse material identified through hotlines (43.98%);
    - Monitor the take down of child sexual abuse material by different stakeholders (38.96).

- In order to ensure **transparency and accountability regarding actions of service providers** to detect, report and remove child sexual abuse online in their services, the EU Centre should:
    - Ensure that the tools employed are not misused for purposes other than the fight against child sexual abuse (59.53%);
    - Ensure that the tools employed are sufficiently accurate (55.69%);
    - Ensure that online service providers implement robust technical and procedural safeguards (44.15%);
    - Draft model codes of conduct for service providers' measures to detect, report and remove child sexual abuse online (37.46%);
    - 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 (30.6%);
    - Receive complaints from users who feel that their content was mistakenly removed by a service provider (50%);
    - Publish aggregated statistics regarding the number and types of reports of child sexual abuse online received (46.49%).

- The EU centre would **support prevention efforts** in the fight against child sexual abuse in the EU:

- 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 (51%);
- Serve as a hub for connecting, developing and disseminating research and expertise, facilitating the communication and exchange of best practices between practitioners and researchers (54.85%);
- Help develop state-of-the-art research and knowledge, including better prevention-related data (51.17%);
- Provide input to policy makers at national and EU level on prevention gaps and possible solutions to address them (49%).

- In addition, the respondents reflected on the possible functions of the Centre which would be relevant to **support efforts to assist victims of child sexual abuse** in the EU:
  - Support implementation of EU law in relation to assistance to child victims of sexual abuse (56.35%);
  - Support the exchange of best practices on protection measures for victims (58.03%);
  - Carry out research and serve as a hub of expertise on assistance to victims of child sexual abuse (56.59%);
  - Support evidence-based policy on assistance and support to victims (58.03%);
  - Support victims in removing their images and videos to safeguard their privacy (57.36%);
  - Ensure that the perspective of victims is taken into account in policymaking at EU and national level (54.18%).

- With regards to the most appropriate type of organisation for the possible centre, 34.78 % of the respondents would welcome the creation of an EU body. A smaller percentage identified public- private partnerships (5.18%) and 20.90% non for profit organisations (20.90%) as the most appropriate types of organisation for the possible Centre.
- More than half of the respondents (53.51%) consider that the possible Centre should be funded directly from the Union budget, while almost 1 in 5 support the idea of mandatory levies on industry (18.73%) or voluntary contributions from industry(19.90%), and non for profit organisations(22.74%) as the most appropriate types of funding.

Problem description [current gaps and possible outcomes]

The majority of the public survey respondents, all categories included, acknowledged the online grooming of children as the most concerning type of child sexual abuse online which needs to be tackled in priority.

Public authorities

Practitioners from **law enforcement** and **other public authorities** stressed that the new legislation should reduce the number of instances of online grooming of children and enable a swift takedown of child sexual abuse material after reporting[222]. The respondents further expect the initiative to reduce the amount of unknown child sexual abuse material distributed in the open web[223] or via messaging applications[224] as well as to reduce the amount of sexual material self-generated sexual by children distributed online[225]. According to 52.38%, the new legislation should aim to ensure that child sexual abuse material stays down (i.e. that it is not redistributed online). In addition, 71.43% of the respondents highlighted the need to improve prevention as one of the main goals of the new legislation. It should further 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)[226], and be future-proof[227]. The new legislation could also serve to improve transparency and accountability of the measures to fight against child sexual abuse online (23.81% of the respondents).
Practitioners furthermore expressed concerns regarding the increased volume of child sexual abuse material detected online in the last decade and the insufficient human and technical resources to deal with it[228].

Companies

Online grooming is perceived as a challenge and should be tackled in priority according to 56.25% of the public survey respondents representing companies, who further identified the need to enable swift takedown of child sexual abuse material after reporting[229]. They further stressed that the new legislation should prioritise the following prevention and victim support outcomes: to 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)[230] as well as to ensure that legislation is future-proof. Improving prevention and assistance to victims of child sexual abuse was also identified as a key concern.18.75% stressed the need to enable a swift start and development of investigations, while (25% flagged that) it should also ensure a victim-centric approach in investigations, taking the best interests of the child as a primary consideration.

Non-governmental organisations

More than half of the respondents from non-governmental organisations stated that the current efforts to tackle child sexual abuse online place too much emphasis on the rights of all users and not enough emphasis on victims' rights[231]. 4.84% believe that the current efforts do not place enough emphasis on the rights of the users.

In their view, the new legislation should aim to reduce the number of instances of online grooming and to enable a swift takedown of child sexual abuse material after

---

222 80.95% (n=17) of the respondents from law enforcement or other public authorities.
223 71.43% (n=15) of the respondents for law enforcement or other public authorities.
224 71.43% (n=15) of the respondents for law enforcement or other public authorities.
225 66.67% (n=14) of respondents from law enforcement or other public authorities.
226 61.9% (n=13) of the respondents from law enforcement or other public authorities.
227 76.19% (n=16) of the respondents from law enforcement or other public authorities.
228 85.71% (n=18) of the respondents from law enforcement or other public authorities.
229 43.75% (n=7) of the respondents from companies.
230 56.25% (n=9) of the respondents from companies or business organisations.
231 56.45% (n=35) of the respondents from non-governmental organisations.

reporting[232], while ensuring that child sexual abuse material stays down (i.e. that it is not redistributed online) and reducing the amount of new child sexual abuse material uploaded in the open web[233]. It should further 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)[234] and improve transparency and accountability of the measures to fight against child sexual abuse online[235]. Legislation should not overlook the importance of prevention and assistance to victims.

General public

Nearly half of the individuals participating in the survey flagged online grooming of children as the most concerning type of child sexual abuse online, which needed to be tackled as a matter of priority.[236] The distribution of known and new child sexual abuse material by uploading it to the open web (e.g. posting it in social media or other websites, uploading it to image lockers, etc.)[237], and the distribution of new child sexual abuse material via darknets[238] were next on their list.

Among the possible outcomes that the new legislation should aim to achieve, the general public referred to the need to enable swift takedown of child sexual abuse material after reporting[239] and to reduce the number of instances of online grooming of children[240]. The new legislation should further aim to reduce the amount of sexual material self generated by children distributed online (23.27%). Two thirds of the respondents stated that the new legislation should aim to improve assistance to victims of child sexual abuse, while close to half flagged the need for a victim-centric approach in investigations, taking the best interests of the child as a primary consideration. Prevention efforts should further be improved[241].

Cooperation between stakeholders

Public authorities referred to the inefficiencies (such as lack of resources) in public-private cooperation between service providers and public authorities as one of the main challenges while investigating child sexual abuse cases[242]. 33.33% of the respondents further expressed concerns regarding the lack of uniform reporting procedures, resulting in variable quality of reports from service providers.

Almost 50% of the **civil society organisations** taking part in the survey reported that their organisations cooperate with law enforcement authorities by forwarding reports of child sexual abuse online received from the public[243]. 13 out of 62 forward reports from service providers to law enforcement authorities, while some of them provide technology of hash lists for the detection of child sexual abuse online (7 and 4 out of 62, respectively). They also cooperate with service providers in the fight against child sexual

---

232 77.42% (n=48) of the respondents from non-governmental organisations.
233 67.74% (n=42) of the respondents from non-governmental organisations.
234 74.19% (n=46) of the respondents from non-governmental organisations.
235 70.97% (n=44) of the respondents from non-governmental organisations.
236 48.43% (n=231) of the general public.
237 32.91% (n=157) of the general public.
238 33.12% (n=158) of the general public.
239 49.69% (n=237) of the general public.
240 45.49% (n=217) of the general public.
241 58.91% (n=291) of the general public.
242 19.05% (n=4) of the respondents from law enforcement or other public authorities.
243 51.61% (n=32) of the respondents from non-governmental organisations

abuse online by advising them on policies to fight child sexual abuse online[244], and by sending notice-and-takedown requests to service providers[245]. However, they saw room for improvement in the area of cooperation in the fight against child sexual abuse both between civil society organisations and law enforcement authorities[246] and between civil society organisations and service providers[247].

Legislative solutions

Voluntary measures

More than 75% of public authorities stated that social media, online gaming and video streaming should fall within the scope of legislation on voluntary measures to detect, remove and report child sexual abuse online.

50% of the participants representing companies were in favour of voluntary measures to detect, remove and report child sexual abuse online in social media, instant messaging, text-based chat (other than instant messaging) and message boards, among others. Concerning voluntary detection, removal and reporting of known and new (unknown) material, 25% of the replies to the open public consultation questionnaire suggested that these measures should be covered by the possible legislation. Online grooming and live-streaming of child sexual abuse should also be covered by rules on voluntary measures[248].

More than 55% of the representatives from non-governmental organisations suggested that social media, online gaming, web and image hosting providers should be included in legislation which would explicitly allow voluntary detection, removal and reporting child sexual abuse online. A smaller percentage (6.45%) supported that no service provider should be legally enabled to take such voluntary measures. Some respondents required a legislation which would cover not only the voluntary detection and removal of known and new (unknown) child sexual abuse material but also voluntary measures to detect and remove online grooming and live-streaming of child sexual abuse.

Over 50% of the respondents from the general public stated that no service provider should be legally enabled to take voluntary measures to detect, remove and report child sexual abuse. Around 1 in 6 (15%) individuals suggested that the possible legislation should cover the voluntary detection and removal of known and new (unknown) child sexual abuse material, online grooming and live-streaming of child sexual abuse. With regards to voluntary reporting, of all types of child sexual abuse online, around 1 in 10 (10%) of the respondents believe that it needs to be covered by the new legislation.

Mandatory detection and removal of known and unknown child sexual abuse material

Law enforcement and other public authorities, non-governmental organisations, academic[249] and research institutions as well as other entities agreed that the new legislation should impose mandatory detection and removal of know and new (unknown) material, online grooming and live streaming of child sexual abuse. One third of the

---

244 43.55% (n=27) of the respondents from non-governmental organisations.
245 30.65% (n=19) of the respondents from non-governmental organisations
246 74.19% (n=46) of the respondents from non-governmental organisations.
247 72.58% (n=45) of the respondents from non-governmental organisations.
248 12.5% (n=2) in favour of voluntary detection and removal, and 12.5% (n=2) in favour of voluntary reporting.
249 100% (n=4) of the respondents from academic and research institutions.

replies coming from companies suggested the mandatory reporting of different types of child sexual abuse[250].

Public authorities

The majority of law enforcement and other public authorities considered that social media[251], online gaming, video streaming, and instant messaging[252] should be subject to obligatory detection, removal and reporting of known child sexual abuse material[253]. More than half of the respondents (57%) thought mandatory detection and removal should also extend to new (unknown) child sexual abuse material and live-streaming.

Companies

While some companies considered that mandatory detection, removal and reporting should encompass known[254] and unknown child sexual abuse material as well as online grooming[255], a majority disagreed. 31.25% of respondents suggested that no service provider should be subject to a legal obligation to detect, remove and report child sexual abuse online. They were particularly concerned about the costs for small businesses.

Business associations, whose input has to be treated with particular caution given the very small sample size, overall identified a need for legal certainty for all stakeholders involved in the fight against child sexual abuse online (e.g. service providers, law enforcement and child protection organisations)[256]. Two of three respondents thought that service providers should not be subject to a legal obligation to detect, remove and report child sexual abuse online. They proposed a more flexible reporting scheme for small and medium-sized enterprises and law enforcement authorities, always with respect to privacy efforts and principles.

Non-governmental organisations

The majority of non-governmental organisations representatives suggested that online service providers should be subject to a legal obligation to perform those actions in their services with a particular focus on social media[257], online gaming and video streaming[258], among others. On the other hand, 12.9% stressed that no service provider should be subject to such legal obligation. More than 50% of the respondents side with some other respondents in giving priority to mandatory detection and removal of known material[259]; highlighting the importance of mandatory detection and removal of new (unknown) material[260] and live-streaming of child sexual abuse[261].

General public

---

250 31.25% (n=5) of the respondents from companies and business organisations.
251 95.24% (n=20) of respondents from law enforcement or other public authorities.
252 80.95% (n=17) of the respondents from law enforcement or other public authorities.
253 71.43% (n=15) of the respondents from law enforcement or other public authorities.
254 25% (n=4) of the respondents from companies.
255 31.25% (n=5) of the respondents from companies.
256 60% (n=3) of the respondents from business associations.
257 70.97% (n=44) of respondents from non-governmental organisations.
258 64.52% (n=40) of the respondents from non-governmental organisations.
259 59.68% (n=37) of the respondents from non-governmental organisations.
260 50% (n=31) of the respondents from non-governmental organisations.
261 53.23% (n=33) of the respondents from non-governmental organisations.

The majority of the individuals participating in the open public consultation argued that no service provider should be subject to such a legal obligation[262]. They also underlined that the legislation should not include the mandatory or voluntary detection, removal and reporting of any of the proposed types of child sexual abuse (known material, unknown material, online grooming, live-streaming).

Service providers located outside the EU

It was acknowledged that a new legislation should apply to service providers that offer services within the EU, even when the providers themselves are located outside the EU. The idea has been widely accepted by public authorities[263], companies[264] and civil society organisations.[265] On the other hand, more than 50% of the general public opposed to the idea of legislation which would be applicable to service providers that offer services within the EU, when the providers themselves are located outside the EU[266].

Encrypted environments

Opinions are divided on the question of whether online service providers who offer **encrypted services** should be obliged to detect, remove and report child sexual abuse online in their services. A large majority of the respondents representing public authorities[267] would support it, as would a majority of the respondents representing NGOs[268]. They highlighted the importance of ensuring that any action of detection, removal and reporting should be in line with applicable human rights and privacy laws.

47.62% of the respondents from public authorities identified the introduction of end-to end encryption as a challenge in their investigative work, because it results in difficulties in accessing evidence of child sexual abuse. 80.95% also considered that 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 and platforms.

However, other stakeholders, such as civil society organisations dealing with privacy and digital rights, consumer organisations, telecommunication operators, and technology companies, raised concerns, flagging the need to preserve the balance between privacy and security; fundamental rights must be preserved, especially the right to privacy and digital privacy of correspondence. Privacy and digital rights organisations also underlined the need to preserve strong encryption.

Like other groups, business associations and individuals expressed their concerns in relation to privacy of communications. According to business associations, new legislation should put in place safeguards to limit the monitoring of private correspondence to known suspects and require judicial authorisation, rather than legally mandate it as the default position of online service providers.

Business associations further expressed concerns about the potential harm to marginalized groups and urge the need for effective encryption to ensure the online

---

262 62.68% (n=299) of the individuals.
263 95.24% (n=20) of the respondents from law enforcement or other public authorities.
264 62.5% (n=10) of the respondents from companies and business organisations.
265 80.65% (n=50) of respondents from non-governmental organisations.
266 55.65% (=265) disagree, and 38.36% (n=183) agree.
267 95.24% (n=20) of the respondents from law enforcement or other public authorities.
268 69.35% (n=43) of the respondents from non-governmental organisations.

safety of groups at risk (including children, member of the LGBTQ+ community, and survivors of domestic abuse).

Service providers and digital technology industry highlighted the need to distinguish services which host and serve public, user-generated content from private messaging services and warned not to undermine, prohibit or weaken end-to-end encryption. The new legislation should take into account the key role of encryption in providing and ensuring private and secure communications to users, including children, and its integrity should be safeguarded and not weakened.

Individuals stressed that service providers should not be obliged to enforce such measures (detection, removal, reporting) in encrypted services[269] Searching encrypted communications in their view would require adding backdoors to encryption technology and thus threaten to weaken the security of communications in general, which many citizens, businesses and governments rely on.

Safeguards

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.

Public authorities

Public authorities agreed that the legislation should put into place safeguards to ensure the respect of fundamental rights of all users, prevent abuses and ensure proportionality. In particular, the tools used to detect, report and remove child sexual abuse online needed to comply with the data minimization principle and rely on anonymised data where this is possible[270]. The tools should further comply with the purpose limitation principle, and use the data exclusively for the purpose of detecting, reporting and removing child sexual abuse online[271]. Some respondents warned as to the challenges relating to the data retention period and the legislative compliance assessment of online service providers.

Companies

About half of company respondents also highlighted that the tools used to detect, report and remove child sexual abuse online should be the least privacy intrusive, comply with the data minimization principle and rely on anonymised data where possible[272]. Close to half stated that the new legislation should also include safeguards to ensure that 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[273]. Data should be used exclusively for the purpose of detecting, reporting and removing child sexual abuse online and the tools used should comply with the storage limitation principle.

Non-governmental organisations

269 89.73% (n=428) of the respondents from the general public.
270 57.14% (n=12) fully agree and 9.52% (n=2) partially agree, of the respondents from law-enforcement or other public authorities.
271 76.19% (n=16) of the respondents from law enforcement or other public authorities.
272 37.5% (n=6) fully agree and 12.5% (n=2) partially agree, of the respondents from companies.
273 31.25% (n=5) fully agree and 12.5% (n=2) partially agree, of the respondents from companies.

Service providers' actions to detect, remove and report child sexual abuse online need to be proportionate and subject to safeguards, according to NGO respondents. Most of the respondents agreed on the need for a clear complaint mechanism for users[274]. A significant majority stressed that effective remedies should be provided to users[275] that have been erroneously affected by the actions of the service provider to detect, report and remove child sexual abuse online. Furthermore, most deemed essential that service providers would make clear in the Terms and Conditions that they are taking measures to detect, report and remove child sexual abuse online[276].

General public

Concerning safeguards, more than half of individual respondents flagged the need to ensure the availability of a clear complaint mechanism[277] and effective remedies[278] for users that have been erroneously affected. Slightly more than half also thought it was important that providers made clear in the Terms and Conditions that they are taking measures to detect, report and remove child sexual abuse online,[279] as well as to ensure that the tools used to detect, report and remove child sexual abuse online are the least privacy intrusive[280].

Sanctions

The majority of the respondents from law enforcement and other public authorities[281] and from non-governmental organisations[282] would support both financial and criminal sanctions if companies have been found to not meet their legal obligations related to the detection, reporting and removal of child sexual abuse. However, 4.84% of the respondents from NGOs partially disagree with imposing financial sanctions, while 9.67% would further disagree with imposing criminal sanctions to online service providers[283].

50% of the respondents from companies and 60% business associations stated that online service providers that erroneously detect, report or remove child sexual abuse online in good faith should not be subject to financial or criminal sanctions. 60% of the respondents from business associations disagree with imposing criminal sanctions to companies if they fail to meet the legal obligations related to detection, reporting and removal of child sexual abuse online. Detection and removal, in their view, were best placed as part of voluntary requirements to encourage innovation to further develop and deploy technology in this area, while it was also seen as crucial to support national law enforcement authorities responsible for pursuing and prosecuting crimes related to CSAM.

---

274 83.87% (n=52) of the respondents from non-governmental organisations.
275 75.81% (n=47) of the respondents from non-governmental organisations.
276 82.26% (n=51) of the respondents from non-governmental organisations.
277 59.54% (n=284) of the respondents from the general public.
278 61.64% (n=294) of the respondents from the general public.
279 57.23% (n=273) of the respondents from the general public.
280 51.78% (n-247) of the respondents from the general public.
281 33.33% (n=7) fully agree and 52.38% (n=11) partially agree on criminal sanctions; 80.95% (n=17) fully agree and 14.29% (n=3) partially agree on financial sanctions. At the same time, 9.52% (n=2) would partially disagree with such measures.
282 38.71% (n=24) fully agree and 22.58% (n=14) partially agree on criminal sanctions; 54.84% (34) fully agree and 16.13% (n=10) partially agree on financial sanctions.
283 8.06% (n=5) partially disagree and 1.615(n=1) fully disagree with imposing criminal sanctions.

General public

Around 26% of the respondents suggested that companies should not be subject to any financial or criminal sanctions[284] while 19.92% and 15.72% believe that companies should be subject to financial and criminal sanctions, respectively.

Transparency reports and performance indicators

Three quarters of public authorities and non-governmental organisations underlined that transparency reports should be obligatory[285,286] and standardized[287,288] in order 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

Public authorities

More than 80% of law enforcement and other public authorities expect transparency reports to include information on the number of reports of instances of child sexual abuse online reported, by type of service[289]. They also highlighted that reports, as well as the number of perpetrators investigated and prosecuted as a result of a report, by company and type of service, should be taken into account in assessing the success of the possible legislation. The number and ratio of false positives (an online event is mistakenly flagged as child sexual abuse online) of the different technologies used should also be included, based on the 38% of the replies.

Companies and business associations

Close to half of respondents thought that transparency reports should include information on whether data are shared with any third party and on which legal basis, as well as information related to the policies on retention of data processed for the detecting, reporting and removal of child sexual abuse online and the data protection safeguards applies[290]. The number and ratio of false positives (an online event is mistakenly flagged as child sexual abuse online) of the different technologies used should be also taken into account[291]. The size of each organisation and enterprise should be taken into account to ensure that they have the necessary infrastructure in place to respond to any regulatory and/or supervisory requirements.

Non-governmental organisations

82.26% of the replies coming from *non-governmental organizations,* flagged that reports should include information about the time required to take down child sexual abuse material after it has been flagged to/by the service provider while the measures applied to remove online child sexual abuse material in line with the online service provider's policy (e.g. number of accounts blocked) identified as an important element of a transparency report by 80.65% of the respondents.

---

284 25.79% (n=123) fully disagree (on financial sanctions) and 26.62% (n=127) fully disagree (on criminal sanctions), of the respondents from the general public.
285 76.19% (n=16) of the respondents from law enforcement or other public authorities.
286 75.81% (n=47) of the respondents from non-governmental organisations.
287 80.95% (n=17) of the respondents from law enforcement or other public authorities.
288 74.19% (n=46) of the respondents from non-governmental organisations.
289 85.71% (n=18) of the respondents from law enforcement or other public authorities.
290 43.75% (n=7) of the respondents from companies and business organisations.
291 43.75% (n=7) of the respondents from companies and business organisations.

General public

According to individuals, the success of the possible legislation should be monitored based on the number of victims identified and rescued[292] and the number of perpetrators investigated and prosecuted as a result of a report[293], by company and type of service.

Academia

75% of academic and research institutions supported the idea of transparency reports which would be obligatory, and evaluated by an independent entity. They further stated[294] that these reports need to be standardized in order 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.

European centre to prevent and counter child sexual abuse

There is broad consensus among all respondents on the need for additional coordination and support to EU level in the fight against child sexual abuse online and offline. Stakeholders further emphasized the need to avoid duplication of efforts.

In the area of prevention, overall, respondents supported an EU initiative to create an EU Centre to stimulate the exchange of best practices and research and cooperate with non-governmental organizations, law enforcement authorities, educational institutions and academia, and experts, with a view of facilitating the coordination of actions undertaken by competent authorities and relevant stakeholders.

The majority of the respondents, all categories included, reflected that a possible EU Centre would serve to 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[295].

Public authorities

Law enforcement and other public authorities confirmed almost unanimously the need for additional coordination and support at EU level in the fight against child sexual abuse online and offline[296], to maximize efficiency and avoid duplication. A coordinated response at EU level (and beyond) could deal with challenges related to law enforcement, prevention and assistance to victims.

Among the most widely supported functions of the EU Centre, to support law enforcement, respondents acknowledged the need to maintain a single EU database of known child sexual abuse material to facilitate its detection in companies' systems[297]. The EU Centre would further help ensure the relevance of the received reports, determine jurisdiction(s), and forward them to law enforcement for action[298]. In addition, the EU Centre would support law enforcement authorities to coordinate and facilitate the take

---

292 41.93% (n=200) of the general public.

293 41.51% (n=198) of the general public.

294 100% (n=4) of the respondents from academic and research institutions.

295 85.71% (n=18) from public authorities; 37.5% (n=6) from companies; 83.87% (n=52) of the respondents from non-governmental organisations; 40% (n=2) from business associations; 37.53% (n=179) from the general public; and 100% (n=4) from academic and research institutions.

296 85.71% (n=18) of the law enforcement authorities or public authorities.

297 76.19% (n=16) of the respondents from law enforcement or other public authorities.

298 66.67% (n=14) of the respondents from law enforcement or other public authorities.

down of child sexual abuse material identified through hotlines[299]. Regarding the implementation of robust technical and procedural safeguards, respondents flagged it is critical in order to ensure transparency and accountability as regards the actions of service providers[300]. Coordinated actions on a global level, law enforcement cooperation, and exchange of best practices as well as proper resources distribution and support noted as key actions to stop the cycle of abuse.

Practitioners from law enforcement or other public authorities[301] acknowledged the key role of the implementation of EU law in relation to **assistance to victims** of sexual abuse while highlighting the importance of cooperation with different stakeholders in the area of victim protection, assistance and support[302]. Identification of possible legislative gaps, research, and victim's participation, awareness raising campaigns, proper education and training were further listed amongst the suggested measures and good practices. A majority of the respondents would welcome the creation of an EU body[303]. 4.76% identified public- private partnerships and non for profit organisations as the most appropriate types of organisation for the possible Centre. The Centre should be funded directly from the Union budget (90.48% of the replies); or to receive funding from voluntary contributions from industry or non for profit organisations (28.57% and 23.81% of the replies, respectively).

Companies

37.5% of the survey participants representing companies and business organisations confirmed the need for additional coordination and support at EU level in the fight against child sexual abuse online and offline, to maximize the efficient use of resources and to avoid duplication of efforts. Companies and business organisations representatives reflected that the Centre should be serve as a hub for connecting, developing and disseminating research and expertise, facilitating the communication and exchange of best practices between practitioners and researchers[304], to support prevention efforts Furthermore, the role of the Centre would be relevant to support efforts to assist victims of child sexual abuse. The Centre could further support the exchange of best practices on protection measures for victims and further support victims in removing their images and videos to safeguard their privacy. At the same time, it is crucial to ensure that the perspective of victims is taken into account in policymaking at EU and national level.

Like other groups, most of the respondents[305] considered that the possible Centre should be funded directly from the Union budget, while 18.75% support voluntary contributions from industry or non for profit organisations as the most appropriate type of funding.

The idea of the creation of an EU Centre to prevent and counter child sexual abuse had found broad support from business associations. The EU Centre can play a key role in the fight against child sexual abuse and exploitation if designed to complement and build

---

299 61.9% (n=13) of the respondents from law enforcement or other public authorities.
300 57.14% (n=12) of the respondents from law enforcement or other public authorities.
301 80.95% (n=17) of the law enforcement authorities or other public authorities.
302 Civil society organisation, non-governmental organisations, child protection associations and victim protection institutions, law enforcements authorities, lawyers, doctors, experts and academia.
303 76.19% (n=16) of the law enforcement authorities or other public authorities.
304 37.5% (=6) of the respondents from companies.
305 56.25% (n=9) of the respondents from companies.

upon the existing infrastructure. The EU Centre should remain in full harmony and cooperation with other bodies to avoid duplication of efforts and a conflict of reporting obligations to avoid an impact on the efficiency of the system. Additional coordination and support at EU level is needed to improve the sufficiency of communication and exchange of best practices between practitioners and researchers in the area of prevention[306]. In parallel, it was seen as critical to publish aggregated statistics regarding the number and types of reports of child sexual abuse online received in order to ensure transparency and accountability regarding actions of service providers[307].

Non-governmental organisations

The majority of respondents[308]confirmed the need for additional coordination and support at EU level in the fight against CSA online and offline. Most of the participants from non-governmental organisations identified as main challenges in the fight against child sexual abuse that could benefit from additional support and coordination at EU level, the lack of evaluation of the effectiveness of prevention programmes[309] as well as the insufficient communication and exchange of best practices between practitioners (e.g. public authorities in charge of prevention programmes, health professionals, NGOs) and researchers[310], both in the area of prevention and in relation to the assistance to victims.

Respondents from non-governmental organisations acknowledged, as the most relevant functions of the EU Centre to support law enforcement, the need to monitor the take down of child sexual abuse material by different stakeholders[311] as well as to maintain a single EU database of known child sexual abuse material to facilitate its detection in companies' systems[312]. In parallel, they agreed that, it is critical, amongst others, to ensure that the tools employed are sufficiently accurate[313], and are not misused[314]for purposes other than the fight against child sexual abuse. Non-governmental organisations further acknowledged the key role of the implementation of EU law in relation to **assistance to victims** of sexual abuse while highlighting the need for supporting the exchange of best practices on protection measures for victims and the importance of an evidence-based policy on assistance and support to victims[315]. Support victims in removing their images and videos to safeguard their privacy and ensure that the perspective of victims is taken into account in policymaking at EU and national level were also identified as key functions of the future Centre in the area of assistance to victims.

Amid the respondents from non-governmental organisations, 22 welcomed the idea of an EU body[316], as the most appropriate type for the possible Centre. That was followed by public-private partnership (11.29%) and not for profit organisation (12.9%). 79.03% welcomed the idea of an EU Centre which will receive EU funding. Mandatory levies on

306 60% (n=3) of the respondents from business associations.
307 40%(n=2) of the respondents from business associations.
308 83.87% (n=52) of the respondents from non-governmental organisations.
309 66.13% (n=41) of the respondents from non-governmental organisations.
310 69.35% (n=43) of the respondents from non-governmental organisations.
311 51.61% (n=32) of the respondents from non-governmental organisations.
312 61.29% (n=38) of the respondents from non-governmental organisations.
313 48.39% (n=30) of the respondents from non-governmental organisations.
314 48.39% (n=30) of the respondents from non-governmental organisations.
315 83.87% (n=52) of the respondents from non-governmental organisations.
316 35.48% (n=22) of the respondents from non-governmental organisations.

industry (33.87%), voluntary contributions from industry (20.97%) or not-for-profit organisations (17.74%) included in the list.

General public

Additional coordination and support at EU level could be beneficial in the context of prevention and assistance to victims, in particular to tackle the lack of evaluation of the effectiveness of prevention programmes in place[317] as well as the effectiveness of programmes to assist victims[318]. Individuals further identified the 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 (24.11 %) and the lack of an EU approach to determine relevant jurisdiction(s) of the instances of child sexual abuse online and to facilitate investigations (28.93%) as main challenges.

In order to ensure accountability and transparency regarding actions of services providers to detect, report and remove child sexual abuse online in their services, the Centre should ensure that the tools employed are not misused for purposes other than the fight against child sexual abuse[319]. 42.77% of the individuals consider that the Centre could receive complaints of users who feel that their content was mistakenly removed by a service provider, and ensure that the tools employed are sufficiently accurate.

In the area of prevention, the Centre could serve as a hub for connecting, developing and disseminating research and expertise, facilitating the communication and exchange of best practices between practitioners and researchers[320]. The Centre could further carry out research and serve as a hub of expertise on assistance to victims of child sexual abuse as well as support the exchange of best practices on protection measures on victims[321]. Support victims in removing their images and videos to safeguard their privacy and ensure that the perspective of victims is taken into account in policymaking at EU and national level were also identified as key functions of the future Centre in the area of assistance to victims. Almost 50% of the respondents agreed that the new Centre should receive direct funding from the Union budget. Voluntary contributions from not-for-profit organisations (24.11%) or from industry (19.71%) and mandatory levies on industry (17.61%) were next on the list.

Academia

Academics and researchers fully support the idea of the creation of an EU Centre to face the challenges in the area of prevention. The Centre could 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. Providing help to develop state-of-the-art research and knowledge, including better prevention-related data to monitor the take down of child sexual abuse material by different stakeholders could also be a key function of the possible Centre. It could further serve as a hub for connecting, developing and disseminating research and expertise, facilitating the communication and exchange of best practices between practitioners and researchers[322],

[317] 47.17% (n=225) of the respondents from the general public.
[318] 46.54% (n=222) of the respondents from the general public.
[319] 55.14% (n=263) of the respondents from the general public.
[320] 50.95% (n=243) of the respondents from the general public.
[321] 39.41% (n=188) of the respondents from the general public.
[322] 100% (n=4) of the respondents from academic and research institutions.

and providing input to policy makers at national and EU level on prevention gaps and possible solutions to address them.

Practitioners from academic and research institutions further acknowledged the key role of the implementation of EU law in relation to assistance to victims of sexual abuse[323] while highlighting the importance of cooperation with different stakeholders in the area of victim protection, assistance and support. All the respondents from academic and research institutions would welcome the creation of an EU body which should be directly funded from the Union budget.

Inception Impact Assessment324

In total, 41 replies were submitted: 13 by non-governmental organisations, 11 by companies and business organisations, 2 by public authorities, 2 by EU citizens, 1 by academia/research institutions, 2 by business associations, and 10 by other entities (e.g. UNIFEC, Global Partnership to End Violence against Children, etc.). Interested stakeholders could provide feedback to the Inception Impact Assessment from 2 to 30 December 2020.

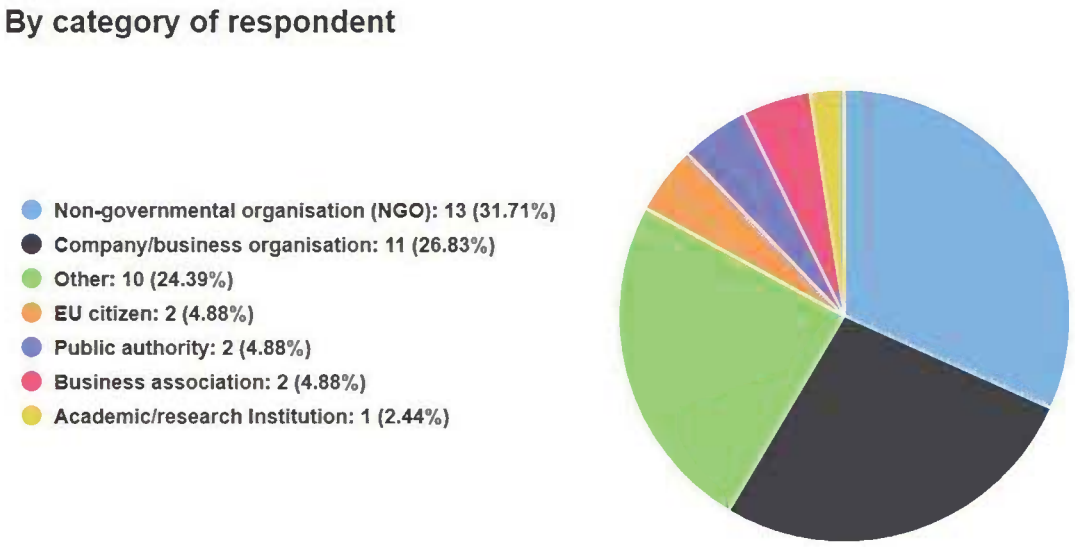
The Inception Impact Assessment aimed to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities.

The feedback gathered in reaction to the Inception Impact Assessment shows that, in summary, the initiative enjoys significant support as the stakeholders welcome the Commission's efforts to tackle child sexual abuse online. Providing legal clarity and certainty as well as the holistic approach of the proposed Centre are seen as the main positive attributes of the proposal. Some concerns regarding mandatory reporting, however, arise amongst different actors. The business representatives are primarily concerned about the duplication of reports and the disadvantageous impacts on SMEs. Furthermore, some believe the legislation should be future proved based on the dynamic development of technology.

[323] 75% (n=3) of the respondents from academic and research institutions.

[324] The Inception Impact Assessment consultation is available here. All contributions received are publically available.

Table 1: Origin of valid feedback by category of respondent



Voluntary measures

Companies

Companies and business organisations call for an EU framework allowing continuing voluntary measures to detect report and remove CSAM on their platforms. Many efforts undertaken by companies to tackle CSAM have already been successful on a voluntary basis e.g. the development of tools such as PhotoDNA. Mandatory detection of known and new CSAM could have serious consequences. A legal requirement to apply such tools risks incentivizing companies towards prioritizing removal over accuracy, and could effectively amount to an obligation to screen all content. Taking into account the limited capability of small and medium-sized companies (SME), voluntary measures to detect CSAM online should be given preference. Reporting mechanisms should be flexible to avoid burdensome requirements for SMEs and overburden LEA. A harmonized approach across the EU, including definitional clarity and exchange of best practices will increase the effectiveness of online platforms' voluntary efforts.

Legal certainty regarding the detection of child sexual abuse material is fundamental. Any new EU legal instrument needs to provide sufficient legal basis for online platforms to continue to operate their detection.

Other entities/stakeholders

Most of the contributions from business associations illustrated that any legislation should take into account the limited capability of small and medium-sized companies (SME). Thus, voluntary measures to detect CSAM online should be given preference. The different (technical and financial) capabilities of SMEs could not be taken into consideration within a legislative framework that imposes mandatory measures. Companies could be safeguarded by creating a legal framework allowing voluntary proactive measures under clear conditions securing compliance with fundamental rights.

Obligation to detect known CSAM

An obligation to detect known CSAM is expected to have a significant impact on SMEs in terms of capacity, resources and economics. Especially SMEs do not always have

access to essential tools to detect CSAM as well as resources to develop this kind of tools. Using external tools or services can be challenging for small operators, as understandable legal restrictions on the ability to access CSAM.

Companies

Some of the contributions from companies and business associations urge the Commission to take into consideration the potential financial and technical burden that would be placed on smaller companies as a result of the adoption of binding legislative measures The data privacy and customer security issues were also highlighted as important among companies.

One the other hand, it was flagged that a legal framework which would create a binding obligation for relevant service providers to detect, report and remove known child sexual abuse material from their services could encourage improvement and provide legal certainty. Simple and streamlined reporting obligations that avoid duplication and confusion in a well-functioning system is essential. Participants further underlined the need for transparency reporting obligations to be reasonable, proportionate, and based on clear metrics.

Other entities/stakeholders

The detection, removal and reporting of child sexual abuse online is a necessary element in the broader fight against the exploitation of children and the protection of their fundamental rights. Any legal framework that is put in place in pursuit of these objectives will need to encompass binding obligations for relevant service providers, on a proportionate basis, and including necessary safeguards. It should ensure legal certainty, transparency and accountability.

Obligation to detect new and known CSAM

Like already mentioned above the legislative option to detect new and known CSAM would have a significant impact on SMEs. Such proposal to mandate the detection and removal of 'new' materials must consider technical realities.

Companies

The responding companies and business associations said there is a need to to formulate requirements in terms of best reasonable efforts at the current state of technology. In addition, that obligations could be differentiated on the basis of size and capability of small and medium enterprises (SMEs) to avoid putting excessive burdens on them. It was further stated that a legal obligation for relevant service providers to detect, report and remove child sexual abuse from their services, applicable to both known and new material, and to text-based threats such as grooming would currently be in contravention of existing EU law (and the proposed DSA) regarding the prohibition of general monitoring efforts, and would also be a more difficult and costly implementation, especially for the smallest platforms.

Participants further underlined the need for transparency reporting obligations to be reasonable and proportionate. Simple and streamlined reporting obligations that avoid duplication and confusion in a well-functioning system is essential.

Non-governmental organisations

Non-governmental organisations called for long term legislation that makes reporting and removal of child sexual abuse material and grooming on their platforms mandatory for

service providers. Mandatory detecting, reporting and removal requires a holistic approach with close cooperation between relevant service providers and stakeholders. As it was further flagged, it is vital that the objectives and obligations are consistent and compatible with the measures set out in the Digital Services Act, particularly around transparency and reporting mechanisms. Any policy and legislative options shall incorporate the strongest available safeguards and address the need for greater transparency and accountability within the industry. The Commission needs to provide legal clarity and certainty as well as to adopt a victim-centred approach. The new legislation must be flexible and future-proof.

Among others, it was stressed that voluntary measures does not meet the overall objectives of the initiative, which means that efforts to counteract child sexual abuse will continue to be fragmented and insufficient.

Other entities/stakeholders

The contributions recognised the importance of legal certainty, transparency and accountability. Any legal framework that is put in place in pursuit of these objectives (detection, removal and reporting of child sexual abuse online) will need to encompass binding obligations for relevant service providers, on a proportionate basis, and including necessary safeguards. In addition, any new initiative should take into account the best interest of the child as well as ensure that functional prevention measures and victim support services are in place.

Encryption

Public authorities

The great importance of balancing the protection of privacy and the confidentiality of communication with the legal interests concerned was specifically highlighted among public authorities.

Companies

Companies' representatives urged for legal certainty for the processing of personal data for the purpose of detecting child sexual abuse material. They further stressed that end-to-end encryption must be preserved; any framework should not undermine, prohibit or weaken end-to-end encryption.

Several parties further advised against requirements to weaken and break encryption and recommend instead that appropriate measures are taken so that content can be detected at the endpoints of encrypted communications, whenever appropriate. It was of utmost importance that the legislative solution chosen remains proportionate to the very purpose of the fight against CSAM.

It was also stressed that any new EU framework should define adequate safeguards efficiently balancing the digital safety interests with users' privacy rights.

Non-governmental organisations

A few stakeholders have shared views on encryption. Specifically, it was recommended that the regulation would include a requirement for service providers of encrypted services to at the minimum facilitate reporting of CSAM and CSE online, including self-generated material, and prompt action to remove confirmed materials upon request from hotlines and law enforcement authorities.

The need for clear legislative frameworks that allow online CSEA to be detected, removed and reported efficiently in order to safeguard the rights of existing victims but also to prevent abuse from occurring in the first place, protecting the privacy of some of the most vulnerable users of online services, was further underlined. Appropriate and realistic rules should be adopted to ensure the roll out of tools scanning text for potential CSE and CSA in line with the GDPR.

European centre to prevent and counter child sexual abuse

Public authorities

The possible creation of a European Centre would create a common front for the harmonization of European legislation in order to prevent and protect children.

Companies

Overall, representatives from companies and business organisations recognised the importance of the role of an EU Centre to prevent and counter child sexual abuse. Among the objectives identified objectives are, the role of the Centre as a hub to provide information regarding programmes, services and legislation that could benefit exploited children; as well as to develop and disseminate programmes and information to law enforcement agencies, nongovernmental organisations, schools, local educational agencies, child-serving organisations, and the general public on the prevention of child sexual abuse exploitation; internet safety, including tips for social media. Provide adequate assistance and support to victims (and their families) as well as specialized training to law enforcement authorities, civil society organisations and the general public.
Non-governmental organisations

Non-governmental organisations welcomed the idea of a European centre to prevent and counter child sexual abuse, which could play an important role in strengthening the global effort to combat child sexual abuse online. Participants pointed out that the existence of a European Centre would help to ensure continued and improved implementation of the European Directive on combating the sexual abuse and exploitation of children as well as to share and promote learning and best practice, and provide rigorous evaluation of existing responses to child sexual abuse.

Address early intervention and prevention of predatory behaviour, as complementary to the detection and identification of perpetrators and child victims is key.

They also flagged the need to enhance global and multi-stakeholder cooperation and enable a coherent approach to tackle child sexual abuse, online and offline. The Centre's functions could include initiatives to improve victim support, law enforcement and prevention. This must be against a wider background of support for children's rights. Legislation and regulations that may be overseen by the Centre have to prioritize these rights.

Other entities/stakeholders

Respondents noted that the proposed European centre to prevent and counter child sexual abuse may address some of the challenges relating to coordination and/or duplication of efforts among different stakeholders. The European centre to prevent and counter child sexual abuse and exploitation could also play a critical role to promote enhanced cross-sector collaboration and engagement modalities, particularly with industry players.

Focusing on the legal framework, a clear legal framework should be developed to empower and protect hotlines engaged in handling and accessing illegal material. For effective investigations and prosecutions, law enforcement authorities need adequate staffing and technical solutions. Currently, there seems to be a lack of resources resulting in delays of analysing hard disks etc. after house searches, and identification of victims and offenders. In addition, it should be taken into account that citizens are often afraid or reluctant to report CSAM to law enforcement authorities directly.

There is an additional need to ensure that the new Regulation and the possible EU centre are fully aligned with relevant EU initiatives as well as legislations, policies and regulations addressing related matters such as other forms of violence.

The EU Centre could further enable improved educational opportunities in schools within the framework of media literacy for both children and parents. It was also highlighted as an important element towards the fight against child sexual abuse, the increased attention to prevention of offending and victimization of children as the best approach to achieve sustainable results at scale and ultimately ensure that children are safe in digital environments. Ensure the views of children are heard and facilitate appropriate ways for meaningful child participation throughout the consultation, decision making and implementation processes.

Academic / research institutions

Academic and research institutions welcome an effort to establish an EU centre to support the effective prevention of child sexual abuse and to help ensure coordinated post-abuse reporting, detection and intervention efforts.

Targeted survey 1 – Law enforcement authorities

The replies to Targeted Survey 1 revealed that:

- Origin of reports:
    - For most EU law enforcement authorities responding (61%), reports received from service providers, either through NCMEC or directly, constitute the single largest source of reports of child sexual abuse online.
    - In the case of 45% of EU law enforcement authorities responding, NCMEC reports amounted to more than half of all reports received.

Participants were asked several questions regarding the origin and quality of reports of child sexual abuse online received by their organisation. Participants were asked to provide data in respect of several possible sources of reports:

- NCMEC;
- Members of the public;
- The respondent's own organisation (e.g., based upon a lead arising in another investigation);
- Other public authorities (including law enforcement authorities) in the same country;
- Public authorities (including law enforcement authorities) in another country;
- National hotlines in the same country;
- National hotlines in another country;
- Directly from service providers; and

- Other sources.

EU law enforcement authorities were invited to participate via EMPACT. Following the validation of data after the survey closed, there were responses from 49 law enforcement authorities in 16 Member States.

Origin of reports

Participants were asked to respond to the following survey question:

'To understand the various sources of child sexual abuse reports that you receive, please estimate the percentage of reports from each of the sources (the total should be around 100%)'

For each of the possible sources, participants were required to select the percentage range corresponding to the approximate percentage of reports received from that source.

Quality of reports

Participants were asked to respond to the following survey question:

Question: 'To understand the quality of the child sexual abuse reports that your organisation receives, please estimate the percentage of reports that are actionable (i.e. that can be used to start an investigation) for each of the different sources'

For each of the possible sources, participants were required to select the percentage range corresponding to the approximate percentage of reports from that source that are typically actionable.

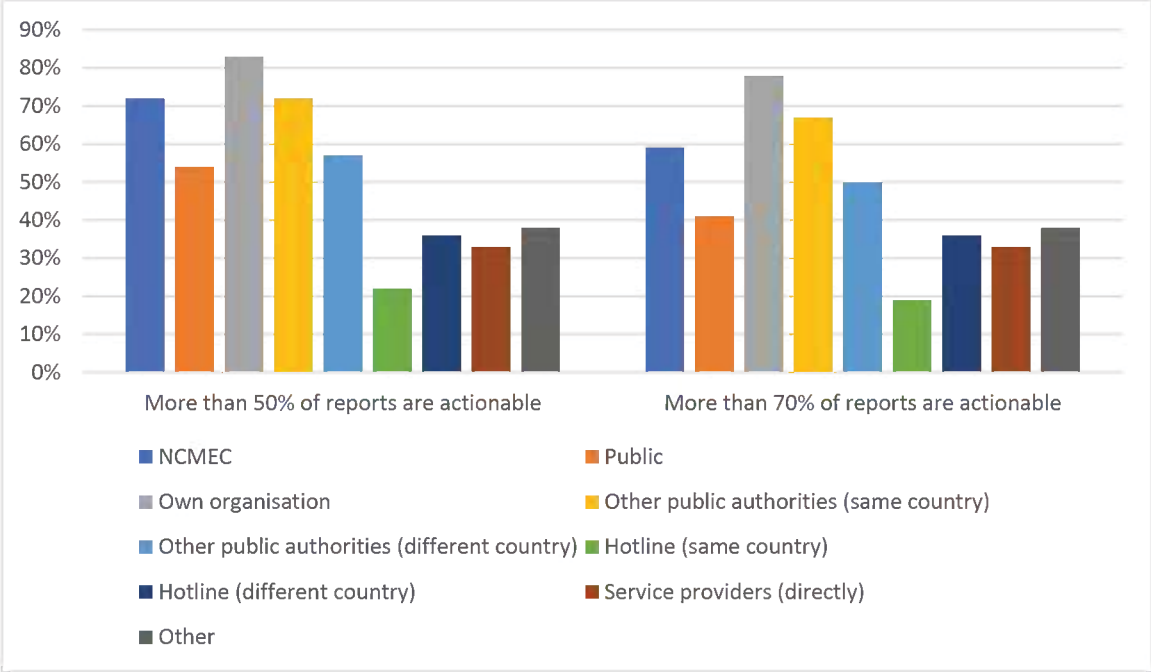
Table 2 shows, for each source, the number of EU law enforcement authorities that estimated that the percentage of reports received by their organisation falls into each of the percentage ranges.

Table 2: Number of respondents answering that a given percentage of reports of CSA online are received from each source

	0-10%	11-20%	21-30%	31-40%	41-50%	51-60%	61-70%	71-80%	81-90%	91-100%	Cannot Estimate / No Answer
NCMEC	6%	8%	12%	14%	10%	6%	6%	10%	20%	2%	4%
Public	47%	22%	4%	12%	4%	0%	0%	2%	0%	0%	8%
Own organisation	47%	22%	8%	2%	0%	2%	2%	0%	0%	0%	16%
Other public authorities (same country)	37%	22%	16%	4%	0%	6%	0%	0%	0%	0%	14%
Other public authorities (different country)	59%	18%	4%	0%	0%	2%	0%	0%	0%	0%	16%
Hotline (same country)	67%	8%	0%	0%	0%	0%	0%	0%	0%	0%	24%
Hotline (different country)	61%	0%	0%	0%	0%	0%	0%	0%	0%	0%	39%

Service providers (directly)	51%	4%	2%	0%	0%	0%	0%	0%	0%	0%	43%
Other	31%	2%	2%	0%	2%	0%	0%	0%	0%	0%	63%

Table 3: Percentage of respondents answering that more than 50% and 70% of reports received from a given source are actionable



Participants were also asked to respond to the following survey question:

'What are the main reasons that make a report non-actionable?'

For each of the possible sources, participants were required to select the typical reasons which lead to a report from that source being non-actionable. There was no limit on the number of reasons that could be selected for each source. Reasons were to be selected from the following list, with the option for respondents to specify other reasons:

- Reported content is not illegal under national law;
- Insufficient information contained in report;
- Report relates to reappearance of known content;
- Insufficient resources;
- Investigation not promising;
- Other (please specify)

Use of reports (investigations)

Participants were asked to respond to the following survey question:

'To understand how investigations of child sexual abuse typically start, please estimate the percentage of investigations that start with a lead from each of the sources below (the total should be around 100%)'

For each of the possible sources, participants were required to select the percentage range corresponding to the approximate percentage of reports received from that source.

Targeted survey 2 – Data regarding reports of child sexual abuse online received by law enforcement authorities

Time required to process reports

Participants were asked to estimate the average time taken to process a report. For the purposes of this survey, the time to process a report was interpreted as meaning the total number of hours of work required to prioritise an incoming report, to investigate the report, and to report back on the outcome of any resulting investigation.

Table4 shows the average time required for each of these tasks.

Table 4: Time required for processing of reports of child sexual abuse online by law enforcement authorities

Task	Reports containing known CSAM	Reports containing new CSAM	Reports relating to grooming
	Time per report (hours)	Time per report (hours)	Time per report (hours)
Prioritisation of reports (time per report)	0.47	0.47	0.47
Investigation	57.75	102.27	89.82
Reporting on the outcome of the investigation	0.32	0.32	0.32
Total	58.54	103.06	90.61
Total (rounded to nearest 10 hours)	60	100	90

Information to be included in reports

In order to determine the information that a report should contain to make it actionable to law enforcement, participants were asked to indicate the importance of several types of information by categorising them under the following possible options:

- Critical – the report cannot be actioned without this information.
- Useful – the report can be actioned without this information, but it should be included if it is available.
- Not relevant – there is no need to include this information in a report.

Participants were also given the option to specify other relevant information.

Table 5 shows the percentage of respondents that categorised each type of information as critical, useful or not relevant (excluding participants who did not select an option for a given type of information).Table 5 shows the percentage of respondents that categorised each type of information as critical, useful or not relevant (excluding participants who did not select an option for a given type of information).

Table 5: percentage of respondents indicating that each type of information is critical, useful or not relevant in order to ensure that a report is actionable

Information to be included in report	Critical %	Useful %	Not Relevant %
Information relating to the provider making the report			
Name of the provider	81%	19%	0%
Point of contact in service provider	33%	57%	10%
Jurisdiction in which the service provider is located	25%	50%	25%
Other information (please specify)	40%	20%	40%
General information relating to the report:			
Indication of whether the report is urgent (child in imminent danger of actual sexual abuse) or not	62%	38%	0%
More detailed indication of level of urgency (please specify)	35%	41%	24%
Nature of report (e.g., CSAM images/videos, grooming, live-streaming of abuse)	48%	52%	0%
Copy of reported content	95%	5%	0%
Additional relevant content data (please specify)	46%	38%	15%
Type of service on which reported content was detected	67%	33%	0%
Date/time the reported content was detected	76%	24%	0%
Languages used in the reported content	29%	57%	14%
Technology which detected the abuse	14%	62%	24%
Traffic data	60%	40%	0%
Other information (please specify)	33%	33%	33%
Information relating to child victim(s) related to reported content:			
Actual age of child victim(s)	48%	48%	5%
Estimated age of child victim(s) (if actual age unknown)	20%	75%	5%
Name of child victim(s)	48%	43%	10%
Contact information of child victim(s)	43%	52%	5%
Jurisdiction(s) in which child victim(s) are located	43%	52%	5%
Relationship between child victim and suspect	33%	67%	0%
Injuries displayed by child	24%	76%	0%
Psychological state of child	14%	71%	14%
Other information (please specify)	33%	22%	44%
Information relating to suspect(s) related to reported content			
Name of suspect(s)	71%	29%	0%
Contact information of suspect(s)	65%	35%	0%
Jurisdiction(s) in which suspect(s) are located	35%	65%	0%
Other information (please specify)	42%	25%	33%

Impact of encryption on investigations into child sexual abuse

In order to obtain further insight into the manifestation of encryption in criminal investigations relating to child sexual abuse and the level of challenge this poses to law enforcement, participants were asked to estimate the proportion of investigations in which encryption had an impact.

Participants were asked to consider the proportion of investigations of child sexual abuse where encryption (at rest/at motion):

- Appeared;
- Delayed the course of an investigation, having a negative impact on safeguarding victims;
- Resulted in an inability to achieve prosecution and/or conviction; and
- Resulted in investigations being altogether stopped.

In each case, participants were asked to indicate which of the following categories applied:

- **None – very few** (0%-25% of investigations affected in this way);
- **Very few – half of my workload** (25-50% of investigations);
- **Half of my workload - very often** (50-75% of investigations); or
- **Very often – all the time** (75-100% of investigations).

Table6 shows the percentage of respondents that indicated that the proportion of cases impacted fell into each category:

Table 6: proportion of cases impacted by encryption (percentage of respondents selecting each category)

	Proportion of cases affected			
	None – very few	Very few – half	Half – very often	Very often – all the time
Proportion of cases where encryption at rest…				
Appears	29%	47%	24%	0%
Delayed the course of a criminal investigation, having a negative impact on safeguarding victims	53%	21%	16%	11%
Resulted in an inability to achieve prosecution and/or conviction	53%	32%	16%	0%
Resulted in investigations being altogether stopped	82%	6%	24%	0%
Proportion of cases where encryption in motion…				
Appears	47%	29%	18%	6%
Delayed the course of a criminal investigation, having a negative impact on safeguarding victims	47%	26%	26%	0%
Resulted in an inability to achieve prosecution and/or conviction	63%	16%	21%	0%
Resulted in investigations being altogether stopped	79%	5%	16%	0%

Participants were also asked to indicate where encryption 'at rest' is most commonly found in investigations, based on four options. The responses to this question are summarised in

Table.

Table 7: Where do law enforcement authorities most commonly encountered encryption of data 'at rest'?

Where do you most commonly encounter encryption of data 'at rest'?	Percentage of respondents
External hard-drives/ thumb storage	26%
Encrypted smartphones/laptops	42%
Password protected File sharing/file hosting/Cloud storage	32%
Other (please specify)	0%
Total	100%

2. Meetings

The meetings, and in particular the "expert process" organised by the Commission, were an integral part of the consultation activities and were instrumental in developing the problem definition and the options described in the impact assessment.

The feedback received in the meetings was not limited to ideas presented by the Commission. In many occasions, they were the stakeholders themselves who produced ideas for discussion.

See Annex 2.3. for procedural information on the different meetings in which feedback from stakeholders was gathered.

3. Conferences

The conferences were an opportunity to present the Commission's work and gather feedback in person from stakeholders in a setting that allows a wider reach than the above meetings.

See Annex 2.3. for procedural information on the different meetings in which feedback from stakeholders was gathered.

2. Surveys

1) Open public consultation

The European Commission launched an open public consultation[325] on 11 February 2021 which closed after 8 weeks, on 15 April 2021. The shorter consultation period to compared to the 12 weeks period usually applied by the Commission was defined in order to ensure that its outcome could be used for the preparation of the Impact Assessment. To mitigate the impact that a reduced timeframe could have on the participation in the consultation, the Commission disseminated the call for contributions widely, including through the targeted discussions and consultations. In addition, the Commission run campaigns on mainstream social media. The purpose of the present open public consultation was to gather evidence from citizens and stakeholders to inform

[325] Available here.

the preparation of the EU Strategy for a more effective fight against child sexual abuse initiatives and it was part of the data collection activities that the related inception impact assessment announced in December 2020.It aimed to gather feedback on current practices as well as on practical and legal problems arising both at national and EU level from gaps and weaknesses of existing regulations. It also listed possible options to address shortcomings and provided an opportunity to indicate preferences for elements that should be included in a solution. It was addressed to a broad range of interested stakeholders, including public authorities, EU institutions and agencies, international organisations, private companies, professional and business associations, NGOs, academics and the general public.

The Open Public Consultation was conducted through an online questionnaire published on the internet in all EU official languages. It was advertised on the European Commission's website, through social media channels (DG HOME, DG CNECT and Europol's EC3 Twitter accounts[326]), through established networks of stakeholders (e.g. WePROTECT Global Alliance, public authorities, hotlines, academia, etc.) and at all relevant meetings.

603 responses were collected: 477 from individuals in the general public and 94 from practitioners in a professional capacity or on behalf of an organisation. Among the 477 responders from general public, there was 1 person who has been a victim of child sexual abuse.

The members of the general public selected a range of countries of residence: (AT, BE, BG, HR, CZ, DK, FI, FR, DE, EL, HU, IE, IT, LT, NL, PL, PT, RO, ES, SE, UK, RU, BW, XK, AL, IL, Philippines, US, VEN, and India. ES,

63 practitioners were members of non-governmental organisations, which is the largest professional group among the 129 practitioners who submitted the questionnaire in their professional capacity or on behalf of an organisation. Other responders included:

- private companies (private sector);
- international or national public authorities (e.g. law enforcement agencies, Ministries, etc.)
- business or professional associations (e.g. trade associations)
- consumer organisations;
- academic and research institutions;
- other entities (e.g. Bar Associations, faith-based organisations, etc.)

They were based across 23 European countries (AT, BE, BG, CY, DK, FI, FR, DE, EL, IE, IT, LV, LU, MT, NL, NO, PT, RO, SI, ES, SE, CH, UK), as well as Thailand, AU, NZ, ZI, RU, BR, French Guinea, and US.

The respondents could also upload a document in order to provide additional information or raise specific points which were not covered by the questionnaire. The following entities submitted additional information:

- Leaseweb Global B.V. - EU based IAAS Cloud hosting provider, The Netherlands

[326] Based on the latest Twitter analytics for the open public consultation to the fight against child sexual abuse, the total number of impressions on DG HOME's main tweet was over 110.000.

- GISAD i.G. (Global Institute for Structure relevance, Anonymity and Decentralisation), Germany
- University of Ljubljana, Faculty of Education, Slovenia
- University of Hull, United Kingdom
- Internet society, United States of America
- Ministry of Justice, Denmark
- BTplc, United Kingdom
- Bundesverband der Freien Berufe – BFB, Germany
- German Bar Association (Deutscher Anwaltverein – DAV), Germany
- EDRi, Belgium
- DOT Europe, Belgium
- Twitter, United States of America
- TikTok Technology, Ireland
- Match Group, United States of America
- Secomba GmbH, Germany
- Open-Xchange AG, Germany
- Austrian Bar Association, Austria
- Global Encryption Coalition, United States of America
- COMECE (Commission of the Episcopates of the European Union), Belgium
- International Justice Mission Netherlands
- Electronic Frontier Foundation, United States of America
- International Centre on Sexual Exploitation, United Kingdom
- Thorn, United States of America
- Terre des Hommes Netherlands, The Netherlands
- Defence for Children - ECPAT the Netherlands
- Defend Digital Me, United Kingdom
- Google, United States of America
- Victim Support Europe, Belgium
- National Center on Sexual Exploitation / International Centre on Sexual Exploitation, United States of America
- Irish Safer Internet Centre, Ireland
- End FGM : European network, Belgium
- Federation of Catholic Family Associations in Europe, Belgium
- Facebook, United States of America
- ETNO (European Telecommunications Network Operators' Association), Belgium
- Norwegian authorities (Ministry of Justice, Ministry of Health and Care Services, Ministry of Children and Families, Ministry of Local Government and Modernisation, Ministry of Culture and Equality), Norway
- Permanent Representation of France to the EU, Belgium
- Digital Europe, Belgium
- Bumble, United States of America

- The Lego Group, Denmark
- Ministry of Justice and Security, The Netherlands

In addition, two EU citizens submitted additional information.

Results of the public consultation are analysed and integrated in this annex as well as in the dedicated sections of the Impact Assessment.

Inception Impact Assessment

A call for feedback, seeking views from any interested stakeholders, on the basis of the Inception Impact Assessment. The consultation, sought feedback from public authorities, businesses, civil society organisations and the public, was open for response from 2 December 2020 to 30 December 2020. Participants of the consultation were able to provide online comments and submit short position papers, if they wished, to provide more background on their views.

2) Targeted surveys

Targeted Survey 1 - Online survey for law enforcement: Tackling child sexual abuse online

The purpose of this survey was to gather qualitative and qualitative information on the current **state of play** in Member States concerning the origin, quality and use of reports of child sexual abuse online law enforcement authorities receive.

The survey was addressed to law enforcement authorities in all Member States.

The Commission received replies from sixteen (16) Member States. The national replies were coordinated at national level amongst different responsible ministries, the judiciary and law enforcement authorities.

The questionnaire was launched on 4 March 2021 and closed on 19 March 2021.

Targeted survey 2 - Data regarding reports of CSA online received by law enforcement authorities

The purpose of this targeted consultation was to gather data on:

- the costs associated with reports of child sexual abuse online received by law enforcement authorities (LEAs);
- how the quality of reports can be improved;
- and the impact of encryption on investigations.

The survey was addressed to law enforcement authorities in all Member States.

The questionnaire was launched on 26 April 2021 and closed on 10 May 2021.

3. Expert Groups, conferences and bilateral meetings

To gather feedback and data to support the evidence-based preparation of the new legislation to fight child sexual abuse, the Commission services organised and participated in various group meetings: with Member States, including the Presidency, but also with a number of private sector service providers and civil society organisations.

Group expert meetings

Expert group on the implementation of Article 25 of Directive 2011/93/EU

The Commission organised an expert workshop to support Member States in the implementation of Article 25 of Directive 2011/93/EU on the detection, taking down and blocking of online child sexual abuse material. Representatives of EU Member States, Europol, Interpol and the INHOPE hotlines took part. Participants discussed detection, removal of CSAM hosted in and outside of Member States' territories, and blocking of illegal content. Challenges included issues such as mandatory reporting, bulletproof hosting, and removing fast moving content.

Expert workshop on current and future challenges in the fight against child sexual abuse

On 6 September 2020, representatives from the EU Member States, Europol, Interpol, the US department of Homeland Security and US department of Justice, and the WeProtect Global Alliance participated in an expert workshop organised by the Commission on current and future challenges in the fight against child sexual abuse. During the workshop participants identified and suggested possible solutions to a number of existing and upcoming trends and challenges in the fight against child sexual abuse, both in its offline and online forms.

Meeting with civil society organisations on the upcoming legislation to fight against child sexual abuse

On 19 February 2021 with participation of close to 100 representatives of civil society organisations focused on children's rights and in particular on the fight against child sexual abuse. The focus of the meeting was to give floor to the civil society organisation to present their views on the key point of the upcoming legislation.

Plenary meeting of the Victims' Rights Platform

The first plenary meeting of the Victims' Rights Platform took place on 23 February 2021. The meeting regrouped over 40 participants, including members of the Victims' Rights Platform and Commission representatives responsible for the victims' related strategies adopted in the past months. DG HOME presented the state of play of the EU strategy for a more effective fight against child sexual abuse focusing on victims' related actions, such as the upcoming European Centre to prevent and counter child sexual abuse.

Meeting with privacy-focused civil society organisations on the upcoming legislation to fight child sexual abuse

On 26 February 2021, an online **meeting with privacy-focused civil society organisations**. The meeting was attended by six representatives of civil society organisations dealing with privacy and digital rights. Participants welcomed the opportunity to share their views on key points that the upcoming legislation could address and contribute to find effective means to detect abuse and support victims, while avoiding interfering with fundamental rights of all internet users.

Meeting with the National Centre for Missing and Exploited Children

The Commission organised a targeted consultation meeting with experts from the National Centre for Missing and Exploited Children (NCMEC) on 4 March 2021. NCMEC welcomed the opportunity to share their views on the upcoming legislation and

to contribute to ensure that any process set up within the EU is effective and complementary to other ongoing efforts. The setting up of the Centre and a number of legislative and practical/operational concerns were discussed.

Meeting with industry stakeholders on the long-term instrument on the fight against child sexual abuse

On 5 March 2021, the Commission brought together a wide range of industry stakeholders with a total of 50 participants attending from 25 companies and representative organisations. During this targeted consultation meeting, participants expressed their strong support for the creation of a European Centre to prevent and counter child sexual abuse. Several speakers emphasised the need to ensure that legislation has regard for the diverse nature of services, and many speakers argued that the initiative should avoid creating duplication of reporting obligations, in particular where companies are subject to obligations to report in the US.

Meeting with Member States' experts (experts from law enforcement, JHA counsellors)

On 8 March 2021, the Commission organised a meeting to hear the views of **Member States' experts (experts from law enforcement, JHA counsellors)** and to exchange on key points that the legislation should cover and any other consideration that would be useful for the Commission to take into account in the preparation of this legislative proposal. The meeting was attended by 70 representatives of Member States. Participants welcomed the opportunity to share their views and ask questions about the key points of the upcoming legislation. They described a number of problems law enforcement encounters in their actions against child sexual abuse.

Targeted consultation meeting with European Parliament Staff

The Commission organised a targeted consultation meeting with European Parliament Staff (APAs, advisors, etc.) on 10 March 2021, for a dedicated meeting on the long-term instrument on the fight against child sexual abuse. Participants stressed that that the legislation should be cover both online and offline CSA; and welcomed the possible European centre to prevent and counter child sexual abuse. Challenges included issues such as mandatory reporting and encryption have been discussed.

Network of prevention of child sexual abuse

On 12 March 2021, the Commission brought together the members of the network on prevention of child sexual abuse, composed of researchers, academics and key NGOs working in this field, for a dedicated meeting. The Commission presented the efforts on the upcoming legislation to address online child sexual abuse. Participants provided feedback on the efforts that industry could further undertake in this space and the possible roles that an EU Centre to prevent and counter child sexual abuse could fulfil.

Technical meetings on end-to-end encryption and the fight against child sexual abuse

Several group meetings and bilateral meetings took place from February to December 2020 with technical experts to discuss possible technical solutions to detect child sexual abuse in end-to-end encrypted electronic communications. The paper summarising the outcome of that work is in annex 9.

Technical meeting on safety by design

A technical meeting on safety by design took place under the umbrella of the EU Internet Forum on 21 October 2021, where industry and civil society stakeholders shared experiences and views.

Bilateral meetings

In the course of the preparation of this Impact assessment, the Commission has had bilateral meetings with a wide range of stakeholders. The Commission participated in bilateral meetings to gather feedback from stakeholders, including meetings with:

- Service providers, including individual companies and industry associations;
- Public authorities from Member States;
- Europol;
- UK, US and AU public authorities;
- Members of the European Parliament;
- NGOs;
- Relevant ongoing EU funded project consortia.

Conferences

Commission representatives also participated in various workshops and conferences to and gather additional input. The list below contains the conferences and workshops in which the Commission participated to provide information on the ongoing work and gather feedback from stakeholders:

- ERA seminars on Preventing Child Sexual Abuse (multiple dates)
- Meeting of the Committee of the Parties to the Council of Europe "Lanzarote" Convention on the protection of children against sexual exploitation and sexual abuse, 25 September 2020
- Technology Coalition, 24 & 25 March 2021
- RENEW webinar on children's rights in the digital world, 30 August 2021
- Safer Internet Forum, Deep Dive on Child Sexual Abuse material (CSAM), 7 October 2021
- Ministerial videoconference on the prevention and investigation of child sexual abuse, 12 November 2021
- Council of Europe Octopus conference, Workshop 6 – Automated detection of child sexual abuse materials, 17 November 2021
- EU Internet Forum Ministerial, 8 December 2021

Letters from stakeholders

The list below contains letters and public statements expressing their views on the commitments in the EU Strategy for a more effective fight against child sexual abuse, and the interim Regulation in particular:

- Joint letter signed by six non-governmental organisations (Save the Children, Denmark, MiudosSegurosNa.Net, Portugal, ArcFund Bulgaria, ECPAT Sweden, e-Enfance, France, 5Rights, UK) on the EU Strategy for a more effective fight against

child sexual abuse and the new Commission's proposal for a Regulation on Privacy and Electronic Communications (11 August 2020), Ares(2020)4231528

- Computer & Communications Industry Association statement10 - September 2020
- Microsoft letter of 2nd September 2020, Ares(2020) 4589540
- CSAM survivors open letter (supported by 8 organizations including the Canadian Centre for Child Protection and NCMEC Statement , 3 December 2020
- Canadian Center for Child protection letter to LIBE, 6 October 2020
- Canadian Center for Child protection letter to the Rapporteur of European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 9 October 2020
- Letter to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) from supporters (signed by more children's organizations in 21 EU Member States, 2 EU Associated Countries, 18 international children's organizations and nine academics or experts), 12 October 2020
- EDRi open letter, of 27th October 2020
- Press release WeProtect Global Alliance, 30 Oct 2020 and 15 Jan 2021
- Australian eSafety Commissioner to LIBE Chair and Vice-Chairs, of 4 November 2020, Ares(2020)6329384
- NCMEC letter to LIBE, CULT, FEMM, 17 27 November 2020
- Europol – EUCTF Statement, 23 November 2020
- Match Group open statement, 5 December 2020
- Missing Children Europe, open statement signed by 25 organisations, 23 December 2020
- Missing Children Europe letter to Commissioners Johannsson and Reynders, 17 December 2020, Ares (2020)7732402
- Letter to the Rapporteur of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) signed by children's rights organisations , 22 January 2021
- UNICEF paper , January 2021
- ECPAT International Statement , 22 December 2020
- EP Intergroup on Children's Rights statement, 22 January 2021
- UN Special Representative of the Secretary-General on Violence against Children, the UN Special Rapporteur on sale and sexual exploitation of children and the UN Special Rapporteur statement, 10 February 21PT Minister of Justice to Commissioner Johansson, 22 February 2021, Ares(2021) 1424242
- European Network of Ombudspersons for Children (ENOC) letter to the European Parliament and the Council of the European Union of 15 February 2021
- US Senator Cotton announces Resolution urging European Union to Protect Children from Online Exploitation, 3 December 2020

Other activities in relation to the interim derogation:

- Canadian Center for Child protection website dedicated to the interim proposal website dedicated to the interim proposal
- NCMEC website dedicated to the interim proposal (including data reduction of reports since December 2020) (NCMEC website dedicated to the interim proposal (including data reduction of reports since December 2020) (
- NCMEC petition in Chicago[327] (35 000 signatures)

4. How the results have been taken into account

The results of the consultation activities have been incorporated throughout the impact assessment in each of the sections in which feedback was received.

This impact assessment is built on the input of a large number of consultation activities in multiple forms and with a wide range of stakeholders, to whom the Commission is grateful for their **fundamental** contributions.

The input has been incorporated in each of the dedicated sections of the Impact Assessment. In particular, the problem definition, the policy option and the impacts reflect the views of the relevant stakeholders that participated in the expert process as well as in other consultation activities. As repeatedly conveyed during the consultations, and at political level, the exponential development of the digital world will continue to play a pivotal role in the worsening of the current challenges to addressing child sexual abuse. EU action to address these increasing challenges is keenly expected by stakeholders.

The general objective of the new legislation is to improve identification, protection and support of victims of child sexual abuse, ensure effective prevention and facilitate investigations, notably through a clarification of the role and responsibilities of online service providers when it comes to child sexual abuse. It would further aim at three specific objectives to ensure the effective detection, removal and reporting of online child sexual abuse, increased coordination of efforts as well as to improve legal certainty, protection of fundamental rights, transparency and accountability.

In the determination of available policy options, the Commission took into account four criteria to assess the impacts of each policy option, namely effectiveness/social impact, efficiency, fundamental rights, and international relations. In particular, the **effectiveness** as well as the **social impact** of each policy option to improve identification, protection and support of victims of child sexual abuse, ensure effective prevention, and facilitate investigations has been assessed. The Commission further measured the **efficiency** of each policy option giving strong consideration to SMEs (i.e. focusing on the assessment of the economic impact of the different options on service providers and public authorities).

Given the significant impact on **fundamental rights**, the effectiveness of the measures and of these conditions and safeguards should be subject to dedicated monitoring mechanisms. The main differences between the options are rather linked to the extent of their effectiveness in safeguarding and balancing fundamental rights and their ability to

[327] Change.org, 'We are in danger of losing the global battle of child safety' petition, accessed 17 May 2021.

offer a more adequate response in light of both the current and the evolving risks emerging in a highly dynamic digital environment. The Commission services suggested that the proposed options have to strike the appropriate balance of interests between ensuring an effective approach to illegal content and activities and the protection of children and their rights, on the one hand, and on the other hand the interests and rights of all users, including freedom of expression and privacy of communications.

In addition, the Commission services identified the significant risk that some providers may cease voluntary measures altogether. It was further acknowledged that increased detection and reporting would have several benefits, including increased identification of suspects and victims in third countries; and reliable information on known CSAM which could be shared with competent authorities in third countries. Standards regarding the quality of reports, safeguards and transparency obligations could positively influence practices in third countries.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. Practical implications of the initiative

For children, child victims and their environment

The initiative addresses **children** who may be at risk of becoming victims of sexual abuse or have experienced abuse. Since child sexual abuse has such severe consequences for children's physical and mental health, their family and social environment are also indirectly affected. The increasing documentation of abuse for online sharing has extended the impact of child sexual abuse far into the adult lives of some victims. The Canadian Centre for Child Protection found that **69% of victims fear being recognised** as a result of their imagery online – and **30% have been recognised.**[328]

From a purely financial perspective, the costs that arise as a consequence of child sexual abuse are significant. **Victims of child sexual** abuse require **immediate and long-term assistance,** which includes physical and mental health care (both in childhood and adulthood), social services and services addressing additional educational needs[329]. The **total lifetime costs** of **assistance to victims** arising from new substantiated cases of child sexual abuse in the United States in 2015 is estimated at 1.5 billion USD (approx. 1 billion EUR)[330].

Even where measures for assistance to victims are in place, they do not fully mitigate the short and long-term effects of child sexual abuse on victims' lives, resulting in additional costs such as a **lifelong loss of potential earnings** due to abuse during childhood[331]. These costs are believed to constitute the largest portion of the overall economic cost of child sexual abuse. The total lifetime cost of such losses in the United States in 2015 was estimated at 6.8 billion USD (approx. 4.7 billion EUR)[332].

The initiative also addresses the environment of the child that provides support in cases of sexual abuse. The overall impact on them is expected to be positive, as set out here below for each group:

- **Victim Support Practitioners.** They are the members of civil society that are in the first line of contact for victims and perpetrators of child sexual abuse, such as hotline employees or child rights NGOs. Increasing the impact of their work and giving them access to expertise and lessons learned is expected to have a positive impact on them, as is the initiative's creation of more effective measures to stem the flow of online child sexual abuse. At the same time, the identification of additional victims that is expected to result from increased detection efforts will put a strain on their resources; in the long term, however, it is hoped that the

---

328 Canadian Centre for Child Protection, Full Report 2017: Survivors' Survey, 2017.

329 Letourneau, E., The Economic Burden of Child Sexual Abuse in the United States, May 2018, p.413-22.

330 *Ibid*, based on combined estimated costs for child health care, adult health care, child welfare and special education.

331 *Ibid.*

332 *Ibid*, based on combined estimated productivity losses for non-fatal and fatal cases of child sexual abuse.

combined measures could eventually lead to an overall reduction in child sexual abuse, particularly online.

- **Social services**, providing support to child victims and their families, based on the best interests of the child, would be expected to benefit from the exchange of best practices and ideas across Member States, which may provide opportunities to identify new and better solutions, or more effective approaches. Like other victim support providers, the detection of additional victims will lead to an increase in workload that may eventually level off and perhaps start declining again in the long run.
- **Health care professionals**: they support victims and families, and deliver treatment to offenders and persons who fear they may offend. Here, the same considerations as for social services and NGOs apply when it comes to an increase in workload related to child victims. In the area of prevention measures targeting offenders, they should benefit from the facilitation of exchange of best practices and lessons learnt, as well as of evidence-based approaches, which can help them to apply the best approaches in their personal practice.
- **Educators:** they play an important role in prevention, in particular through awareness raising, and on detecting early signs of possible abuse. Giving them access to a greater array of tools and options for prevention, based on rigorous scientific analysis and evidence of effectiveness, may contribute to their ability to protect children from child sexual abuse, but also to detect its signs earlier. Their workload is not expected to be affected, but their interventions may become more effective, which they might welcome, given their natural interest in the well-being of the children entrusted to them.
- **Civil society organisations:** they take action against child sexual abuse by, e.g. contributing to make public authorities aware of the crimes, assisting victims, and contributing to preventing child sexual abuse through awareness raising campaigns and programmes for offenders or persons who fear that they might offend. This initiative and especially its measures to support prevention and victim support would help them in their work and facilitate their access to up-to-date and relevant information, as well as to similar initiatives in other Member States or outside the EU. It would help them network and leverage their limited resources more effectively, reducing the risk of inefficient or duplicate investment of their resources.
- **Researchers.** They contribute to expand the knowledge about the nature and prevalence of the problem, and about possible solutions to address it. The information exchange with practitioners is key to ensure that the research remains relevant, is effectively used, and that the solutions proposed are properly evaluated. The initiative, and especially the creation of a centre, would enable access to more data on the phenomenon and facilitate a rigorous analysis of the effectiveness of measures, with a view to further improvements.

For digital service providers (businesses)

The initiative also addresses certain service providers (businesses) that are active on the EU market. The practical implications of this initiative on them are related to two areas: non-legislative action, and legal obligations relating to the detection and reporting of child sexual abuse material. The legislative action focuses on mandatory detection of child sexual abuse material (known/unknown), potentially regardless of encryption.

The **non-legislative actions** considered would be voluntary, and thus compliance will depend on the willingness and capabilities of service providers to take these actions. Under these voluntary measures, service providers are encouraged to increase their transparency on how they fight child sexual abuse on their services through e.g. standardised reports.

In addition, a number of measures considered relate to improved technical capabilities to make the detection and reporting of material more efficient. These measures (sharing of hash databases, Application Programme Interfaces (APIs) for remote checking of hashes, sharing of hash databases of service providers, sharing of technologies between service providers) would generate integration and maintenance costs for them, especially if technical capabilities are inefficient or not available to date. However, if service providers made use of the available technologies that are free of charge or had access to more reliable data on what is considered child sexual abuse in the EU, this could significantly improve the detection process, speed up investigation processes and contribute to the identification and rescue of child victims. Law enforcement could act more swiftly, based on higher-quality, standardised reports.

As to the **legal obligations** for service providers, this initiative would introduce significant changes for service providers and the way they operate. As not all service providers currently detect child sexual abuse material or do so to the same extent, many will have to adapt to changing regulations and deal with increased costs. Significant changes are also expected for those services which are currently offering encrypted exchanges between users. Especially for SMEs, there is a concern that this initiative could represent a practical and financial burden. However, the possibility for businesses to use detection technology free of charge somewhat limits the impact. In addition, an EU Centre making available databases of indicators of known material (e.g. hashes) can significantly support businesses of any size in their practical operations, reduce costs of implementation, limit the risk of false positives, and increase legal certainty. Also, shared databases could result in cumulated cost reductions for individual companies, as they do not have to compile their own databases anymore and run them individually.

Users of online services

The initiative would also impact users of online services. While some service providers, including a number of social media providers and other platforms, already perform detection of child sexual abuse on their services, the present initiative would significantly expand these efforts. This has an impact on the rights of users to privacy of communications, protection of personal data and freedom of expression and information, as detection efforts would need to perform a horizontal analysis of materials shared and of conversations in order to detect those where child sexual abuse materials are being shared or where children may be groomed into child sexual abuse.

Given that the detection would be obligatory in nature and would apply horizontally, users would face limitations in choosing services that do not perform detection of child

sexual abuse if they would prefer to avoid being subjected to such detection measures. The impact on users is therefore significant.

At the same time, the specific category of content targeted by the measures – the sexual abuse of children – is illegal regardless of context and constitutes a particularly egregious violation of fundamental rights of the child. Children, as a particularly vulnerable group, deserve special protection. Especially in the online environment, the existing protection is currently not sufficient to prevent them from being harmed, as has become more evident during the COVID-19 pandemic. As outlined above, the specific type of harm that lies in child sexual abuse has particularly negative and life-long consequences for children. While protection can never be expected to create full safety, these considerations have to be balanced against the impact on users outlined above.

Given the significant impact on users, the initiative includes a number of conditions and safeguards to ensure respect for children's rights and all users' rights including the right to freedom of expression, right to private life and communications as well as to data protection. These would notably include requiring service providers to use technologies and procedures that ensure accuracy, to limit the number of false positives to the greatest extent technically possible and therefore reduce the risk of an unwarranted suspicion of involvement in child sexual abuse. In addition, the initiative aims to create greater transparency of measures, to ensure that users are fully informed about the detection measures and their possible consequences in case child sexual abuse is found, and accountability of processes, including supervision by designated authorities.

The initiative also proposes the creation of an EU Centre in the preferred form of an EU agency, which would provide reliable information to service providers on what is illegal in the EU, and thus contribute to the limitation of false positives. It would also facilitate transparency and accountability, by serving as an independent central point that can publish information about tools used, cases launched, error rates, and, in a few years, possibly also the number of children identified and rescued based on these measures. The centre could help ensure that there is no erroneous takedown or abuse of the search tools to detect legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse) and in facilitating complaints from users who feel that their content was mistakenly removed. These safeguards should help ensure that the impact on users is limited to what is strictly necessary to achieve the legitimate objective and to achieve a fair balance between the important rights on both sides.

For Member States, law enforcement and judicial authorities

As some Member States struggle to put in place effective prevention programmes, lack coordination and efforts are of unclear effectiveness, this initiative intends to offer more structured support to them. This initiative would facilitate and streamline Member States efforts in the fight against child sexual abuse and even facilitate their cooperation with non-EU countries. Areas which could benefit from a more structured approach are prevention efforts concerning child victims and people who fear that they may offend or re-offend as well as research and exchange of best practices.

Law enforcement would also benefit from this initiative as technologies used to detect child sexual abuse would become more reliable when making use of indicators provided by the Centre, reducing the time they have to spend reviewing reports that turn out to contain materials that are not illegal in the EU. At the same time, the expected overall increase in the number of reports will significantly increase the need for law enforcement action and put law enforcement agencies under strain. To mitigate the additional burden, the EU Centre could also support law enforcement by providing reliable classification of

materials as illegal, especially where they have been previously detected. In addition, this is one of the few administrative burdens that has to be categorised as positive overall as it would contribute to a more effective approach to a particularly egregious group of offences.

2. Summary of costs and benefits

The following tables present systematically the average annual and one-off costs and benefits which have been identified and assessed during the impact assessment process.

I. Overview of Benefits (total for all provisions) – Preferred Option *(EUR million/year)*		
Description	***Amount***	***Comments***
Direct benefits		
Reduction of crime/ child sexual abuse.	3 448.0	Annual benefits from reduction of crime.
Indirect benefits		
Facilitation of efforts by the EU Centre.	N/A	Cost savings due to a more effective and efficient use of resources (e.g. avoid duplication of efforts in the EU).
Administrative cost savings related to the 'one in, one out' approach		
Replacement of Interim Regulation and Council Decision.	0.9	Compliance of service providers and public authorities with the existing legislation.

II. Overview of costs – Preferred option *(EUR million/year)*							
Policy measure		**Citizens/Consumers**		**Businesses**		**Administrations**	
		One-off	**Recurrent**	**One-off**	**Recurrent**	**One-off**	**Recurrent**
1	Direct adjustment costs	-	-	€0,21	€2,69	€0,41	€3,36
	Other costs	-	-	€0,01	€0,14	€0,02	€0,18
3	Direct adjustment costs	-	-	-	€0,00	€4,75	€24,42
	Other costs	-	-	-	€0,00	€0,25	€1,29
4***	Direct adjustment costs	-	-	-	€6,55	-	€10,58
	Other costs	-	-	-	€0,34	-	€0,56
5	Direct adjustment costs	-	-	€19,43	€1,62	-	€3,09
	Other costs	-	-	€1,02	€0,09	-	€0,16
6	Direct adjustment costs	-	-	€334,59	€436,46	-	€478,45
	Other costs	-	-	€17,61	€22,97	-	€25,18

7	Direct adjustment costs	-	-	€574,18	€494,45	-	€237,62
	Other costs	-	-	€30,22	€26,02	-	€12,51
8	Direct adjustment costs	-	-	€587,13	€448,32	-	€26,76
	Other costs	-	-	€30,90	€23,60	-	€1,41
Costs related to the 'one in, one out' approach (EUR million/year)							
Total	Direct adjustment costs	-	-	€1.515,54	€1.390,09		
	Indirect adjustment costs	-	-	-	-		
	Administrative costs (for offsetting)	-	-	€79,77	€73,16		

The preferred option E results from the combination of policy measures 1, 3, 4, 5, 6, 7 and 8. The one-off costs of policy measure 4 have been adjusted to take into account the synergies of combining with measures 6, 7 and 8, which replace the voluntary detection in measure 4 for mandatory detection of known CSAM, new CSAM and grooming. See annex 4 for more details.

It is estimated that the administrative costs are 5% of the total costs in each of the policy measures, with the rest of the costs being direct adjustment costs.

The administrative costs savings related to the 'one in, one out' approach result from the replacement of the Interim Regulation. It could be assumed that the cost savings would be equivalent to the administrative costs estimated under measure 4 on voluntary detection (5% of the total costs). This is an approximation, given that the Interim Regulation enables voluntary practices to detect and report CSA online and remove CSAM for the online services that today generate most CSA reports (but not all, see annex 6 on magnitude).

3. Relevant Sustainable Development Goals

This section describes the expected impacts of the most relevant Sustainable Development Goals (SDG) identified in the impact assessment.

Two main SDGs which will be affected by Options B to E, are SDG 16 on peace, justice and strong institutions - considering that one of its targets is to protect children from abuse, as well as SDG 5 on gender equality- considering the previously mentioned statistics which display how girls particularly harmed by sexual offenders.

As the SDGs are interdependent and broad, there are also three main other SDGs which will benefit indirectly from the Options A to E. One of them is SDG 3 on health and well-being, because the Options will contribute to access to safe sexual care for children. Another is SDG 4 on quality education seeing as the Options will ensure children have a safe environment to focus on education. In addition, SDG 9 on industry, innovation and infrastructure will be indirectly affected as the Options and in particular the creation of the Centre, will facilitate technological development.

III. Overview of relevant Sustainable Development Goals – Preferred Option(s)		
Relevant SDG	**Expected progress towards the Goal**	**Comments**
SDG no. 1 – no poverty	An overall reduction of child sexual abuse could limit the risk of poverty and social exclusion of victims of CSA. It could limit the long-term consequences of CSA, which can affect the quality of life.	CSA has long-term consequences that may include e.g. trauma leading to inability hold a job can lead to poverty and social exclusion. The creation of an EU Centre, which would serve as a hub for coordinating best practices, would ensure that research work and best practices are shared concerning countering long-tem economic consequences of CSA, and the link between poverty and CSA, thereby also contributing to SDG no. 1. Children from economically disadvantaged background are at a risk of forced to be sexually abused e.g. to support their families. This includes online abuse, through production and circulation of CSAM, but also livestreaming abuse, the victims of which can be located anywhere in the world. Options A to E would also contribute to locating victims of such abuse and ensuring that they are rescued and given appropriate support including providing for such basic needs as food and shelter.
SDG no. 3 – health and well being	Increase in promoting healthy lives and well-being for children, both from a physical point of view and a mental one.	Considering that SDG 3 has 28 indicators to measure progress, Options A to E will certainly contribute to a few of them. ▪ The Options, and in particular the creation of an EU Centre which focuses on prevention, will also lead to a promotion of mental health for both victims of CSA and potential perpetrators. ▪ Considering the psychological and physical impact which CSA has on its victims, as demonstrated in previous statistics, Options A to E will contribute to safeguarding and treating mental health issues both for children and potential victims. ▪ With regard to Option E in particular, the detection, reporting and removal of CSAM and grooming will actually foster sexual care and sexual health among both children and teenagers. This is because it could aid to prevent and report any related abuse, thereby diminishing the number of victims, as well as victims' risk of self-harm, depression, potential use of substance abuse, and other mental and physical health issues.
SDG no. 4 – quality	Expected increased quality education on	▪ Options A to E will facilitate achieving SDG no. 4 as more children will be able to concentrate on

education	reproductive health and the risks of online and offline child sexual abuse might substantially prevent a number of potential victims in the future.	their education instead of being affected by child sexual abuse. ▪ Also, the creation of an EU Centre, which will serve as a hub for coordinating best practices, will ensure that research work and member state initiatives are shared concerning educational campaigns in schools, thereby also contributing to SDG no. 4.
SDG no. 5 – gender equality	A majority of victims of child sexual abuse are girls. A reduction of child sexual abuse would contribute to reduce gender inequality.	▪ Child sexual abuse leads to harmful psychological and mental consequences which, as mentioned in previous statistics, will diminish the possibility of the affected girls leading full, healthy lives. ▪ SDG 5 has nine targets, which also include adopting legislation to promote gender equality, ending all forms of discrimination against girls and ending violence and exploitation of girls.
SDG no. 9 – industry, innovation and infrastructure	The proposed legislation will lead to service providers exploring and developing new technologies which will allow for innovation across industry, both in the EU and globally	▪ Option E in particular, and the creation of the EU Centre will strengthen the development of online tools to counter child sexual abuse, thereby contributing to technological innovation. ▪ While EU Member States gain and share new knowledge, best practices could be shared globally, including with developing countries, facilitated by the EU Centre.
SDG no. 16 – peace, justice and strong institutions	Option E would have the strongest impact in protecting children from sexual abuse and sexual exploitation.	The UN itself has recognized that the global pandemic has actually increased challenges in child protection and mental health services, and that therefore common action is necessary together. ▪ Options A to E will increasingly support this SDG, as demonstrated in the assessment of the benefits throughout the options which will have a positive impact towards children ▪ The safeguards included in the legislation, including the increased transparency, will contribute to strengthening institutions involved in the fight against child sexual abuse, including on prevention, assistance to victims, and detection, reporting and removal of CSA online.

ANNEX 4: ANALYTHICAL METHODS

1. Qualitative assessment of policy measures

The following process was applied to determine the **policy measures and the policy options** formed on the basis of these measures:

1) **mapping** of possible policy **measures:**
    a. The mapping covered the full spectrum of possible EU intervention: no action, non-legislative action and legislative action.
    b. Given that the issue at hand is basically a **regulatory failure**, it was important to lay out the full range of tools to determine the most proportionate EU response.
    c. The mapping stage included a first filter to **identify** the policy measures to **discard** at an **early stage** (section 5.3 of the main report and Annex 11).
    d. The outcome of the mapping stage was a set of policy measures retained for further elaboration and analysis.
2) **description** of policy **measures** retained in the mapping stage (section 5.2 of the main report)
3) **analysis** of the policy **measures** retained in the mapping stage (this Annex):
    a. This stage included a second filter to **identify** the policy measures to **discard**.
    b. It includes a qualitative analysis using the same assessment criteria as those used to analyse the options. The policy measures **retained** are therefore those that provide the alternatives that are most feasible (legally, technically and politically), coherent with other EU instruments, effective, relevant and proportional to tackle the problem and its drivers analysed in section 2 of the main report.
    c. The outcome of this stage was the final set of measures for the policy options as set out in the overview diagram in section 5.2 of the main report;
4) **description** of policy **options**, formed by combining the retained measures into different groups:
    a. The formation of options follows a **cumulative logic**, with an increasing level of EU legislative action (as set out in the overview diagram in section 5.2 of the main report).
    b. The cumulative logic was followed not only because the measures are in general not mutually exclusive and can be combined but also because they are **complementary** in a number of ways, presenting **synergies** that the combined options can benefit from.
5) **analysis** of policy **options**: the options are analysed in sections 6 (impacts), 7 (comparison of options) and 8 (preferred option) of the main report, as well as in the present annex in more detail.

Non-legislative action

Measure 1: Practical measures to enhance voluntary efforts

Standard code of conduct

Social impact

Developing a standard code of conduct for service providers to sign up to, setting out the ways in which they will use technologies for the detection, removal and reporting of child sexual abuse online, and the standards and processes they will adhere to in doing so, would to some extent enhance prevention, detection and reporting and assistance to victims.

By establishing voluntary minimum standards, the code would lead to increased levels of detection and reporting of online child sexual abuse, enabling the provision of assistance to victims, and enabling interventions to prevent criminal offences. The code would also lead to improved transparency and possibly inspire safeguards regarding actions taken by service providers and their effect on users.

Economic impact

Compared to the baseline scenario, the development of a standard code of conduct would be expected to lead to an increase in the annual number of reports of online child sexual abuse received by EU law enforcement authorities.

There would also be an impact on non-EU countries, which would also experience an increase in the annual number of reports of online child sexual abuse. This increase would to some extent depend on the extent to which the code of conduct was adopted by service providers in relation to their operations outside the EU.

Fundamental rights impact

There would be a slight impact on fundamental rights compared to the baseline scenario. The absence of a clear legal framework for voluntary measures by service providers would not be remedied. Whilst such absence of EU-level legislation would leave service providers flexibility, it would also mean a lack of clarity and possible diverging obligations under national law. The impact on fundamental rights of service providers (mainly freedom to conduct a business) is therefore mixed. Increased adoption by providers of voluntary measures signing up to the code of conduct and increased transparency would affect the fundamental rights of users (especially right to privacy and to protection of personal data).

Voluntary action by online service providers to detect, report and remove online child sexual abuse would continue to be insufficient, and inefficiencies in public-private cooperation would be only partially addressed. The situation would therefore also still negatively affect the fundamental rights of persons who are or may become victims of child sexual abuse (rights of the child, among others).

Standardised reporting forms

Social impact

Developing standardised forms for reports of online child sexual abuse from service providers to authorities would to some extent reduce inefficiencies in public-private cooperation between online service providers and public authorities. Standardised reporting forms would improve the quality of reports and facilitate investigations by ensuring that all relevant information is received by the relevant law enforcement authorities in a coherent manner, maximising the potential for efficient intake of information and for swift and therefore possibly more successful investigations. The impact would be mainly limited to providers not reporting to NCMEC, where

standardisation is already in place; for those reports that EU Member States' law enforcement authorities receive via NCMEC, standardisation has been achieved to some extent. To ensure coherence, standardised forms should align with the standards set by NCMEC to the extent possible, to expand standardisation rather than to establish competing standards.

Standardised reporting forms could also be used by service providers making reports to non-EU law enforcement authorities, improving the quality and relevance of reports in third countries.

Economic impact

The standardisation of reporting forms would create initial implementation costs and should afterwards reduce the costs of dealing with reports for both public authorities and service providers, by ensuring that all critical information is included in reports, facilitating law enforcement responses and reducing the need for follow-up requests for further information from service providers.

Fundamental rights impact

There would be a slight impact on fundamental rights of victims compared to the baseline scenario, resulting from improved efficiencies in investigations. For providers, the voluntary standardisation provides a choice and therefore does not impact their freedom to conduct a business. The creation of standardised forms should not significantly impact users' rights to privacy and data protection and freedom of expression.

Improved feedback mechanisms and communication channels

Social impact

Improved feedback mechanisms would ensure that relevant authorities provide meaningful and timely feedback to service providers regarding the quality of their reports and the nature of the materials or activity reported as illegal or legal. This feedback would serve to assist providers in improving the quality of their reports. In particular, providers could use the feedback to ensure that reports contained all relevant information available to them, and to avoid making reports of content that has been found not to be illegal. Many service providers have requested feedback to help them improve and target their processes more accurately, and it is therefore expected to be welcomed by them. Feedback could help reduce the rate of false positives and therefore improve the accuracy of the whole process.

Economic impact

Improved feedback mechanisms would lead to a slight positive effect on the cost of reports to public authorities and service providers by improving the quality and relevance of reports, and consequently reducing the need for follow-up requests for information from service providers, and reducing the amount of time spent by law enforcement authorities on reports relating to content that is not illegal. At the same time, the initial investment for authorities is likely to be important, as they will need to set up the procedures for feedback, which will also require authorities to determine when and how they can legally share meaningful information with the service provider. In addition, they will then incur ongoing costs in investing time to provide the feedback. It is to be expected that the feedback should launch a virtuous cycle of improving quality of reports and reduced rates of false positives, which would over time reduce the need for feedback other than to confirm that the report was accurate.

Service providers would need to set up procedures to take into account feedback provided, both on individual content detected and to improve their overall procedures,

which would create costs; however, the economic impact on them would be expected to be a mere fraction of the impact on public authorities. It is also to be expected that there would be an economic benefit in the longer term resulting from more accurate detection, which could reduce the number of instances of follow-up on false positives.

Fundamental rights impact

There would be a slight positive impact on fundamental rights of users compared to the baseline scenario, resulting from decreased likelihood of reports erroneously being made to law enforcement authorities by service providers.

APIs for remote checking of hashes

Social impact

The provision of Application Programming Interfaces (APIs) by public authorities to allow service providers to remotely check hashed images and videos would possibly facilitate greater adoption of voluntary measures by service providers, and ensure that such measures can be based on reliable information about materials illegal in the EU. In turn, this would be expected to lead to improved detection, reporting and removal of online child sexual abuse.

Such APIs would, in particular, facilitate the implementation of voluntary measures by smaller providers for whom lack of expertise or financial challenges would otherwise disincentivise action. It is to be expected that it would incentivise providers that have been reluctant to take measures against CSA because of costs to implement such measures, and therefore increase the overall volume of content subject to detection measures. As a result, an increase in the volume of CSAM detected is likely, which would have a positive impact on the ability to detect and investigate crime.

Economic impact

This measure would necessarily entail costs for public authorities, including costs arising from the development of APIs and integration with existing databases of hashes. Similarly, integration would result in costs for service providers choosing to make use of the APIs. These costs would be to some extent offset by savings to service providers resulting from the reduced need to implement their own technological solutions.

Fundamental rights impact

The expected increase in detection measures would impact users' rights, including those to privacy and data protection, and their freedom of expression. Detection measures require mitigating measures and safeguards to limit that impact to what is strictly necessary[333]. Service providers would be supported in taking measures against illegal content at low cost to them, where they so choose, which would have a slight positive impact on their freedom to conduct a business. The rights of the child would similarly experience a positive impact as further instances of CSAM would likely be detected, allowing authorities to take action.

Sharing of databases of hashes between service providers

Social impact

This practical measure to encourage the voluntary sharing of hashes between service providers would improve the ability of service providers to detect known CSAM in their services. However, service providers would continue to lack a centralised source of hashes of material reliably identified as constituting child sexual abuse material

[333] For an overview of conditions and safeguards, please refer to section 5.2.2 of the main report.

throughout the Union, causing law enforcement authorities to continue to receive reports of material that is not illegal, and some material that is illegal to go unreported.

The improved ability to detect known CSAM would likely lead to an increase in reports to authorities, however without any assurances as to an improvement in quality of the reports. Nonetheless, it is likely that the overall volume of CSAM detected and therefore of investigations would rise, resulting in a moderate positive impact on action to protect children and investigate and prosecute crime.

Economic impact
The voluntary sharing of hash databases between service providers would result in minor costs to service providers relating to the provision of hashes through a secure channel. No economic impact is expected on other stakeholders.

Fundamental rights impact
Service providers would be free to participate or not, and are therefore not impacted in their freedom to conduct a business.

The impact on users' rights would be more negative compared to the availability of an authoritative set of indicators, as there are no guarantees as to the quality of hash sets shared, and as these are usually based on the national law at the place of main establishment, which may be outside the EU. This could result in the inclusion of hashes of content that is not considered CSAM under EU and Member States' law. As a result, additional verification of any reports submitted based on this approach would be required.

In parallel, the positive impact on child rights resulting from an increased volume of CSAM detected is similarly more limited than in the previous measure, given the more limited benefits of a pure sharing approach without quality control mechanisms compared to a centralised, vetted system of indicators.

Sharing of technologies between service providers

Social impact
This practical measure to encourage the voluntary sharing of technologies between service providers would improve the availability of technologies for the detection of known CSAM, new CSAM and grooming. Detection, reporting and removal of all these forms of online child sexual abuse would increase as a consequence.

Economic impact
The voluntary sharing of technologies between service providers would result in minor costs to service providers relating to the provision of technologies through a secure channel.

Fundamental rights impact
Service providers would be free to participate or not, and are therefore not directly impacted in their freedom to conduct a business. However, from a competition angle, cooperation between competitors has to respect certain limits in order to preclude or mitigate possible antitrust concerns; a particular point of importance for service providers lies in the speed of detection tools, which are designed to avoid any friction or latency in the user experience and can be a source of competitive advantage. Therefore, such sharing mechanisms would need to be carefully tailored and orchestrated in order to preclude any impact on competition.

Technology sharing could have a positive impact on the freedom to conduct a business of service providers that currently have no tools in place, as they would be supported in taking measures against illegal content at low cost to them, where they so choose.

On the other hand, the expected increase in detection measures would impact users' rights, including those to privacy and data protection, and their freedom of expression, especially in case of erroneous detection, and would therefore require mitigating measures and safeguards to limit that impact to what is strictly necessary.

Continued support to Member States on the implementation of the relevant provisions of the Child Sexual Abuse Directive

Social impact

This practical measure would imply action from the Commission: continuation of workshops and bilateral exchanges with Member States, and continued funding under ISF national programmes. Based on the experience, this measure would lead to improvements in the implementation of the Directive, but would not address any issues outside of the scope of the Directive.

Economic impact

Continued support to Member States would result in minor costs for the Commission budget; the funding under ISF programmes would remain unchanged. Member States would be encouraged to take further measures in particular in the areas of prevention and support to victims, which would likely come with increased costs to them. These increased costs would be offset to some extent by the availability of centralised expertise and materials through Commission support, in particular also under the following measure to facilitate research, exchange and coordination.

Fundamental rights impact

There would be no impact on fundamental rights compared to the baseline scenario; the impact of measures implemented by Member States would depend on the precise measures taken.

Facilitating research, exchange of best practices and coordination in the area of prevention and assistance to victims

Social impact

This practical measure to encourage research, dissemination of good practices between relevant actors would improve the cooperation and coordination between relevant actors. This measure would also help to develop evidence-based policy in prevention and assistance to victims. It is therefore expected to have a positive social impact.

Economic impact

This measure would result in minor costs for the Commission budget, as well as for Member States' authorities, practitioners and other stakeholders participating in the exchange and possibly investing in additional measures on that basis.

Fundamental rights impact

While the measure itself would not have a direct fundamental rights impact, such impacts could result from the measures that Member States may take on the basis of lessons learnt from research and exchange of best practice.

In the long run, this measure should facilitate more impactful prevention efforts at Member State level. This would have a positive impact on the fundamental rights of children, who would stand a greater chance of not falling victim to child sexual abuse.

Also for those who have fallen victim, even though they have already suffered significant disadvantages, more impactful measures to support them could have a moderate positive impact on their rights.

More effective prevention measures could also extend to running joint awareness-raising campaigns or joint work on online safety measures with providers. Where Member States mandate the participation of providers in such programmes, there would be an impact on the freedom to provide services, which Member States would have to take into account and mitigate, where applicable.

Where prevention and victim support measures are conducted in cooperation with service providers, the overall impact on users' rights will depend on the precise measures taken and would need to be taken into account by Member States.

Measure 2: EU Centre on prevention and assistance to victims

This measure is analysed in detail in Annex 10.

Legislative action

Measure 3: EU Centre on prevention and assistance to victims and combating CSA online

This measure is analysed in detail in Annex 10.

Measure 4: Legislation specifying the conditions for voluntary detection of online child sexual abuse

Social impact

This legislative measure would establish for the first time an explicit legal basis permitting service providers to take action to detect online child sexual abuse in their services. The creation of such a legal basis would remove existing legal uncertainties, facilitating wider implementation of such measures by providers who do not currently do so.

As a result, a modest increase in the detection, reporting and removal of online child sexual abuse could be expected, which in turn would lead to a modest increase in victims rescued, suspects detained, and offences prevented.

In addition to removing any existing legal uncertainty that may prevent providers from taking voluntary action, this measure would also address the limitations of the interim Regulation. Without a legal basis for voluntary action, once the interim Regulation ceases to apply three years after entering into force, providers of number-independent interpersonal communications services will be prohibited from using technologies to detect, report and remove online child sexual abuse in their services. These services are estimated to account for more than **two-thirds** of all EU reports of online child sexual abuse made by providers[334].

The creation of a clear legal basis would ensure that such providers are not prohibited from taking action against online child sexual abuse following the expiry of the interim

[334] Data provided by NCMEC to European Commission:
2019 CyberTipline Reports: Trends Seen in Chat and Messaging, October 2020, and 2020 CyberTipline Data: Reports Resolving to the European Union, March 2021

Regulation, thereby avoiding the loss of the majority of reports from providers and consequential impacts on assistance to victims, identification of suspects, and prevention of offences.

Economic impact

Compared to the baseline scenario, the creation of an explicit legal basis for providers' voluntary efforts against online child sexual abuse would, to some extent, lead to an increase in the implementation by service providers of measures to detect such abuse in their services. This would likely result in an increase in the overall volume of reports.

This would imply additional costs both for providers – where they choose to implement measures – and for public authorities in order to adequately process and respond to reports.

Fundamental rights impact

This measure would have several impacts on fundamental rights, including the right to protection of personal data; the right to respect for private life; the right to freedom of expression and information; the right to security and the freedom to conduct a business.

Increased adoption of voluntary measures by service providers as a result of the enhanced legal clarity provided by this measure would lead to safer services, increasing the likelihood of detection of online child sexual abuse. This would contribute to reducing the dissemination of child sexual abuse material (right to protection of personal data, right to respect for private life), increased identification and rescue of victims from abuse (right to security) and increased apprehension of offenders and prevention of future offences (right to security).

Processing of users' personal data under providers' voluntary measures to detect online child sexual abuse would affect the affects users' rights to freedom of expression and information and, to the privacy of their communications.

While the rights to freedom of expression and information do not extend to protecting an exchange of CSAM or other illegal activities, the detection would also need to check legal materials and exchanges for the presence of CSAM. As a result, this measure would need to include strong safeguards to ensure an appropriate balance of the different fundamental rights. These safeguards could include requiring service providers to use technologies and procedures that ensure accuracy, transparency and accountability, including supervision by designated authorities. In addition, a database of confirmed child sexual abuse indicators provided by a designated authority, such as the potential EU centre under Measure 3, would ensure a reliable basis for determining which content is illegal. The transparency and accountability provided by reporting to a designated authority could also help ensure that there are no erroneous takedowns or abuse of the search tools to detect legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse). The centre could provide information on possibilities for redress for users who consider that their content was mistakenly removed.

For interpersonal communications services, the users' fundamental right to privacy of communications will be impacted. Therefore, supplementary safeguards would be required, including targeting the detection of grooming to services where children may be at risk, and providing clear information to users that a provider is using detection tools, as well as information once suspected abuse has been reported, as well as possibilities for

redress. An additional safeguard lies in the anonymised processing by technologies,[335] which helps to ensure that the impact on the fundamental rights of users whose communications are scanned is limited to what is proportionate and strictly necessary, since no personal data deriving from their communications would be processed unless there is a suspicion of child sexual abuse.

This measure would have no impact on the rights of service providers who choose to take no action. On the other hand, service providers who choose to detect child sexual abuse would be subject to new requirements that have not applied previously, in addition to those arising from the DSA proposal, including with regard to the aforementioned safeguards, which would therefore have a moderate effect on their business decisions (freedom to conduct a business). Such requirements however are important safeguards for the fundamental rights of users, given the gravity of the accusation.

Measure 5: Legal obligation to report and remove all types of online child sexual abuse

Social impact

This measure would impose a legal obligation on service providers who become aware of online child sexual abuse in their services to report the abuse to a designated authority. The obligation would apply in relation to all forms of abuse within the scope of this initiative, i.e., previously-known CSAM, new CSAM, and grooming. The reporting obligation would ensure both swift investigations to identify offenders and, where possible, identify and rescue victims, as well as independent verification of the illegality of the content.

While US providers are currently subject to an obligation under US law to report online child sexual abuse to NCMEC, there is no comparable obligation under Union legislation. Where abuse relating to an EU Member State is detected in a US provider's services, the relevant law enforcement authority receives a report via NCMEC, the US Department of Homeland Security and Europol. Where abuse is detected in an EU provider's services, reporting is typically not subject to any legal obligation, and no standardised reporting channels exist.

This measure would ensure that all reports of online child sexual abuse relating to EU Member States are reported directly to the authority designated in the legislation, improving efficiency in comparison to the current reporting channels. Through the incorporation of definitions relating to child sexual abuse under EU/Member State law, this obligation would lead to improved quality of reports, reducing the number of non-actionable reports which relate to content that is not illegal in Member States. Similarly, this measure would ensure that an obligation to report applied in relation to content that is not illegal in a third country, but that is illegal under Union/Member State law.

Finally, this measure would ensure that those providers that currently choose not to report online child sexual abuse in their services are obliged to do so.

---

[335] For example tools such as Microsoft's PhotoDNA software or other techniques to detect child sexual abuse materials. PhotoDNA and similar techniques automatically convert images into a "hash", a code describing the image. This code cannot be converted back into an image and does not contain any personal data. The company then compares the hash of the image to a database of hashes of known CSAM. Where the hash of the user's image matches a hash in the database, the image is flagged as potential CSAM.

Economic impact

Compared to the baseline scenario, the imposition of a legal obligation for providers to report online child sexual abuse where they become aware of such abuse could lead to an increase in the number of reports made by service providers. Nevertheless, it is assumed that where providers choose to voluntarily detect online child sexual abuse, those providers are highly likely to report such abuse even in the absence of an obligation to do so. Furthermore, US service providers are already subject to an obligation to report child sexual abuse under US law.

This measure is therefore expected to result in only a slight increase in the number of reports of online child sexual abuse, and only a slight increase in costs for service providers and public authorities.

Fundamental rights impact

This measure would affect several fundamental rights, including the right to protection of personal data; the right to freedom of expression and information; the right to security and the freedom to conduct a business.

The reporting of suspected online child sexual abuse would inherently involve the processing of sensitive personal data, namely the transfer of the reported content to the designated authority and ultimately (if different) to the relevant law enforcement authority (right to protection of personal data, right to respect for private life). The processing of reports by relevant law enforcement authorities would continue to be subject to the Law Enforcement Directive[336]. Processing for the purpose of making a report would be subject to safeguards to ensure transparency.

This measure would require service providers to take certain actions, incurring costs while doing so (freedom to conduct a business).

The extent of the impact of this measure on the above-mentioned rights is affected to a significant extent by other measures which may be implemented in tandem. In particular, the magnitude of the impact of an obligation to report online child sexual abuse will depend on the volume of abuse that is detected, which is strongly influenced by whether the detection is voluntary or mandatory.

Measure 6: Legal obligation to detect known CSAM

Social impact

This measure would impose a legal obligation on service providers to detect known child sexual abuse material in their services, regardless of whether those services are encrypted (depending on the availability of suitable technology).

The measure would ensure that the detection of known CSAM would no longer be dependent on the voluntary action of providers. Implementation of this measure would

[336] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, 4.5.2016, p. 89–131.Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, 4.5.2016, p. 89–131.

require providers to have access to a reliable source of information on what constitutes CSAM, in order to avoid an undue administrative burden on service providers, to allow for reliable identification of relevant content and ensure proportionality of requirements, in line with the prohibition on imposing general monitoring obligations.

This measure would have a positive social impact by preventing the recirculation of materials previously confirmed as constituting CSAM. Over time, the overall number of images and videos depicting child sexual abuse available on services within scope should be reduced significantly, and, with it, the instances of secondary victimisation inherent in the continued viewing of the abuse. At the same time, it should entail a significant increase in the number of relevant service providers participating, in the volume of detection and reporting, and hence in the proportion of overall cases investigated and number of children identified and removed from abusive situations.

This would also have a positive impact on the overall confidence of users in services, as their exposure to CSAM would also be reduced. This positive impact would extend also to society's expectation that services do not facilitate the sharing of illegal content, especially in the particularly egregious case of child sexual abuse. While the targeting to specific services would possibly somewhat reduce the overall effectiveness of the obligation which could be greater if more services were included in scope, this can be justified in light of the greater impact that such detection might have.

For the detection of known content, the availability of reliable indicators of what constitutes CSAM under EU law and of free-of-charge technologies facilitating automatic detection would support service providers in their identification of relevant content and ensure proportionality of requirements, in line with the prohibition on imposing general monitoring obligations. Known child sexual abuse material is the most common type of child sexual abuse online. The tools to detect it (see annex 8) have a high accuracy rate and have been reliably used for over a decade. The obligation to detect known material would level the playing field and ensure the detection of that content where is currently missing, with all the necessary safeguards. The EU centre would make available the database of indicators of known material (e.g. hashes) that providers should use. The mandatory detection would also encompass materials that victims have referred for detection and removal.

As a downside, such an obligation could result in occasional false positives, that is, in images and videos erroneously identified as CSAM. The obligation to detect therefore could be limited and not be extended to direct removal, as a first safeguard.

Given the impact on fundamental rights of all users, additional safeguards would need to apply, building on and going beyond those set out above for voluntary detection (Measure 4) and for the reliability of the database of indicators. These could include independent expert auditing of the database of indicators and regular supervision and verification of the procedures of the centre, independent expert certification of tools for automated detection to ensure accuracy, as well as additional transparency and accountability measures such as regular reporting. The legislation could also set out information rights of users and mechanisms for complaints and legal redress.

The question of how to deal with encryption is arguably its most complex aspect, given the high stakes on both sides. The inclusion of encrypted content within the scope of this measure ensures a comprehensive approach to combating known CSAM. Encryption, while beneficial in ensuring privacy and security of communications, also creates secure spaces for perpetrators to hide their actions, such as trading images and videos, and approaching and grooming children without fear of detection. Any solution to detect

child sexual abuse therefore needs to ensure both the privacy of electronic communications and the protection of children from sexual abuse and sexual exploitation, as well as the protection of the privacy of the children depicted in the child sexual abuse material. It would also need to ensure that comparable services are treated equally, in line with the principle of equality before the law.

Economic impact

For both the public and the private sector, administrative and compliance costs would arise from implementing new legislation.

For service providers, the introduction of systems for the detection, where applicable, and the new or increased generation of reports would result in costs, also in relation to follow-up requests for further relevant data from public authorities, and for handling complaints and requests for review by affected users. Service providers who are not already investing in developing technologies that would allow the detection of child sexual abuse in encrypted environments will require additional dedicated resources to implement feasible technical solutions that are a good fit for large-scale deployment. This burden may be considerably higher for smaller companies that may not have access to in-house resources. However, they would benefit from the fact that this option would limit further fragmentation of the Internal Market with regard to administrative procedures and obligations required from hosting service providers. Technologies for the detection of known CSAM outside of end-to-end encrypted communications channels have been available free of charge for years and have proven their reliability.

SMEs offering hosting services are particularly vulnerable to exploitation of illegal activities, including child sexual abuse, not least since they tend to have limited capacity to deploy state-of-the-art technological solutions to child sexual abuse material or specialised staff. Therefore, they should not be exempted from any rules and obligations which are mitigated by ensuring that measures are proportionate. The free availability of reliable hash databases and the requisite detection tools are important in this regard. Even though companies may have unequal resources to integrate technologies for the detection of child sexual abuse material into their products, this negative effect is outweighed by the fact that excluding them from this obligation would create a safe space for child sexual abuse and therefore defeat the purpose of the proposal. To further mitigate the economic impact on smaller companies, there is no obligation to take action other than to report the suspicion, and the verification could be left to the expertise of the relevant authorities which would inform the provider whether the material did in fact constitute CSAM. Therefore, service providers would not be forced to invest in additional human resources for confirmation of suspected CSAM. In addition, an obligation to detect child sexual abuse in encrypted spaces would only apply where reliable technologies exist and can be made available for adaptation to providers' products.

The expected increase in reports from service providers would result in significant additional costs to public authorities, in particular law enforcement and judicial authorities, arising from the corresponding increase in investigations and prosecutions. However, this financial impact is expected to be outweighed by the positive economic impact on victim support measures and survivor quality of life and productivity.

A positive effect on the Single Market could result from additional legal clarity and certainty, thus limiting compliance costs. Furthermore, both the public and the private sector would benefit from a common framework creating more legal certainty and mutual trust between the public and the private sector.

Fundamental rights impact

This measure would result in significantly expanded and more effective action against CSAM. It would therefore have a significantly positive impact on fundamental rights of victims whose images are circulating on the internet, in particular on their right to respect for private life. In addition, in creating a more effective approach to child sexual abuse, it is expected to have a positive effect on child rights more generally, including the rights to human dignity and to the integrity of the person.

At the same time, the mandatory nature of the detection has an important impact on providers' freedom to conduct their business. This can only be justified in view of the necessity of the measure to achieve an objective of fundamental importance, namely the more effective protection of children and their rights. The necessity of the measure is based on the experience that victims themselves are frequently unable to seek help, in view of their inherent vulnerability and the specific efforts by offenders to avoid disclosure of their offences. At the same time, offenders are increasingly likely to share evidence of abuse with others online, as is evident from the growing figures of new materials circulating online, as set out in the problem definition. Especially in the context of interpersonal communications, providers are therefore the only ones that have visibility on the abuse taking place. Given that up to 80% of investigations in some Member States are possible only because of reports from providers, such a measure is objectively necessary.[337]

Nonetheless, the impact itself needs to be limited to the maximum extent possible to ensure that it is limited to what is strictly necessary. For providers, this requires providing support for the implementation of the measures. Specifically, providers should have access to a reliable set of indicators of what is illegal in the EU to enable them to search for specific content. In addition, providers need to have access to free and verified detection tools, to reduce the burden on them.

In addition, users' rights are impacted to a greater extent than under the voluntary measures provided for under Measure 5. While some service providers, including a number of social media providers and other platforms, already perform detection of child sexual abuse on their services, the present measure would significantly expand these efforts. This has an impact on the rights of users to privacy and confidentiality of communications, protection of personal data and freedom of expression and information, as detection efforts would need to perform a horizontal analysis of materials shared and of conversations in order to detect those where child sexual abuse materials are being shared or where children may be groomed into child sexual abuse.

Given that the detection would be obligatory in nature and would apply horizontally, users would face limitations in choosing services that do not perform detection of child sexual abuse if they would prefer to avoid being subjected to such detection measures. The impact on users is therefore significant.

At the same time, as set out above, the specific category of content targeted by the measures – the sexual abuse of children – is illegal regardless of context and constitutes a particularly egregious violation of fundamental rights of the child. Children, as a particularly vulnerable group, deserve special protection. Especially in the online environment, the existing protection is currently not sufficient to prevent them from

[337] While the prohibition to impose a general monitoring obligation does not rank as a fundamental right, it serves as a safeguard to facilitate the appropriate balancing of rights and interests. The option ensures compatibility with this principle through the provision of reliable indicators of CSAM and automated tools, as set out in more detail above in section 5.2.3.5.2.3.

being harmed, as has become more evident during the COVID-19 pandemic. As outlined above, the specific type of harm that lies in child sexual abuse has particularly negative and life-long consequences for children. While protection can never be expected to create full safety, these considerations have to be balanced against the impact on users outlined above.

Given the significant impact on users, the initiative includes a number of conditions and safeguards to ensure respect for children's rights and all users' rights, including the right to freedom of expression, right to private life and communications as well as to data protection. These would notably include requiring service providers to use technologies and procedures that ensure accuracy, to limit the number of false positives to the greatest extent technically possible and therefore reduce the risk of an unwarranted suspicion of involvement in child sexual abuse. In addition, the initiative aims to create greater transparency of measures, to ensure that users are fully informed about the detection measures and their possible consequences in case child sexual abuse is found, and accountability of processes, including supervision by designated authorities.

Where encryption is deployed, the detection of CSAM is compatible with most types of encryption provided by the service provider, as both the service provider and the user retain access to the encrypted information.[338] For the specific context of end-to-end encryption in interpersonal communications, some providers have already developed proprietary approaches, and further technologies are under development. Safeguards would therefore also include not to generally weaken encryption and to ensure a high level of information security.

The initiative also proposes the creation of an independent EU Centre, preferably in the form of an EU Agency, which would provide reliable information to service providers on what is illegal in the EU, and thus contribute to the limitation of false positives. It would also facilitate transparency and accountability, by serving as an independent central point that can publish information about tools used, cases launched, error rates, and, in a few years, possibly also the number of children identified and rescued based on these measures. The centre could help ensure that there is no erroneous takedown or abuse of the search tools to detect legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse) and in facilitating complaints from users who feel that their content was mistakenly removed. These safeguards should help ensure that the impact on users is limited to what is strictly necessary to achieve the legitimate objective and to achieve a fair balance between the important rights on both sides.

Measure 7: Legal obligation to detect new CSAM

Social impact

This measure would impose a legal obligation on service providers to detect previously-unknown child sexual abuse material in their services, regardless of whether those services are encrypted.

Whereas the detection of known CSAM reduces the **re-victimisation** of the child depicted in those images and videos and, at times, the investigation initiated with such a report may lead to uncovering ongoing abuses, this material depicts **past abuse**, which in some cases may be years old. By its nature, previously undetected CSAM usually depicts more recent and at times still ongoing abuse, provides particularly valuable leads, and is therefore treated as highest priority by law enforcement. The added value of detecting

[338] This applies, e.g. to the encryption in transit for international data transfers that the ECJ recommends.

"new" CSAM in terms of the ability to identify and rescue children is significant. The positive social impact on children's welfare consequently is significantly higher than in the case of detection of known content, as in Measure 6.

The prompt detection of new CSAM also allows for prevention of its distribution, reducing the possibility of it "going viral" in circles of abusers and being repeatedly recirculated in the future, by adding it to databases of known material. These databases are used both to feed the tools for the detection of known CSAM, and to train and improve the tools for the automated detection of 'new' CSAM. The subsequent detection based on the comparison with these databases can also provide important information about the way in which CSAM is disseminated online and the circles of abusers, facilitating detection and effective action against such groups, which would have a significantly positive social impact of tackling the problem closer to its roots.

The reliability and efficacy of technologies to detect new CSAM is quite advanced, ensuring error rates in the low percentages (0.01% in a recent benchmarking test of one of the key tools), yet the administrative burden on relevant service providers in ensuring the accuracy of efforts is higher and would require an additional degree of human oversight and human confirmation of suspected CSAM.

The proportion of materials flagged as suspected and previously new CSAM in a given year is naturally lower than that of known CSAM, where hashes reflect content created over many years, resulting in a much smaller number of materials requiring verification. Nonetheless, it needs to be considered whether this additional burden can still be considered as proportionate and compatible with the general monitoring prohibition.

The same considerations on encryption mentioned in relation to Measure 6 apply to this measure.

Economic impact

The economic impact of the imposition of a legal obligation to detect previously-new CSAM would, in some respects, be similar to the economic impact of a legal obligation to detect known CSAM (measure 6).

As in the case of Measure 6, for service providers, the introduction of systems, increased volume of reports, follow-up requests and complaints would result in costs. Technologies for the detection of new CSAM outside of end-to-end encrypted communications channels have been available free of charge for years and have proven their reliability.

For public authorities, the expected increase in reports from service providers would result in significant additional costs to public authorities due to the increase in investigations and prosecutions. While the overall number of new materials detected under this measure is expected to be much lower than that of known CSAM under Measure 6, cases of new CSAM require particularly urgent and detailed attention, given the greater likelihood of ongoing abuse and the need for victim identification. However, this financial impact is expected to be outweighed by the positive economic impact on victim support measures and survivor quality of life and productivity.

As in the case of Measure 6, a positive effect on the Single Market could result from additional legal clarity and certainty, thus limiting compliance costs. Furthermore, both the public and the private sector would benefit from a common framework creating more legal certainty and mutual trust between the public and the private sector.

Fundamental rights impact

The fundamental rights impacts of this measure are similar to those for Measure 6, yet are increased both in the positive and in the negative sense by virtue of the greater scope of the measure.

The mandatory detection of new CSAM would be based on verified indicators, to be provided by a designated, trusted authority, such as the possible EU centre under Measure 3. In principle, this would lead to a comparable level of intrusiveness as the detection of previously known material under Measure 6. However, given that accuracy levels of current tools, while still being above 99% in recent testing, are lower than for the detection of known CSAM, human confirmation is essential (and is in any case explicitly set out as a possible safeguard in case of automated decision-making with legal consequences). The impact on users' rights to privacy and confidentiality of communications and personal data protection would therefore be greater and would require additional safeguards.

To limit the impact on providers' rights, especially for SMEs, they could choose to rely on confirmation by the EU Centre, which would in any case review all reports as a safeguard. In addition, strict requirements would need to apply to the technologies deployed, including on the reliability of indicators used, and reliable detection tools would be made available free of charge.

In light of the very recent nature of most undetected CSAM, this option would have a positive impact on the fundamental rights of victims of ongoing abuse and would significantly enhance the possibility of safeguarding victims from additional abuse. In addition, the early detection and swift addition of newly-detected materials to databases of verified CSAM can limit the spreading of content across platforms and hence serve to protect victims' fundamental rights to privacy and data protection.

Measure 8: Legal obligation to detect grooming

Social impact

This measure would impose a legal obligation on service providers to detect grooming in their services, regardless of whether those services are encrypted.

The detection of grooming typically relies on tools for automatic text analysis, which are trained on verified grooming conversations and assess a given exchange according to risk factors identified on the basis of the verified grooming conversations. Such tools are lower in accuracy than tools for the automatic detection of known or new CSAM and would therefore require additional conditions and safeguards to avoid reports of false positives. At the same time, existing figures show that the proportion of suspicious cases flagged is significantly lower still than that of new content, limiting the administrative burden on providers to the verification of a few cases per month.

At the same time, the detection of grooming is of particular relevance for the protection of victims and therefore arguably has the strongest positive impact. While the detection of both known and new CSAM is always detection of evidence of past abuse (but may nevertheless lead to the detection of ongoing abuse), the identification of grooming and subsequent intervention is a measure that can ideally serve to protect children from falling victim to in-person abuse, or to stop ongoing abuse. The comparably higher invasiveness of text analysis tools and lower accuracy rate therefore has to be weighed against the interest in more effective protection of the child.

The same considerations on encryption mentioned in relation to Measure 6 apply to this measure.

Economic impact

The economic impact of the imposition of a legal obligation to detect grooming would, in some respects, be similar to the economic impact of a legal obligation to detect known and new CSAM (measures 6 and 7).

As in Measures 6 and 7, for service providers, an obligation to detect grooming would require investment in the integration of tools to detect grooming. As reports about grooming are subject to human review in many cases, service providers could also incur significant costs related to hiring trained staff. These costs could be mitigated by making available technologies free of charge, limiting service providers' expenses to the integration of such tools into their services, and by allowing service providers to rely on specialised competent authorities, such as the Centre under Measure 3, for the confirmation of cases identified as suspected grooming. By contrast, staffing costs for those authorities would increase as such cases require immediate reaction in order to ensure the protection of victims. Where service providers choose to rely on such authorities for verification before taking action, swift turnaround would have to be ensured in order to inform the provider about the need to intervene in an interaction and to protect a child.

Under this measure, law enforcement authorities would incur higher costs related to the processing of additional reports. While the number of additional reports is expected to be quite low compared the number of additional reports under Measure 6, in the case of reports of grooming, swift action is required in order to ensure protection of the victim, who may be at risk of imminent or ongoing abuse.

This measure would be expected to have a positive economic impact related to victim support and quality of life, as some children would not fall victim to hands-on child sexual abuse because of the timely detection of grooming. This could potentially reduce the impact on victim support systems, as well as having a decisive impact on the quality of life and productivity of the children throughout their lifetime.

Fundamental rights impact

Mandatory detection of grooming would have a more positive impact on the fundamental rights of children as potential victims, compared to Measures 6 and 7, by contributing to the prevention of abuse. At the same time, this obligation would be significantly more intrusive than obligations under Measures 6 and 7, since it would involve searching text in interpersonal communications as the most important vector for grooming.

On the one hand, such searches have to be considered as necessary since the service provider is the only entity able to detect grooming. Automatic detection tools have acquired a very high degree of accuracy (usually above 80%), and indicators are becoming more reliable with time as the algorithms learn. At the same time, the scanning of text in conversations is inherently more invasive into users' rights than the identification of an image or a video as constituting CSAM and require additional safeguards. This is the case even where it is targeted to services where children might be at risk and subject to strict safeguards, as set out above for the voluntary detection of grooming.

In addition, it is questionable whether the reliability of the indicators to be provided is sufficiently high at present to justify the limitation of providers' right to conduct a business. In particular when it comes to avoiding a disproportionate burden as set out notably in the prohibition of general monitoring obligations, it is doubtful whether a fair balance of rights could be achieved here. The assessment of whether a conversation

constitutes grooming of a child is less of a black-and-white assessment compared to CSAM. After automatic flagging, it requires a careful analysis of the exchange and the context and is therefore both inherently more intrusive and requires a significant additional investment of resources of the service provider. At the same time, the possibility to protect children from imminent harm and the significant negative impact of that harm can help justify this measure. Further increasing the quality of the indicators and hence the accuracy of the detection process is of key importance, and safeguards must include the need to deploy state-of-the-art technology in order to reflect advancements, and a requirement for human verification.

2. Qualitative comparison of policy options

The options are compared below through listing positive (+), negative (-) and 'no-change' (~) impacts compared to the baseline (with > indicating more costs in relation to baseline).

Option A: ***practical measures*** *to enhance* ***prevention, detection, reporting and removal, and assistance to victims,*** *and establishing an* ***EU Centre*** *on* ***prevention and assistance to victims***

Criteria	Assessment	Score
Effectiveness	+ Improved prevention and assistance to victims through EU centre on prevention and assistance to victims + Slightly improved detection, reporting and removal of child sexual abuse online in short-term + Limited improvement through legal advice, jurisprudence and establishment of best practices to be adhered to on a voluntary basis + Limited improvement of protection of fundamental rights through better coordination of efforts on prevention and assistance to victims of child sexual abuse - Limited impact of centre to small scale and limited abilities of a non-legislative hub. --- Continued dependence on voluntary measures by providers --- Continued inability for public authorities to investigate and prosecute many crimes --- Providers of number-independent personal communications services would be prohibited from taking measures to detect, report and remove online child sexual abuse following the expiry of the Interim Regulation in 2024 --- Continued violation of rights of victims through failure to detect child sexual abuse offences, rescue victims from ongoing and imminent abuse and prevent crimes -- Continued violation of rights of victims as a result of failure to detect online child sexual abuse, rescue victims from ongoing and imminent abuse and prevent crimes	+

Efficiency	+ Reduction in costs to service providers and public authorities arising from improved feedback mechanisms and standardised reporting forms - Additional costs to service providers and public authorities arising from increased detection and reporting of known CSAM, new CSAM and grooming - Costs to public authorities and service providers arising from development and implementation of practical measures (standard codes of conduct, standardised reporting forms, improved feedback mechanisms and communication channels, APIs for remote checking of hashes, sharing of databases of hashes, sharing of technologies, continued support to Member States on implementation of Directive 2011/93, facilitating research, exchange of best practices and coordination in the area of prevention and assistance to victims) -- Fragmentation of Member States' laws on detection, removal and reporting of online child sexual abuse will likely increase++ EU centre on prevention and assistance to victims would provide a degree of coordination and streamlining of activities and better use of resources.	**Costs:** > **Benefits:** +
Coherence	Legislation: ~ No interference with legislation, as this is an option with non-legislative measures. + Coherent with the Victims Rights Directive through a greater facilitation of the cooperation with Member States with regards to CSA victims. Idem with the CSA Directive on the prevention and assistance to victims provisions. Coordination: + EU centre could positively influence cooperation on prevention and assistance to victims Funding: + The EU Centre can play a signposting role that could facilitate a more effective and efficient use of funding for CSA initiatives	+ + +
Proportionality	The practical measures proposed do not go beyond what is necessary to achieve the specific objectives. As practical measures, they are limited to facilitating the work of Member States, without creating new obligations.	+

*Option B: option A + legislation 1) specifying the conditions for **voluntary detection,** 2) requiring **mandatory reporting and removal** of online child sexual abuse, and 3) expanding the **EU Centre** to **also support detection, reporting and removal***

Criteria	Assessment	Score
Effectiveness/	++ Improvement in terms of decreasing the prevalence of CSA and providing assistance to victims thanks to the EU centre to prevent and counter child sexual abuse + Slightly improved detection, reporting and removal of child sexual abuse online in short-term ++ Clear legal framework for voluntary measures to detect known and new CSAM and grooming --- Continued dependence on voluntary measures by providers --- Continued inability for public authorities to investigate and prosecute many crimes -- Continued violation of rights of children and child victims as a result of failure to detect a significant amount of online child sexual abuse, rescue victims from ongoing and imminent abuse and prevent crimes	++
Efficiency	+++ EU centre could facilitate a more effective use of resources. + Reduction in costs to service providers and public authorities arising from improved feedback mechanisms and standardised reporting forms - Additional costs to service providers and public authorities arising from increased detection and reporting of known CSAM, new CSAM and grooming - Costs to public authorities and service providers arising from development and implementation of practical measures (standard coded of conduct, standardised reporting forms, improved feedback mechanisms and communication channels, APIs for remote checking of hashes, sharing of databases of hashes, sharing of technologies, continued support to Member States on implementation of Directive 2011/93, facilitating research, exchange of best practices and coordination in the area of prevention and assistance to victims)	**Costs:** >> **Benefits:** ++
Coherence	<u>Legislation:</u> + Coherent with relevant horizontal and sectorial legislation at EU level + Coherent with the general monitoring obligation prohibition. <u>Coordination:</u> +++ Facilitation of Member States' and service providers'	+

	efforts on prevention, and assistance to victims through the EU Centre Funding: + The EU Centre can play a signposting role that could facilitate a more effective and efficient use of funding for CSA initiatives	++ +
Proportionality	The provisions do not go beyond what is necessary to achieve the specific objectives. In particular, they do not impose new obligations on Member States on prevention and assistance to victims and they are limited to facilitating their work on those areas. As for detection, reporting and removal obligations imposed on service providers, they are proportionate to the seriousness of the problem and the need to act at EU level to avoid legal fragmentation that affects the Single Market.	+

*Option C: option B + **mandatory detection** of **known** CSAM*

Criteria	Assessment	Score
Effectiveness	++ Effective detection, removal and reporting of known CSAM ++ Clear legal basis for voluntary measures to detect known and new CSAM and grooming +++ Strong safeguards and accountability mechanisms to ensure strong protection of fundamental rights -- Dependent on voluntary action by providers for detection of new CSAM and grooming, which has proven insufficient -- Continued violation of rights of victims as a result of failure to detect new CSAM and grooming, rescue victims from ongoing and imminent abuse and prevent crimes	+++
Efficiency	+++ EU centre could facilitate a more effective use of resources, including reducing law enforcement workload by reviewing the reports and filtering them to ensure that the reports are actionable + Reduction in costs to service providers and public authorities arising from improved feedback mechanisms and standardised reporting forms --- Additional costs to service providers and public authorities arising from increased detection, reporting and removal of known CSAM. - Additional costs to service providers and public authorities arising from increased detection, reporting and removal of new CSAM and grooming.	**Costs:** >>> **Benefits:** +++

Coherence	Legislation: + Coherent with relevant horizontal and sectorial legislation at EU level + Coherent with the general monitoring obligation prohibition. Coordination: +++ Facilitation of Member States' and service providers' efforts on prevention, assistance to victims and detection, reporting and removal of CSA online through the EU Centre Funding: + The EU Centre can play a signposting role that could facilitate a more effective and efficient use of funding for CSA initiatives	+ +++ +
Proportionality	The provisions do not go beyond what is necessary to achieve the specific objectives. In particular, they do not impose new obligations on Member States on prevention and assistance to victims and they are limited to facilitating their work on those areas. As for detection, reporting and removal obligations imposed on service providers, they are proportionate to the seriousness of the problem and the need to act at EU level to avoid legal fragmentation that affects the Single Market.	+

Option D: option C + ***mandatory detection*** *of* ***new*** *CSAM*

Criteria	Assessment	Score
Effectiveness	++++ Effective detection, removal and reporting of known and new CSAM ++++ Strong safeguards and accountability mechanisms to ensure strong protection of fundamental rights -- Dependence on voluntary action by providers for detection of grooming, which has proven insufficient -- Continued violation of rights of victims as a result of failure to detect grooming, rescue victims from ongoing and imminent abuse and prevent crimes	++++
Efficiency	++++ EU centre could facilitate a more effective use of resources, including reducing law enforcement workload by reviewing the reports and filtering them to ensure that the reports are actionable + Reduction in costs to service providers and public authorities arising from improved feedback mechanisms and standardised reporting forms -- Additional costs to service providers and public authorities	**Costs:** >>>> **Benefits:** ++++

	arising from increased detection, reporting and removal of known and new CSAM. - Additional costs to service providers and public authorities arising from increased detection and reporting of grooming.	
Coherence	Legislation: + Coherent with relevant horizontal and sectorial legislation at EU level + Coherent with the general monitoring obligation prohibition. Coordination: +++ Facilitation of Member States' and service providers' efforts on prevention, assistance to victims and detection, reporting and removal of CSA online through the EU Centre Funding: + The EU Centre can play a signposting role that could facilitate a more effective and efficient use of funding for CSA initiatives	+ +++ +
Proportionality	The provisions do not go beyond what is necessary to achieve the specific objectives. In particular, they do not impose new obligations on Member States on prevention and assistance to victims and they are limited to facilitating their work on those areas. As for detection, reporting and removal obligations imposed on service providers, they are proportionate to the seriousness of the problem and the need to act at EU level to avoid legal fragmentation that affects the Single Market.	+

Option E: option D + ***mandatory detection*** *of* ***grooming***

Criteria	Assessment	Score
Effectiveness	+++++ Effective detection, removal and reporting of known and new CSAM and grooming with a clear legal basis +++++Strong safeguards and accountability mechanisms to ensure strong protection of fundamental rights	+++++
Efficiency	+++++ EU centre could facilitate a more effective use of resources, including reducing law enforcement workload by reviewing the reports and filtering them to ensure that the reports are actionable + Reduction in costs to service providers and public authorities arising from improved feedback mechanisms and standardised reporting forms	**Costs:** >>>>> **Benefits:** +++++

	----- Additional costs to service providers and public authorities arising from increased detection, reporting and removal of known CSAM and grooming.	
Coherence	Legislation: + Coherent with relevant horizontal and sectorial legislation at EU level + Coherent with the general monitoring obligation prohibition. Coordination: +++ Facilitation of Member States' and service providers' efforts on prevention, assistance to victims and detection, reporting and removal of CSA online through the EU Centre Funding: + The EU Centre can play a signposting role that could facilitate a more effective and efficient use of funding for CSA initiatives	+ +++ +
Proportionality	The provisions do not go beyond what is necessary to achieve the specific objectives. In particular, they do not impose new obligations on Member States on prevention and assistance to victims and they are limited to facilitating their work on those areas. As for detection, reporting and removal obligations imposed on service providers, they are proportionate to the seriousness of the problem and the need to act at EU level to avoid legal fragmentation that affects the Single Market.	+

3. Quantitative assessment of policy measures

This section describes how the **model** to **estimate the costs** works, the **assumptions** used and the **limitations**.

How the model works

Box 1: How the model estimates costs related to reports of online child sexual abuse

The model estimates the cost of each of the policy measures using the concept of an 'average or typical report' of online child sexual abuse.

The composition of an average/typical report and the number of reports expected annually are used to estimate the costs to public authorities and service providers in the baseline scenario. For each measure, modifiers are used to estimate the expected changes to the composition of an average report and number of reports. This allows the net costs of the measure relative to the baseline to be estimated. The baseline scenario naturally leads to no net costs.

The measures considered under this initiative would give rise to costs to three groups of stakeholders: the possible European **Centre** to prevent and counter child sexual abuse, **public authorities**, and **service providers**. The model attempts to estimate both **one-off** and continuous (annual) **costs**. Typically, these costs have two components: the salary/hour and the hours it takes to do the tasks:

Costs = **cost/hour** of the person doing the tasks x **hours** required to do the tasks.

- Cost/hour:
  - Labour cost per hour for **service providers:**
    - In the case of service providers, the labour cost per hour is based on the average of the salaries in the EU of workers whose activities are classified under Section J (information and communications)[339] in the NACE Rev. 2 statistical classification of economic activities in the European Community[340].
    - This cost includes compensation of employees, plus taxes, minus subsidies.
    - An additional 25% is added to account for overheads (i.e. expenses not related to direct labour, such as the cost of office equipment.).
    - The value is **49.25 EUR/hour**, including the overheads described above.
    - Where the options include a legal obligation to detect child sexual abuse, the costs include an estimate for the deployment (one-off cost) and maintenance (continuous/annual costs) of pre-existing technologies and infrastructure, and the cost of initial and ongoing training.
    - The costs for such options assume a total of **34 600 providers affected by such obligations**[341]. It is also assumed that costs will be

[339] Eurostat, Labour cost levels by NACE Rev. 2 activity, accessed 9 April 2021.

[340] Eurostat, NACE Rev. 2 - Statistical classification of economic activities, accessed 26 April 2021.

[341] Eurostat, Annual enterprise statistics for special aggregates of activities (NACE Rev. 2), accessed 12 May 2021. As clear data for the number of relevant online service providers are not available, this analysis uses data on the number of enterprises in industries J61 (Telecommunications) and J63 (Information Service Activities). In addition to providers falling within the scope of the definition of 'relevant online service providers' for the purposes of this initiative, J61 and J63 include many enterprises falling outside the scope. Therefore, for the purpose of this analysis, it is assumed that 20%

comparatively higher for the 20 providers with the largest market share, due to the need for specialised infrastructure to handle the high volume of expected reports, and the need to integrate the obligations into larger and more complex ecosystems.

- Developing new technical solutions to detect child sexual abuse online (e.g. in in encrypted spaces), only for measures 6-8 below:
  - The cost includes the development, deployment and maintenance of technical solutions by a small number of service providers possibly in partnership with public authorities. The technology would subsequently be made available to other relevant online service providers through the Centre.
  - In order to achieve a realistic estimate, market wages that experienced software engineers and testers[342] are expected to make working for a large technology company were taken as a baseline where this was possible. The estimates are prepared utilising yearly wage figures as available instead of cost per hour.
  - The average salary was taken as 148 000 EUR/year for experienced software engineers and 49 000 EUR/year for testers.
- Labour cost per hour for **public authorities:**
  - In the case of public authorities, the labour cost per hour is based on the **average** of the salaries in the EU of whose activities are classified under Section O (public administration)[343] in the NACE Rev. 2 statistical classification of economic activities in the European Community.
  - This cost includes compensation of employees, plus taxes, minus subsidies.
  - An additional 50% is added to account for overheads (i.e. expenses not related to direct labour, such as the cost of equipment).
  - The value is **46.20 EUR/hour**, including the overheads described above.
- It is assumed that this value remains **constant** for all options and over time.

- **Hours** required to do a task:
  - Since the salary/hour is assumed to be constant, the model focuses on estimating the hours required to do the tasks.
  - These hours required to do the tasks can change if:
    - the **time** required to do **one task** changes, or

---

of enterprises in these industries are relevant online service providers, and that others do not provide relevant online services.

342 Levels.fyi and payscale provide information on salary levels with popular technology companies to help prospective job candidates make decisions.

343 As this category is not included in the source cited above in 339, this data was calculated using the following sources:
Eurostat, Labour cost, wages and salaries (including apprentices) by NACE Rev. 2 activity - LCS surveys 2008, 2012 and 2016, accessed 13 April 2021;
Eurostat, Labour cost index by NACE Rev. 2 activity – nominal value, annual data, accessed 13 April 2021.

- the total number of tasks changes.

Taking into account the proportion of reports of each type (known CSAM, new CSAM and grooming) under the baseline scenario, and the number of hours required to process a report by service providers and public authorities[344], the baseline cost of processing a **typical report of online child sexual abuse** was estimated.

The **one-off costs** were calculated using estimates of the time it takes to carry out the tasks (e.g. development or integration of technologies).

The **continuous costs** were calculated in comparison with the baseline:

1. First, the costs of the baseline were calculated, including the time taken by service providers and public authorities to process a **typical report of online child sexual abuse**, and average number of annual reports expected for the years 2021-2025 based upon the number of reports received in previous years. The number of reports processed by public authorities was adjusted to reflect the percentage of reports received by public authorities that are typically actionable[345]. The model assumes that the costs of public authorities derived from taking action on the actionable reports. The costs of public authorities in processing **all the reports** and discard the non-actionable ones has been incorporated as part of the costs for taking action on actionable reports for the purposes of the model.
2. Second, it was estimated how each of the options changed the time required for a provider or public authority to process a report of online child sexual abuse of each type (known CSAM, new CSAM, grooming) and the number of reports:
    a. For measures involving **voluntary detection**, these changes were estimated as percentages of deviation from the baseline parameters, i.e., percentages by which the number of reports or the time required to process a report increased or decreased as a result of the measure. These group of percentages are called "modifiers" in the explanations below, and are tabled for each of the options.
    b. For measures imposing **obligations** on service providers to detect specific forms of online child sexual abuse, changes in the number of reports were estimated by modelling the potential number of reports (see Table):
        i. The number of **reports per user account** of online child sexual abuse in 2020 was estimated for the service provider which currently makes the overwhelming majority of reports to NCMEC (Facebook)[346]. Facebook was responsible for 95% of service provider reports to NCMEC globally in 2020. Assuming that for EU reports in 2020, Facebook was also responsible for 95% (990 000 reports), and assuming that there were 203 million Facebook accounts in the EU[347], approximately 0.005 reports were made to NCMEC for each EU user account.

[344] Based on discussions with service providers and a targeted survey to law enforcement authorities (see Annex 2).
[345] Targeted surveys of law enforcement authorities (See Annex 2).
[346] *Ibid*.
[347] WeAreSocial, 'Digital 2020' country reports, accessed 9 April 2021

ii. The total **number of EU user accounts** was estimated by combining data on the number of users of social media and messaging services in the EU (252 million) with data on the typical number of accounts held by each user (7.23)[348]. This leads to an estimated total of 1.8 billion EU accounts on social media and messaging services.

iii. It was **assumed** for the purposes of this model that the number of cases of detected online child sexual abuse per user account estimated for the service in (i) above, is **typical** of the number of cases that would be detected by the services in (ii) under mandatory detection.

iv. The data and assumptions in (i), (ii) and (iii) above were combined to produce an estimate for the potential number of reports under an obligation to detect online child sexual abuse. The **total number of potential EU reports** of all types of online child sexual abuse is approximately **8.8 million per year** according to this model.

v. Based on the assumption that **70%** of such reports are actionable[349], this leads to a potential of **6.6 million actionable reports per year**.

3. Finally, the continuous costs for that option resulted from applying the modifiers to the baseline values or substituting the modelled number of potential reports to obtain the time/attempt and the number of attempts for each option's scenario.

   In the case of measures 6-8, the continuous costs include the maintenance and development of technical solutions to detect child sexual abuse regardless of the technology used in the online exchanges (e.g. encrypted environments,) and costs relating to implementation and training arising from obligations to detect each form of online child sexual abuse

Table 1: Estimation of number of potential EU reports of online child sexual abuse (all figures are estimates and refer to 2020)

Number of EU reports	Percentage of global reports from Facebook	Number of EU reports from Facebook	EU Facebook Accounts	Number of reports per EU Facebook Account	Number of EU social media and messaging users	Social media and messaging accounts per EU user	Number of EU social media and messaging accounts	Number of potential EU reports
1,046,350	95%	990,706	203,610,000	0.0049	252,057,500	7.23	1,822,476,819	8,812,811

In summary, to calculate the costs of each option, the following questions were analysed for each of the measures:

1. Are there any one-off costs?
2. Does the measure **change** the **time** required for a service provider or public authority to process a **typical report of online child sexual abuse**? i.e., does the

[348] WeAreSocial, 'Digital 2020' country reports, accessed 9 April 2021

[349] Targeted surveys of law enforcement authorities (see Annex 2).

measure **change** the proportion of reports that are of each type, or the time required to process reports of each type?

3. Does the measure **change** the **total number** of **typical reports** of child sexual abuse online?
4. Combining the above, does the measure **change** the **total continuous costs** for a provider to detect, report and remove child sexual abuse online, or for a public authority to investigate and prosecute a report of child sexual abuse online?

The following **general assumptions** were made:

- The cost/hour = 49.25 EUR/hour for service providers, 46.20 EUR/hour for public authorities remains **constant** for all options and over time.
- The time required to process **a typical report** is an estimated average, taking into account the proportion of reports of each type (known CSAM, new CSAM and grooming), and the number of hours required to process a report by service providers and public authorities[350]. This time is updated for each of the measures based upon their effect on the composition of a typical report, i.e., based upon how each measure affects the percentage of reports of each type. The differentiation between different forms of online child sexual abuse is based upon the assumption that a greater level of human oversight and consideration is necessary for certain types of content such as grooming.
- The cost of handling a typical report under each measure is obtained by combining the cost per hour with the overall number of typical reports expected under that measure.
- Measures 6-8 also include costs relating to implementation and training arising from obligations to detect each form of online child sexual abuse. These costs include an estimate for the deployment (one-off cost) and maintenance (continuous/annual costs) of pre-existing technologies and infrastructure, and the cost of initial and ongoing training.
- The costs for such measures assume a total of 34 600 providers affected by such obligations[351]. It is also assumed that costs will be comparatively higher for the 20 providers with the largest market share, due to the need for specialised infrastructure to handle the high volume of expected reports, and the need to integrate the obligations into larger and more complex ecosystems.

---

[350] Based on discussions with service providers and a targeted survey to law enforcement authorities (see Annex 2)

[351] Eurostat, Annual enterprise statistics for special aggregates of activities (NACE Rev. 2), accessed 12 May 2021. As clear data for the number of relevant online service providers are not available, this analysis uses data on the number of enterprises in industries J61 (Telecommunications) and J63 (Information Service Activities). In addition to providers falling within the scope of the definition of 'relevant online service providers' for the purposes of this initiative, J61 and J63 include many enterprises falling outside the scope. Therefore, for the purpose of this analysis, it is assumed that 20% of enterprises in these industries are relevant online service providers, and that others do not provide relevant online services.

The next section describes the **specific assumptions** used to answer the above questions for each of the measures, and presents the estimated costs.

Calculation of the cost estimates for each measure.

Measure 0: Baseline

The analysis of the costs of the baseline serves as a reference to estimate the costs for public authorities and service providers of the other options.

1) One-off costs.

There are logically no one-off costs in the baseline.

2) Time per typical report.

The time per typical report was estimated by first estimating the time taken by service providers and public authorities to process a report of known CSAM, new CSAM, or grooming. These times were then combined with the proportion of reports of each type in a typical report to estimate the time taken by service providers and public authorities to process a typical report of online child sexual abuse under each measure.

The following tasks were considered:

- Service providers:
    - Human review of one case of content flagged as possible child sexual abuse online
    - Preparation/completion of one report of child sexual abuse online
    - Submission of one report of child sexual abuse online to relevant authorities
    - Respond to requests for further information/clarification
- Public authorities:
    - Prioritisation of reports received
    - Decision on commencement of investigation (where applicable)
    - Analysis/classification of reported content
    - Investigation
    - Rescue of victims
    - Arrest of suspects
    - Prosecution of suspects
    - Feedback to person / organisation reporting child sexual abuse online

The estimated time for a service provider to process a report in the baseline scenario is 45 minutes, 60 minutes, and 90 minutes, respectively, for reports of known CSAM, new CSAM and grooming.

The estimated time for a public authority to process a report in the baseline scenario is 1 hour for reports of known CSAM, and 2 hours each for reports of known CSAM, new CSAM and grooming.

3) Total number of reports.

- Reports of child sexual abuse online forwarded by NCMEC to EU law enforcement authorities have increased from 52 000 in 2014 to over 1 million in 2020.

- Based upon annual data for the years 2010-2020, the evolution in the number of reports for subsequent years can be estimated by extrapolation (see Table 2: Estimated number of annual reports (baseline scenario). This analysis produces an estimate of an average of 1.9 million reports annually for the years 2021-2025. This represents the number of reports that would be received if historic trends in the levels of detected abuse continue to develop in the same way.
- The proportion of reports of each type is estimated based upon the files included in EU-related reports received by NCMEC in 2020[352]. These reports included 3 736 985 files of known CSAM, almost 530 000 files of potentially new CSAM, and almost 1 500 reports of grooming[353]. Based upon these proportions, and for the purposes of determining the composition of an average report, the 1.9 million reports described above would be expected to consist of approximately 1.7 million reports of (only) known CSAM, 240 000 reports of (only) new CSAM, and 725 reports of solicitation[354]. Table 3 shows the breakdown of files included in reports in 2020, which is used to estimate the proportion of reports of each type in the baseline scenario, and subsequent measures which apply modifiers to the baseline scenario.

Table 2: Estimated number of annual reports (baseline scenario)

	2021	2022	2023	2024	2025	Average 2021-2025
Total Reports	1,303,129	1,592,421	1,910,635	2,257,769	2,633,825	1,939,556

Table 3: files contained in EU-related reports from online service providers in 2020

Type of child sexual abuse online	**Files**	**%**
All files (known and new CSAM + grooming)	4 266 604	100%
Known CSAM	3 736 985	87,59%
New CSAM	528 166	12.38%
Grooming	1 453	0,03%

Based upon the targeted survey of law enforcement authorities, the number of reports processed by **public authorities was reduced by 30%** to reflect the proportion of reports that are typically found to be **non-actionable**[355].

Table4 shows the composition, time and cost per typical report for the baseline:

[352] 2020 CyberTipline Data: Reports Resolving to the European Union, March 2021.
[353] For the purposes of this analysis, each report of grooming is considered a single file.
[354] In reality, a single report can contain one, two or the three types of CSA online (known and new CSAM and solicitation/grooming). The simplification of assuming that each report only contains one type of CSA online is made just for the purposes of determining the typical/average report in which the cost model is based.
[355] See Annex 2.

Table 4: Composition, time and cost of a typical report for the baseline

Type	Number of reports	Proportion	Time per average report (public authorities, hours)	Cost per average report (public authorities)	Time per average report (service providers, hours)	Cost per average report (service providers)
Known CSAM	1,740,293	87.59%	2	€80.92	0.75	€36.90
New CSAM	198,537	12.38%	4	€184.78	1	€49.25
Grooming	725	0.03%	4	€184.78	1.5	€73.88
Total	**1,939,556**	**100.00%**	**2.25**	**€103.86**	**0.78**	**€38.48**

4) Total continuous costs.

The total continuous costs were calculated as the product of the total time and the salaries indicated above.

Table5 summarises the calculations of the continuous costs per year for the baseline:

Table 5: Calculation of continuous costs per year for the baseline

	Public authorities	Service providers
Cost per average report	€103.86	€38.48
Annual reports (average)	1,357,689	1,939,556
Annual costs	**€141,016,361**	**€74,627,445**

Measure 1: Practical measures to enhance voluntary efforts

1) One-off costs.

Public authorities:

- Development of standard code of conduct:
  - 250 working hours.
  - The development of a standard code of conduct requires consultation between public authorities and service providers in order to conceive, develop and validate a draft code.
- Development of standardised reporting forms:
  - 50 working hours.
  - The development of standardised reporting forms requires consultation between public authorities and service providers in order to determine the appropriate standard based upon data required by law enforcement for reports to be actionable and processed efficiently, and the data that is available from providers.
- Development of improved feedback mechanisms:
  - 250 working hours.
  - The development of improved feedback mechanisms requires consultation between public authorities and service providers in order to determine the nature of information necessary to enable providers to improve and maintain

quality of reporting, while ensuring the information provided is limited to what is feasible and strictly appropriate.

- Development of improved communication channels:
  - 30 working days × 27 Member States
  - The setting up of a single point of contact system and ensuring appropriate security for communication channels requires conceiving, validating and implementing such a system for the whole Member State, involving multiple actors.
  - Costs may differ depending on the nature of the system established. 30 working days is taken to represent an average figure.
- Development and integration of APIs to allow for remote checking against hash databases:
  - 100 000 EUR development cost for API; and
  - 5 working days × 5 Member States
  - Due to the complexity of establishing and maintaining databases of hashes, and the likely redundancy for providers of maintaining API connections to multiple databases, it is assumed that a small number of Member States would integrate such an API.

The total one-off costs to EU and Member States' public authorities under this measure are **EUR 433 990**.

Service providers:

- Development of standard code of conduct:
  - 5 working hours × 10 service providers
  - As the adoption of a standard code of conduct is a voluntary measure, and the vast majority of reports of CSA online are currently made by a small number of service providers, it is estimated that consultations on the development of a code would involve a small number of providers, including both small and large companies.
  - Training and implementation of the finalised code is assumed to be a part of service providers' ordinary activities, not incurring any additional costs.
- Development of standardised reporting forms:
  - 5 working hours × top 10 service providers
  - As the vast majority of reports of CSA online from service providers are currently made by a small number of providers, consultations on development of standardised reporting forms can be most effective by focusing on the providers that are most active in this area in order to determine the information that can and should be included in reports in order to ensure that they are actionable for law enforcement authorities.
- Development of improved feedback mechanisms:
  - 5 working hours × top 10 service providers
  - Consultations on the development of improved feedback mechanisms can be most effective by focusing on the providers that are most active in this area in

order to determine the information gaps which currently prevent providers from improving the quality of their reports.

- Development of improved communication channels:
  - 30 working days × top 10 service providers
  - As this is a voluntary measure, the development of improved communication channels is likely to be of most interest to the providers making the largest numbers of reports of CSA online.
  - The setting up of a single point of contact system and ensuring appropriate security for communication channels requires conceiving, validating and implementing such a system, involving multiple actors.
  - Costs may differ depending on the nature of the system established. 30 working days is taken to represent an average figure.
- Development and integration of APIs to allow for remote checking against hash databases:
  - 5 working days × 50 service providers
  - Due to the complexity of establishing and maintaining databases of hashes, a significant number of service providers are expected to have an interest in the integration of APIs to allow for remote checking against hash databases operated by public authorities.

The total one-off costs to service providers under this measure are **224 088 EUR**.

2) Time per report.

Known CSAM, new CSAM, and solicitation:

- -5% in relation to the baseline.
- Decreased cost per report for all types of CSA online due to improved efficiencies as a result of initiatives under this measure.

3) Total number of reports.

Known and new CSAM:

- +10% in relation to the baseline.
- Increased detection, reporting and removal of both known and new CSAM by relevant online service providers due to increase in voluntary activities as a result of initiatives under this measure.

Solicitation:

- +20% in relation to the baseline.
- Increased detection and reporting of solicitation by relevant online service providers due to:
  - increase in voluntary activities as a result of initiatives under this measure;
  - current low level of adoption of relevant technologies.

Table below summarises the above modifiers for this measure. Table summarises the resulting changes to a typical report.

Table 6: Summary of modifiers under Measure 1

	Known CSAM	New CSAM	Grooming
Time per report (hours)	-5%	-5%	-5%
Annual reports (average)	10%	10%	20%

Table 7: Composition, time and cost of a typical report under Measure 1

Type	Number of Reports	Proportion	Time per average report (public authorities, hours)	Cost per average report (public authorities)	Time per average report (service providers, hours)	Cost per average report (service providers)
Known CSAM	1,914,323	89.72%	1,90	€87.77	0,71	€35.09
New CSAM	218,391	10.24%	3,80	€175.54	0,95	€46.79
Grooming	870	0.04%	3,80	€175.54	1,43	€70.18
Total	**2,133,584**	**100%**	**2.10**	**€96.79**	**0.74**	**€36.30**

4) Total continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above.

Table below summarises the calculations of the total continuous costs per year under Measure 1.

Table 8: Calculation of continuous costs per year under Measure 1

	Public authorities	Service providers
Cost per average report	€96,79	€36,30
Annual reports (average)	1.493.509	2.133.584
Annual costs	€144.557.486	€77.453.822
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€3,541,125**	**€2,826,377**

Measure 2: EU Centre on prevention and assistance to victims

The quantitative assessment of this policy measure is described in detail in Annex 10.

Measure 3: EU Centre on prevention and assistance to victims and to combat CSA online

The quantitative assessment of this policy measure is described in detail in Annex 10.

Measure 4: Legislation specifying the conditions for voluntary detection of online child sexual abuse

1) One-off costs.

Public authorities:

- Development of legislation:
    - The one-off costs to public authorities in this measure concern the development of legislation specifying the conditions for voluntary detection of child sexual abuse online. Assuming that the instrument would be a Regulation, it would not require transposition by the Member States. However some adaptations of national law may be needed to make it compliant with the instrument. In any case, it is assumed that these possible costs of developing the legislation and eventually implement it at national level would be absorbed by existing budget and under the existing resources in public authorities.

Service providers:

- Infrastructure for the detection of online child sexual abuse:
    - +3 460 (+10%) service providers implementing voluntary measures;
    - 30 working days typically required to implement voluntary measures.
    - 2 working days to train content moderators on detection of known CSAM, 4 days for new CSAM and 5 days for grooming.

The total one-off costs to service providers under this measure are **EUR 137 687 240**.

2) Time per report.

There are no changes to the time per report under this Measure.

3) Total number of reports.

Known CSAM, new CSAM, and solicitation:

- +10% in relation to the baseline.
- Increased detection, reporting and removal of all forms of CSA online by relevant online service providers due to increase in voluntary activities as a result of the increased legal certainty regarding processing activities as a result of this measure.
- Where this Measure is included in Policy Options which also include Measures 6, 7, or 8, costs under this measure relating to voluntary detection of types of online child sexual covered by those measures are omitted for the service providers subject to detection orders, as voluntary detection is redundant in that scenario.

Table below summarises the above modifiers for this measure.
Table 10 summarises the resulting changes to a typical report. €

Table 9: Summary of modifiers under Measure 4

	Known CSAM	New CSAM	Grooming
Time per report (hours)	0%	0%	0%
Annual reports (average)	10%	10%	10%

Table 10: Composition, time and cost of a typical report under Measure 4

Type	Number of Reports	Proportion	Time per average report (public authorities, hours)	Cost per average report (public authorities)	Time per average report (service providers, hours)	Cost per average report (service providers)
Known CSAM	1,914,323	89.73%	2,00	€92,39	0,75	€36,94
New CSAM	218,391	10.24%	4,00	€184,78	1,00	€49,25
Grooming	798	0.04%	4,00	€184,78	1,50	€73,88
Total	**2,133,512**	**100.00%**	**2,21**	**€101,88**	**0,78**	**€38,21**

4) Total continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above.

Table 11 summarises the calculations of the total continuous costs per year under this Measure.

Table 11: Calculation of continuous costs per year under Measure 4

	Public authorities	Service providers
Cost per average report	€101.88	€38.21
Annual reports (average)	1,493,458	2,133,512
Annual costs	€152,156,397	€81,524,982
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€11,140,035**	**€6,897,538**

Measure 5: Legal obligation to report and remove all types of online CSA

1) One-off costs.

Public authorities:

- Development of legislation:
  - The one-off costs to public authorities in this measure concern the development of legislation establishing an obligation to report and remove all types of child sexual abuse online. Assuming that the instrument would be a Regulation, it would not require transposition by the Member States. However some adaptations of national law may be needed to make it compliant with the instrument. In any case, it is assumed that these possible costs of developing

the legislation and eventually implement it at national level would be absorbed by existing budget and under the existing resources in public authorities.

Service providers:

- Infrastructure for the reporting and removal of online child sexual abuse:
  - +346 (+10%) service providers implementing additional infrastructure for reporting and removal;
  - It is assumed that the majority of service providers have in place infrastructure that allows them to report instances of CSA online, and remove them once they have become aware.
  - It is therefore assumed that the cost to put in place the necessary infrastructure for reporting and removal would be the equivalent of 15 working days for 10% of the total number of providers concerned by CSA online (€49.25/hour x 3460 providers x 120 h/provider).

The total one-off costs to service providers under this measure are **EUR 20 448 600**.

2) Time per report.

There are no changes to the time per report under this Measure.

3) Total number of reports.

Known CSAM, new CSAM, and solicitation:

- +1% in relation to the baseline.
- Slightly increased detection, reporting and removal of all forms of CSA online by relevant online service providers due to increase in voluntary activities as a result of the increased legal certainty regarding processing activities as a result of this measure.
- It is assumed that, where relevant online service providers carry out voluntary detection and removal of CSA online, the overwhelming majority of those providers will make reports on a voluntary basis, leading to only a slight increase under this measure.

Table 12 below summarises the above modifiers for this measure. Table 3 summarises the resulting changes to a typical report.

Table 12: Summary of modifiers under Measure 5

	Known CSAM	**New CSAM**	**Grooming**
Time per report (hours)	0%	0%	0%
Annual reports (average)	3%	3%	3%

Table 13: Composition, time and cost of a typical report under Measure 5

Type	Number of Reports	Proportion	Time per average report (public authorities, hours)	Cost per average report (public authorities)	Time per average report (service providers, hours)	Cost per average report (service providers)
Known CSAM	1,792,502	89.73%	2,00	€92,40	0,75	€36,94
New CSAM	204,494	10.24%	4,00	€184,80	1,00	€49,25
Grooming	747	0.037%	4,00	€184,80	1,50	€73,88
Total	1,997,743	**100.00%**	**2.21**	**€101.89**	**0.78**	**€38.21**

4) Change in continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above.

Table 4 summarises the calculations of the total continuous costs per year under this Measure.

Table 14: Calculation of continuous costs per year under Measure 5

	Public authorities	Service providers
Cost per average report	€101.89	€38.21
Annual reports (average)	1.415.876	1.997.743
Annual costs	€144,267,579	€76,337,029
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€3,251,217**	**€1,709,584**

Measure 6: Legal obligation to detect known CSAM

1) One-off costs.

Public authorities:

- Development of legislation:
  - The one-off costs in this measure concern the development of legislation establishing a legal obligation for relevant online service providers to detect known child sexual abuse material. Assuming that the instrument would be a Regulation, it would not require transposition by the Member States. However some adaptations of national law may be needed to make it compliant with the instrument. In any case, it is assumed that these possible costs of developing the legislation and eventually implement it at national level would be absorbed by existing budget and under the existing resources in public authorities.
  - Development and integration of tools to detect known CSAM regardless of the technology used in the online exchanges (e.g. in E2EE environments):
    - The one-off costs for public authorities include contributing to the development of those tools. The tools should ideally be developed in

partnership with service providers and be at par with solutions used to detect child sexual abuse in un-encrypted environments in terms of effectiveness, and safeguard fundamental rights, including privacy and data protection.

Service providers

The one-off costs for service providers include the following:

- implementation of infrastructure for the detection of known CSAM (120 hours/year for each of the 34 600 providers concerned);
- development of technical solutions that allows companies to detect child sexual abuse regardless of the technology used in the online exchanges (e.g. encryption). The solution should ideally be developed in partnership with public authorities, and should be tailored to the company's existing services, fit within their business model and be at par with solutions used to detect child sexual abuse in un-encrypted environments and safeguard fundamental rights, including privacy and data protection (10% of the above);
- additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (€5 million per provider);
- training for the providers' content moderators in order to appropriately deal with content flagged as known CSAM (16 hours/year for each of the 34 600 providers);

The total one-off costs to service providers under this measure are **EUR 352 199 400**.

Table 15: Summary of one-off costs under Measure 6

Description	Public Authorities	Service Providers
Integration of infrastructure to detect known CSAM	€0	€204,486,000
Integration of infrastructure to detect known CSAM (top 20 providers)	€0	€100,000,000
Integration of tools to detect known CSAM regardless of the technology used in the online exchanges	€0	€20.448.600
Training of content moderators	€0	€27,264,800
Total	**€0**	**€352,199,400**

2) Time per report.

There are no changes to the time per report under this Measure.

3) Total number of reports.

Known CSAM

- To estimate the number of reports, the model assumes that under the obligation to detect known CSAM, the maximum number of reports containing known CSAM would be reached.

- To estimate this maximum number, the model considers the maximum number of reports that could be achieved under all the obligations in the initiative, 8.8 million (see "How the model works" section).
- Under this scenario, the proportion of reports of new CSAM (18%) and grooming (2%) would increase in relation to the current situation and the baseline (10.24% and 0.04% respectively), which are assumed to increase significantly due to the less extended deployment of technologies for their detection at present compared to known CSAM.
- This means that the total maximum number of reports containing known CSAM would be 80% of 8.8 million (7.1 million). As discussed previously, the model assumes that each report contains just one type of CSA online.

Table 16: distribution of reports under the baseline and all detection obligations scenarios

	Baseline	All detection obligations combined
Known	89.73%	80%
New	10.24%	18%
Grooming	0.04%	2%

Table 17 below summarises the above modifiers for this measure.

Table 17: Summary of modifiers under Measure 6

	Known CSAM	**New CSAM**	**Grooming**
Time per report (hours)	0%	0%	0%
Annual reports (average)	7.1 million in total	0%	0%

Due to the greater clarity and stricter legal rules regarding the detection of known CSAM under this Measure, it is assumed that the number of non-actionable reports made by providers is reduced by **5%** (instead of by 30% under voluntary reporting). For new CSAM and grooming the situation would remain the same in relation to non-actionable reports (i.e. 30%).

The large increase in the number of reports of known CSAM under this measure, while the number of reports of new CSAM and grooming is unaffected, results in a significant change to the composition of the average report. Table8 summarises the resulting changes to the average report:

Table 18: Composition, time and cost of an average report under Measure 6

Type	**Public authorities**				**Service providers**			
	Number of Reports	**Proportion**	**Time per average report**	**Cost per average report**	**Number of Reports**	**Proportion**	**Time per average report**	**Cost per average report**

			(hours)				(hours)	
Known CSAM	6,697,736	97.96%	2.00	92.40	7,050,249	97.25%	0.75	36.94
New CSAM	138,976	2.03%	4.00	184.80	198,537	2.74%	1.00	49.25
Grooming	508	0.01%	4.00	184.80	725	0.01%	1.50	73.88
Total	**6,837,220**	**100%**	**2.04**	**94.29**	**7,249,511**	**100%**	**0.76**	**37.28**

4) Change in continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above.

In addition, continuous cost also include those of operating and maintaining the infrastructure and technologies to detect known CSAM, including:

- Costs for all the providers concerned by this measure (40 hours/year for each of the 34 600 providers);
- Additional costs related to the maintenance and rolling development costs of technical solutions that allows for detection of CSA online regardless of the technology used in the online exchanges (10% of the above);
- Additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (1h per day = 24*365 = 8760 hours/year, at an increased hourly rate of €1000).
- Training of content moderators (8h per year).

Table 19 summarises the calculations of the total continuous costs per year under this Measure.

Table 19: Calculation of continuous costs per year under Measure 6

Description	Public Authorities	Service Providers
Cost per average report	€94.29	€37.28
Annual reports (average)	6,837,220	7,249,511
Detection costs	€644,647,419	€270,250,104
Operation/maintenance of infrastructure to detect known CSAM	€0	€68,162,000
Operation/maintenance of infrastructure to detect known CSAM regardless of the technology used in the online exchanges	€0	€6,816,200
Operation/maintenance of infrastructure to detect known CSAM (top 20 providers)	€0	€175,200,000
Training of content moderators	€0	€13,632,400
Total	€644,647,419	€534,060,690
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€503,631,058**	**€459,433,246**

Measure 7: Legal obligation to detect new CSAM

1) One-off costs.

Public authorities:

- Development of legislation:
    - The one-off costs to public authorities in this measure concern the development of legislation establishing a legal obligation for relevant online service providers to detect, report and remove previously-unknown child sexual abuse material. Assuming that the instrument would be a Regulation, it would not require transposition by the Member States. However some adaptations of national law may be needed to make it compliant with the instrument. In any case, it is assumed that these possible costs of developing the legislation and eventually implement it at national level would be absorbed by existing budget and under the existing resources in public authorities.
    - Development and integration of tools to detect new CSAM regardless of the technology used in the online exchanges (e.g. in E2EE environments):
        - The one-off costs for public authorities include contributing to the development of those tools. The tools should ideally be developed in partnership with service providers and be at par with solutions used to detect child sexual abuse in un-encrypted environments in terms of effectiveness, and safeguard fundamental rights, including privacy and data protection.

The one-off costs for service providers include the following:

- implementation of infrastructure for the detection of new CSAM (240 hours/year for each of the 34 600 providers concerned);
- development of technical solutions that allows companies to detect child sexual abuse regardless of the technology used in the online exchanges (e.g. encryption). The solution should ideally be developed in partnership with public authorities, and should be tailored to the company's existing services, fit within their business model and be at par with solutions used to detect child sexual abuse in un-encrypted environments and safeguard fundamental rights, including privacy and data protection (10% of the above);
- additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (€5 million per provider);
- training for the providers' content moderators in order to appropriately deal with content flagged as known CSAM (32 hours/year for each of the 34 600 providers);

The total one-off costs to service providers under this measure are **EUR 604 398 800**.

Table 20: Summary of one-off costs under Measure 7

Description	Public Authorities	Service Providers
Integration of infrastructure to detect new CSAM	€0	€408,972,000
Integration of infrastructure to detect new CSAM (top 20 providers)	€0	€100,000,00

Integration of tools to detect new CSAM regardless of the technology used in the online exchanges	€0	€40.897.200
Training of content moderators	€0	€54,529,600
Total	**€0**	**€604,398,800**

2) Time per report.

There are no changes to the time per report under this Measure.

3) Total number of reports.

New CSAM

- To estimate the number of reports, following the same logic as in Measure 6, the model assumes that under the obligation to detect new CSAM, the maximum number of reports containing new CSAM would be reached.
- To estimate this maximum number, the model considers the maximum number of reports that could be achieved under all the obligations in the initiative, 8.8 million (see "How the model works" section).
- Under this scenario, the proportion of reports of new CSAM (18%) and grooming (2%) would increase in relation to the current situation and the baseline (10.24% and 0.04% respectively), which are assumed to increase significantly due to the less extended deployment of technologies for their detection at present compared to known CSAM.
- This means that the total maximum number of reports containing new CSAM would be 18% of 8.8 million (1.6 million).

Table 21 below summarises the above modifiers for this measure.

Table 21: Summary of modifiers under Measure 7

	Known CSAM	**New CSAM**	**Grooming**
Time per report (hours)	0%	0%	0%
Annual reports (average)	0%	1.6 million in total	0%

Due to the greater clarity and stricter legal rules regarding the detection of new CSAM under this Measure, it is assumed that the number of non-actionable reports made by providers is reduced by **5%** (instead of by 30% under voluntary reporting). For known CSAM and grooming the situation would remain the same in relation to non-actionable reports (i.e. 30%).

The increase in the number of reports of new CSAM under this measure, while the number of reports of known CSAM and grooming is unaffected, results in a change to the composition of the average report. Table22 summarises the resulting changes to the average report:

Table 22: Composition, time and cost of an average report under Measure 7

Type	Public authorities				Service providers			
	Number of Reports	Proportion	Time per average report (hours)	Cost per average report	Number of Reports	Proportion	Time per average report (hours)	Cost per average report
Known CSAM	1,218,205	44.69%	2.00	€92.40	1,740,293	52.30%	0.75	€36.94
New CSAM	1,506,991	55.29%	4.00	€184.80	1,586,306	47.68%	1.00	€49.25
Grooming	508	0.02%	4.00	€184.80	725	0.02%	1.50	€73.88
Total	**2,725,704**	**100%**	**3.11**	**€143.5**	**3,327,324**	**100%**	**0.87**	**€42.82**

4) Change in continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above. The same considerations as those of Measure 6 apply, with the following changes:

- Additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (1h per day = 24*365 = 8760 hours/year, at an increased hourly rate of **€2000**).
- Training of content moderators (**16h** per year).

Table 23 summarises the calculations of the total continuous costs per year under this Measure.

Table 23: Calculation of continuous costs per year under Measure 7

Description	Public Authorities	Service Providers
Cost per average report	€143.5	€42.82
Annual reports (average)	2,725,704	3,327,324
Detection costs	€391,147,842	€142,461,219
Operation/maintenance of infrastructure to detect new CSAM	€0	€68,162,000
Operation/maintenance of infrastructure to detect new CSAM regardless of the technology used in the online exchanges	€0	€6,816,200
Operation/maintenance of infrastructure to detect new CSAM (top 20 providers)	€0	€350,400,000
Training of content moderators	€0	€27,264,800
Total	€391,147,842	€595,104,219
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€250,131,481**	**€520,476,775**

Measure 8: Legal obligation to detect grooming

1) One-off costs.

Public authorities:

- Development of legislation:
    - The one-off costs to public authorities in this measure concern the development of legislation establishing a legal obligation for relevant online service providers to detect, report and remove previously-unknown child sexual abuse material. Assuming that the instrument would be a Regulation, it would not require transposition by the Member States. However some adaptations of national law may be needed to make it compliant with the instrument. In any case, it is assumed that these possible costs of developing the legislation and eventually implement it at national level would be absorbed by existing budget and under the existing resources in public authorities.
    - Development and integration of tools to detect grooming regardless of the technology used in the online exchanges (e.g. in E2EE environments):
        - The one-off costs for public authorities include contributing to the development of those tools. The tools should ideally be developed in partnership with service providers and be at par with solutions used to detect child sexual abuse in un-encrypted environments in terms of effectiveness, and safeguard fundamental rights, including privacy and data protection.

Service providers:

The one-off costs for service providers include the following:

- implementation of infrastructure for the detection of grooming (240 hours/year for each of the 34 600 providers concerned);
- development of technical solutions that allows companies to detect child sexual abuse regardless of the technology used in the online exchanges (e.g. encryption). The solution should ideally be developed in partnership with public authorities, and should be tailored to the company's existing services, fit within their business model and be at par with solutions used to detect child sexual abuse in un-encrypted environments and safeguard fundamental rights, including privacy and data protection (10% of the above);
- additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (€5 million per provider);
- training for the providers' content moderators in order to appropriately deal with content flagged as known CSAM (40 hours/year for each of the 34 600 providers);

The total one-off costs to service providers under this measure are **EUR 618 031 200**.

Table 24: Summary of one-off costs under Measure 8

Description	Public Authorities	Service Providers
Integration of infrastructure to detect grooming	€0	€408,972,000
Integration of infrastructure to detect grooming (top 20 providers)	€0	€100,000,00
Integration of tools to detect grooming regardless of the technology used in the online exchanges	€0	€40.897.200
Training of content moderators	€0	€68,162,000
Total	**€0**	**€618,031,200**

2) Time per report.

There are no changes to the time per report under this Measure.

3) Total number of reports.

Grooming

- To estimate the number of reports, following the same logic as in Measure 6, the model assumes that under the obligation to detect grooming, the maximum number of reports containing grooming would be reached.
- To estimate this maximum number, the model considers the maximum number of reports that could be achieved under all the obligations in the initiative, 8.8 million (see "How the model works" section).
- Under this scenario, the proportion of reports of new CSAM (18%) and grooming (2%) would increase in relation to the current situation and the baseline (10.24% and 0.04% respectively), which are assumed to increase significantly due to the less extended deployment of technologies for their detection at present compared to known CSAM.
- This means that the total maximum number of reports containing grooming would be 2% of 8.8 million (around 176 000).

Table 25 below summarises the above modifiers for this measure.

Table 25: Summary of modifiers under Measure 8

	Known CSAM	New CSAM	Grooming
Time per report (hours)	0%	0%	0%
Annual reports (average)	0%	0%	176 256 in total

Due to the greater clarity and stricter legal rules regarding the detection of grooming under this measure, it is assumed that the number of non-actionable reports made by providers is reduced by **5%** (instead of by 30% under voluntary reporting). For known and new CSAM the situation would remain the same in relation to non-actionable reports (i.e. 30%).

The increase in the number of reports of grooming under this measure, while the number of reports of known and new CSAM is unaffected, results in a change to the composition of the average report. Table 26 summarises the resulting changes to the average report:

Table 26: Composition, time and cost of an average report under Measure 8

Type	Public authorities				Service providers			
	Number of Reports	Proportion	Time per average report (hours)	Cost per average report	Number of Reports	Proportion	Time per average report (hours)	Cost per average report
Known CSAM	1,218,205	79.90%	2.00	€92.40	1,740,293	82.28%	0.75	€36.94
New CSAM	138,976	9.12%	4.00	€184.80	198,537	9.39%	1.00	€49.25
Grooming	167,443	10.98%	4.00	€184.80	176,256	8.33%	1.50	€73.88
Total	**1,524,625**	**100%**	**2.40**	**€110.97**	**2,115,087**	**100%**	**0.84**	**€41.17**

4) Change in continuous costs.

The change in continuous costs was calculated as the product of the increase in annual reports and the costs per report indicated above. The same considerations as those of Measure 6 apply, with the following changes:

- Additional costs for the top 20 largest providers, derived from the need to ensure interoperability of different platforms, and additional costs due to the larger user base and/or volume of online exchanges (1h per day = 24*365 = 8760 hours/year, at an increased hourly rate of **€2000**).
- Training of content moderators (**20h** per year).

Table 27 summarises the calculations of the total continuous costs per year under this Measure.

Table 27: Calculation of continuous costs per year under Measure 8

Description	Public Authorities	Service Providers
Cost per average report	€110.97	€41.17
Annual reports (average)	1,524,625	2,115,087
Detection costs	€169,188,523	€87,080,985
Operation/maintenance of infrastructure to detect grooming	€0	€68,162,000
Operation/maintenance of infrastructure to detect new CSAM regardless of the technology used in the online exchanges	€0	€6,816,200
Operation/maintenance of infrastructure to detect grooming (top 20 providers)	€0	€350,400,000
Training of content moderators	€0	€34,081,000
Total	€169,188,523	€546,540,185
Annual costs (baseline)	€141,016,361	€74,627,445
Net annual costs	**€28,172,162**	**€471,912,741**

4. Quantitative assessment of policy options

Calculation of the cost estimates for each policy option

Given the cumulative nature of the options, the total costs are the sum of the costs of each of the measures. For options C, D and E, which combine voluntary and mandatory detection, the model takes into account the synergies between measures 4 and 6, 7 and 8 respectively, to consider either the costs of voluntary measures or mandatory depending on the option.

Option A: practical measures to enhance prevention, detection, reporting and removal, and assistance to victims, and establishing an EU Centre on prevention and assistance to victims

Table 28: Calculation of total costs under Option A

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0.4	€0.2	€3.5	€2.8
2	€0.0	€0.0	€10.3	€0.0
Total	€0.4	€0.2	€13.9	€2.0

Option B: option A + legislation 1) specifying the conditions for voluntary detection, 2) requiring mandatory reporting and removal of online child sexual abuse, and 3) expanding the EU Centre to also support detection, reporting and removal

Table 29: Calculation of total costs under Option B

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0.4	€0.2	€3.5	€2.8
3	€5.0	€0.0	€25.7	€0.0
4	€0.0	€137.7	€11.1	€6.9
5	€0.0	€20.4	€3.3	€1.7
Total	**€5.4**	**€158.4**	**€43.6**	**€11.4**

Option C: option B + mandatory detection of known CSAM

In this option, a number of service provider will be subject to mandatory detection of known CSAM. Therefore, the one-off costs of voluntary detection of known CSAM under measure 4 should be deducted (i.e. training of content moderators and integration of infrastructure to detect known CSAM). These are taken into account in measure 4*.

The continuous costs would eventually be lower than the combination of measures 4 and 6 but they have been left in the calculations to maintain a conservative estimates of the costs. This also allows taking into account the transition period before the detection order is imposed on the service provider, during which it may choose to start or continue detecting voluntarily.

Table 30: Calculation of total costs under Option C

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0.4	€0.2	€3.5	€2.8
3	€5.0	€0.0	€25.7	€0.0
4*	€0.0	€94.1	€11.1	€6.9
5	€0.0	€20.4	€3.3	€1.7
6	€0.0	€352.2	€503.6	€459.4
Total	**€5.4**	**€466.9**	**€547.3**	**€470.9**

Option D: option C + mandatory detection of new CSAM

The same considerations in relation to **one-off costs** under measure 4 made in option C apply. In this case, measure 4** should exclude the one-off costs related to training of content moderators and integration of infrastructure to detect new CSAM, in addition to those of known CSAM. Therefore, the only one-off costs under measure 4** are those related to training of content moderators and integration of infrastructure to detect grooming on a voluntary basis. The same considerations in relation to **continuous costs** under measure 4 made in option C apply.

Table 31: Calculation of total costs under Option D

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0.4	€0.2	€3.5	€2.8
3	€5.0	€0.0	€25.7	€0.0
4**	€0.0	€47.7	€11.1	€6.9
5	€0.0	€20.4	€3.3	€1.7
6	€0.0	€352.2	€503.6	€459.4
7	€0.0	€604.4	€250.1	€520.5
Total	**€5.4**	**€1,025.0**	**€797.4**	**€991.3**

Option E: option D + mandatory detection of grooming

The same considerations in relation to **one-off costs** under measure 4 made in option C apply. In this case, there would not be one-off costs, since those are included in the mandatory measures to detect known and new CSAM and grooming. The same considerations in relation to **continuous costs** under measure 4 made in option C apply.

Table 32: Calculation of total costs under Option E

POLICY MEASURES	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS	
	Public Authorities	Service Providers	Public Authorities	Service Providers
1	€0.4	€0.2	€3.5	€2.8
3	€5.0	€0.0	€25.7	€0.0
4* **	€0.0	€90.0	€11.1	€6.9
5	€0.0	€20.4	€3.3	€1.7
6	€0.0	€352.2	€503.6	€459.4
7	€0.0	€604.4	€250.1	€520.5
8	€0.0	€618.0	€28.2	€471.9
Total	**€5.4**	**€1,595.3**	**€825.6**	**€1,463.3**

Calculation of the benefit estimates for each policy option

As discussed in the benefits section in the main report, the total costs of child sexual abuse in the EU are **EUR 13.5 billion**.

This estimate is derived from a paper which estimated the total economic burden of child sexual abuse in the United States, which appeared in the peer-reviewed journal Child Abuse & Neglect[356]. The paper estimates total costs including health care costs, productivity losses, child welfare costs, violence/crime costs, and special education costs, based on secondary data drawn from peer-reviewed journals.

Regrettably, similar studies relating to the EU do not appear to have been published to date. However, studies on the economic cost of violence against children (including child sexual abuse) suggest that costs are comparable among high-income countries[357]. Therefore the estimates provided in the above-mentioned paper are assumed to be applicable in the EU context, when adjusted to take account of the differences between the sizes of the US and EU populations.

The benefits derive from savings as a result of **CSA associated costs**, i.e. savings relating to offenders (e.g. criminal proceedings), savings relating to victims (e.g. short and long-term assistance), and savings relating to society at large (e.g. productivity losses).

[356] Letourneau et al., The economic burden of child sexual abuse in the United States, May 2018.
[357] See, for example Ferrara, P. et al., The Economic Burden of Child Maltreatment in High Income Countries, December 2015.

The calculation of benefits assumes that there is a direct correlation between the only factor that can be quantified, the increase in reports[358], and the estimated savings. Specifically, the model assumed a cost decrease of 25% for option E (highest number of reports) and applied the same ratio of increase in reporting vs decrease in costs from option E to the other options.

To calculate the number of reports under each option, the following was taken into account:

- Option A (measures 1 + 2): the number of reports for this option is the same one as in measure 1, since measure 2 (EU Centre on prevention and assistance to victims) would not lead per se to an increase in the number of reports.
- Option B (measures 1+3+4+5): the number of reports for this option is those of measure 1 + net number of reports in measures 4 and 5 (i.e. number of reports in the measure minus those of the baseline). Measure 3 on the fully fledged EU Centre, would not lead per se to an increase in the number of reports.
- Option C (measures 1+3+4+5+6): the number of reports for this option is those of option B + the number of reports of known material under measure 6 on mandatory detection minus the number of reports for known material under measure 4 on voluntary detection).
- Option D (measures 1+3+4+5+6+7): the number of reports for this option is those of option C + the number of reports of new material under measure 7 on mandatory detection minus the number of reports for new material under measure 4 on voluntary detection and measure 6 under which detection of new CSAM is also voluntary).
- Option E (measures 1+3+4+5+6+7+8): the number of reports for this option is the potential number of reports that could be detected as described in table 1 on section 3 of this annex, "How the model works".

Costs over 10 years

For the purpose of comparing the options and calculating overall costs, the total combined cost (not discounted) to service providers and public authorities over a period of 10 years (2021-2030) was considered (equal to one-off costs + 10 x annual costs for both public authorities and service providers combined):

[358] For simplicity in the internal calculations the model uses the number of reports from service providers rather than the number of reports reaching public authorities. This has no impact on the comparison of options.

Table 33: total costs over 10 years

POLICY OPTIONS	ONE-OFF COSTS		CONTINUOUS (ANNUAL) COSTS		10 years
	Public Authorities	Service Providers	Public Authorities	Service Providers	
A	€0,4	€0,2	€13,9	€2,8	€167,5
B	€5,4	€158,4	€43,6	€11,4	€714,5
C	€5,4	€466,9	€547,3	€470,9	€10.653,7
D	€5,4	€1.025,0	€797,4	€991,3	€18.917,8
E	€5,4	€1.595,3	€825,6	€1.463,3	€24.489,0

Sensitivity analysis

As explained in the report, it would be safe to estimate that the quantitative benefits could be up to 50% of the annual costs of the CSA in the EU (considering that the amount of EUR 13.8 billion was a conservative estimate). And it would be even safer to assume that the benefits could be 25% of the annual costs of CSA in the EU. For comparison purposes, it seems useful to conduct a sensitivity analysis to determine how the benefits would change under various assumptions of decrease of annual costs of CSA in the EU: 50%, 40%, 30%, 20%, 10% and 5%.

Table 34: estimated annual benefits for the policy options (EUR billion)
50% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	1%	0,18 €
B	23%	3%	0,38 €
C	288%	41%	4,54 €
D	348%	49%	4,88 €
E	354%	50%	4,45 €

Table 35: estimated annual benefits for the policy options (EUR billion)
40% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	1%	0,14 €
B	23%	3%	0,29 €
C	288%	32%	3,42 €
D	348%	39%	3,53 €
E	354%	40%	3,07 €

Table 36: estimated annual benefits for the policy options (EUR billion)
30% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	1%	0,10 €
B	23%	2%	0,20 €
C	288%	24%	2,29 €
D	348%	29%	2,17 €
E	354%	30%	1,69 €

Table 37: estimated annual benefits for the policy options (EUR billion)
20% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	1%	0,05 €
B	23%	1%	0,09 €
C	288%	15%	0,99 €
D	348%	18%	0,59 €
E	354%	20%	0,31 €

Table 38: estimated annual benefits for the policy options (EUR billion)
15% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	0,4%	0,04 €
B	23%	1,0%	0,06 €
C	288%	12%	0,61 €
D	348%	15%	0,14 €
E	354%	15%	- 0,38 €

Table 39: estimated annual benefits for the policy options (EUR billion)
10% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	0,3%	0,02 €
B	23%	1%	0,02 €
C	288%	8%	0,05 €
D	348%	10%	-0,54 €
E	354%	10%	-1,07 €

Table 40: estimated annual benefits for the policy options (EUR billion)
5% decrease in annual CSA costs

POLICY OPTIONS	Estimated increase in reporting (%)	Estimated cost reduction	Benefits (billions per year)
A	10%	0,1%	0,00 €
B	23%	0,3%	-0,03 €
C	288%	4,1%	-0,51 €
D	348%	5%	-1,21 €
E	354%	5%	-1,76 €

From the above sensitivity analysis it is possible to determine the minimum decrease in annual CSA costs so that a given option produces net benefits:

Table 41: minimum % decrease in total annual CSA costs to generate net benefits in each policy option

A	0,13%
B	0,6%
C	8%
D	14%
E	18%

ANNEX 5: RELEVANT LEGISLATION AND POLICIES

The following legislative instruments and policies at EU, national and international level, are relevant for fighting against child sexual abuse (online and offline):

1. EU law

- **EU Charter of Fundamental Rights**[359], which recognises that children have the right to such protection and care as is necessary for their well-being, among other provisions.
  - **EU data protection and privacy legislation:**

  The legislation resulting from the data protection reform[360] is of critical importance in the fight against child sexual abuse online:
    - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[361] (**General Data Protection Regulation, GDPR**).
    - Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data[362] (**Police Directive**).
    - The 2002 **ePrivacy Directive**[363] ensures the protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in electronic communications over public networks. In particular, the Directive requires Member States to ensure the confidentiality of communications by prohibiting and limiting the processing of traffic and location data without the consent of the user concerned, except for specific circumstances, and sets out the conditions to be met where national law restricts those rights and obligations. In January 2017 the Commission adopted a **proposal for a Regulation on Privacy and Electronic**

---

359 Charter of Fundamental Rights of the European Union of 26 October 2021, *OJ C* 326, 26.10.2012.

360 See here for more information.

361 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

362 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

363 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Communications[364] to replace the 2002 Directive. This proposal aims at enhancing the protection of rights for users of all electronic communications services and ensure protection of their terminal equipment. It will complete and further harmonise the privacy rules in the European single market and overcome fragmented implementation of the Directive. It will create a level playing field and reduce compliance cost for businesses. It also aims to enhance consistency with the General Data Protection Regulation. . It will strengthen enforcement powers. This proposal is **still under negotiation**. In 2017, the European Parliament adopted a report[365] and gave the mandate to the rapporteur to begin inter-institutional negotiations. On February 2021, the Council agreed on a negotiating mandate[366] At the time of writing, the inter-institutional negotiations between the Council the European Parliament, and Commission started on 20 May 2021.

- **EU legislation on the digital single market:**
  - The **E-commerce Directive**[367] establishes the free provision of information society services inside the EU. These services providers should be subject only to the rules applicable in their country of establishment and Member States cannot restrict the provision of such services in the coordinated field. However, this 'home state control' principle is subject to certain exceptions, including for effectively tackling criminal offences. The e-Commerce Directives also exempts, subject to certain conditions, certain online service providers from liability for user content that they transmit or store.
  - The proposed **Digital Services Act package**[368] (comprising of the proposed Digital Services Act[369] and Digital Markets Act[370]). The Digital Services Act (DSA), proposed on 15 December 2020, aims to clarify and upgrade liability and safety rules for digital services, including new procedures for faster removal of illegal content. The DSA proposes to clarify that intermediary service providers can continue to benefit from the exemptions from liability if they are conducting voluntary own initiative investigations or other activities aimed at addressing illegal content. It also proposes to require providers to establish notice and action mechanisms, prioritise reports received from

---

364 Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.

365 Report on the proposal for a Regulation of the European Parliament and of the Council concerning the Respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

366 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for Private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC - Mandate for negotiations with the European Parliament, 6087/21.

367 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L* 178, 17.7.2000, p. 1–16.

368 'The Digital Services Act package', accessed 8 April 2021.

369 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

370 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

trusted flaggers, suspend the provision of the services for users frequently providing manifestly illegal content and to promptly inform the relevant authorities if they become aware of suspicions of any serious criminal offence involving a threat to the life or safety of persons. This proposal is **still under negotiation**.

- Proposal to amend the **Europol Regulation**[371]**:** it aims at strengthening Europol's mandate among others by enabling Europol to cooperate effectively with private parties, in particular by allowing Europol to exchange data directly with private parties for purposes other than simply identifying the competent authority in Member States. It also proposes to clarify Europol's capacity to process personal data in support of financial or criminal intelligence operations and criminal investigations for crimes falling within Europol's mandate. This proposal is **still under negotiation**.
- The 2011 **Child Sexual Abuse Directive**[372], contains provisions harmonising definitions and criminal offences covering both offline and online acts. It also addresses criminal procedure, administrative and policy measures in the areas of prevention, investigation and prosecution of offences, as well as assistance to and protection of victims. As a directive aiming to harmonise criminal law, it is based on Article 82(2) and Article 83(1) of the Treaty on the Functioning of the European Union (the TFEU)[373] and is addressed to the Member States.
- The **Victims' Rights Directive**[374] ensures that all victims of crime receive appropriate information, support and protection and are able to participate in criminal proceedings. The Directive provides victims with a right to information, a right to understand and to be understood, a right to access support and protection in accordance with their individual needs, as well as with a set of procedural rights. For certain groups of victims, including child victims of sexual exploitation, there are specific rules that respond more directly to the needs of some victims, e.g. in view of protecting them from secondary victimisation, retaliation and intimidation.
- The regulation on preventing the dissemination of **terrorist content online**[375] aims to ensure that online service providers play a more active role in addressing terrorist content online. In particular, it aims at reducing accessibility to terrorist content online, in view of terrorists' misuse of the internet to groom and recruit

---

371 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM/2020/796 final

372 Directive 2011//93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *OJ L* 335, 17.12.2011.

373 Treaty establishing the European Community (Consolidated version 2002), OJ C 325, 24.12.2002, p. 33–184.

374 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, *OJ L* 315, 14.11.2012.

375 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, *OJL* 172, 17.05.2021

supporters, to prepare and facilitate terrorist activity, to glorify in their atrocities and urge others to follow suit and instil fear in the general public. The regulation creates a system of binding removal orders, with a requirement that terrorist content identified in the removal order is removed or access to it is disabled **within one hour**. It also imposes an obligation on service providers, where appropriate, to take certain specific measures to protect their services against the dissemination of terrorist content. The regulation also strengthens co-operation between national authorities and Europol to facilitate follow-up to removal orders.

- The revised **Audiovisual Media Services Directive (AVMSD)**[376] strengthens the protection of minors from harmful content and the protection of the general public from illegal content on video-sharing platforms. Concerning harmful content, the AVMSD focuses on user-generated videos which 'may impair minors' physical, mental or moral development'. Such content is allowed in on-demand services, but they may only be made available in such a way that minors will not normally hear or see them. This could be done by the use of PIN codes or other, more sophisticated age verification systems. Concerning illegal content, the AVMSD focuses on 'content the dissemination of which constitutes an activity which is a criminal offence under Union law', including offences concerning child pornography as set out in Directive 2011/93/EU.

2. EU policy

European Commission:

- The **EU strategy for a more effective fight against child sexual abuse**[377] sets out a comprehensive response to the growing threat of child sexual abuse both offline and online, which aims at improving prevention, investigation, and assistance to victims. The strategy aims to provide the EU with the right legal framework to protect children by ensuring that existing EU rules are fully implemented, and proposing new legislation where needed, particularly to clarify the role that online service providers can play to protect children. The strategy also sets out initiatives to boost coordination, including by examining the possibility to create a European Centre to prevent and counter child sexual abuse. The legislation to be proposed is one aspect of the **strategy's aim** to provide an effective response, at EU level, to the crimes of child sexual abuse.
- The **Security Union strategy**[378] focuses on three main priority areas: fighting organised crime, countering terrorism and radicalisation, and fighting crime in a digital age. The objective of the Security Union Strategy is to create a multidisciplinary, coordinated and integrated approach to security. This strategy sets out the inter-dependent strategic security priorities to be taken forward at EU

376 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, *OJ L* 303, 28.11.2018.

377 EU strategy for a more effective fight against child sexual abuse, COM(2020)607 final.

378 EU Security Union Strategy, COM(2020)605 final.

level in 2020-2024. The EU strategy for a more effective fight against child sexual abuse was adopted as one of the first deliverables of the approach taken by the Security Union Strategy.

- The Communication on **shaping Europe's digital future**[379], which notably states that the "dissemination of illegal content must be tackled as effectively online as it is offline".
- The **EU strategy on victims' rights**[380] outlines actions that will be conducted by the European Commission, Member States and civil society to ensure that all victims of all crime can fully rely on their rights. The EU Strategy on victims' rights is based on a two-strand approach: empowering victims of crime and working together for victims' rights. The Key priorities of the strategy are: (i) effective communication with victims and a safe environment for victims to report crime; (ii) improving support and protection to the most vulnerable victims; (iii) facilitating victims' access to compensation; (iv) strengthening cooperation and coordination among all relevant actors; and (v) strengthening the international dimension of victims' rights.
- **EU strategy on the rights of the child**[381] addresses persisting and emerging challenges and proposes concrete actions to protect, promote and fulfil children's rights in today's ever-changing world. The EU Strategy on the Rights of the Child includes a targeted actions across six thematic areas, each one defining the priorities for EU action. Under the thematic area Combating violence against children and ensuring child protection, the strategy announces actions to put forward a legislative proposal to combat gender-based violence against women and domestic violence, table a recommendation on the prevention of harmful practices against women and girls, and present an initiative aimed at supporting the development and strengthening of integrated child protection systems, which will encourage all relevant authorities and services to better work together.
- **Organised crime strategy**[382] sets out actions to boost law enforcement cooperation, reinforce the effectiveness of investigations on organised crime structures and high priority crimes, remove profits of organised crime and prevent infiltration into the legal economy. It also presents actions to provide a modern law enforcement response to technological developments. The Strategy is accompanied by a new Strategy on Trafficking in Human Beings.
- **The EU Strategy on Combatting Trafficking in Human Beings**[383] proposes concrete actions to identify and stop trafficking early on, to go after criminals by turning trafficking from a low-risk and high-return crime to high-risk and low-return crime, and to protect the victims and help them rebuild their lives. The majority of the victims in the EU are women and girls trafficked for sexual exploitation.

379 Shaping Europe's digital future, COM(2020)67 final
380 EU Strategy on victims' rights (2020-2025), COM(2020)528 final.
381 EU Strategy on the rights of the child, COM(2021)142 final.
382 EU Strategy to tackle Organised Crime 2021-2025, COM(2021)170 final.
383 EU Strategy on Combatting Trafficking in Human Beings, COM(2021) 171 final.

- **The EU Gender Equality Strategy**[384] presents policy objectives and actions to make significant progress by 2025 towards a gender-equal Europe. The key objectives are ending gender-based violence; challenging gender stereotypes; closing gender gaps in the labour market; achieving equal participation across different sectors of the economy; addressing the gender pay and pension gaps; closing the gender care gap and achieving gender balance in decision-making and in politics. The strategy makes a commitment to combat online violence targeting women by clarifying internet platforms' role in addressing illegal and harmful content.

As noted in section 2, this initiative responds to calls for further and concrete action made by the Council and the European Parliament.

Council of the EU. In its October 2019 conclusions on combatting the sexual abuse of children[385], the Council notably:

- reaffirmed "the EU's and Member States' **commitment** to protect the fundamental rights of children, and the rights of victims of crime, and to combat the sexual abuse and sexual exploitation of children, **both offline and online**, irrespective of the physical location or nationality of the child. Reducing the number of children who fall victim to sexual abuse and increasing the proportion of successful investigations remains a **key political and operational priority**.";
- stated that it considered "**industry**, and in particular online platforms, to be a **key contributor** to preventing and eradicating child sexual abuse and exploitation, including the swift removal of child sexual abuse material online. Notwithstanding current efforts, the Council notes that **more must be done** to counter technical, legal and human challenges that hamper the effective work of competent authorities.";
- recognised "the necessity of setting out **a multi-stakeholder approach**, bringing together industry, civil society, law enforcement and governments (including through public-private partnerships) to **coordinate prevention** efforts and thus maximise their effectiveness."; and, among others,
- invited "the EU and its Member States to assess periodically the **effectiveness of legislation** on combatting the sexual abuse and sexual exploitation of children to ensure that it is fit for purpose. Gender-sensitive assessments should address in particular the prevention, investigation and prosecution of crimes, including those committed in abuse of online platforms, as well as the provision of assistance and support to child victims during and after the investigation, and protection measures during criminal proceedings. Measures should however not be limited to the area of criminal law."

European Parliament. In its November 2019 resolution[386], the European Parliament notably:

---

384 A Union of Equality: Gender Equality Strategy 2020-2025, COM(2020)152 final.
385 Council conclusions on combatting the sexual abuse of children of 8 October 2019, No. 12862/19.
386 European Parliament resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child (2019/2876(RSP)).

- **called for the creation of an EU child protection centre** that would ensure an **effective and coordinated approach** on the protection of children's rights in all internal and external EU policies and actions and give an effective and coordinated response to child sexual abuse and all forms of violence against children;
- urged "the Commission and the Member States to work out a national strategy and put in place a holistic multi-stakeholder approach to eradicate sexual violence and child abuse both online and offline.";
- called on the current and upcoming Council presidencies to step up efforts to ensure that Member States take concrete actions to better assist victims and work out effective preventive, investigative and prosecution measures to ensure that perpetrators are brought to justice;
- urged "the Commission and the Member States to take concrete measures to end child sexual abuse by investing in **preventive measures**, identifying specific programmes for potential offenders and more effective support for victims." and, among others,
- called on "ICT companies and online platforms to take their share of responsibility in the fight against child sexual abuse and exploitation online" and stressed "the need for more investment, in particular from industry and the private sector, in research and development and new technologies designed to detect CSAM online and expedite takedown and removal procedures".

In addition, in its December 2020 resolution on the Security Union strategy[387], the **European Parliament** notably:

- reiterated the European Parliament's support for the creation of a **European centre to prevent and counter child sexual abuse**, as set out in the July 2020 EU strategy for a more effective fight against child sexual abuse;
- stressed the importance of **preventing, detecting and reporting** child sexual abuse; and, among others,
- noted that a growing number of children and teenagers are falling victim to **online grooming**.

European Economic and Social Committee. In its October 2020 Opinion on combatting child sexual abuse online[388], the Committee notably:

- stated that it "believes that it is time for the EU to have its own European Centre to Prevent and Counter Child Sexual Abuse and calls on the Commission to urge that such a centre will be set up and developed. The centre should build on Europol's work, to work with companies and law enforcement bodies, to identify victims and bring offenders to justice."

[387] European Parliament resolution of 17 December 2020 on the EU Security Union Strategy (2020/2791(RSP)).

[388] European Economic and Social Committee, Combatting child sexual abuse online, TEN/721 COM (2020) 568 final 2020/0259 COD, 29 October 2020.

- considers it would be useful to have a third party perform regular testing/auditing, using a sample non-CSAM (Child Sexual Abuse Material) match similar to EICAR test files in the anti-virus industry

3. National law

- **EU Member States.** Several Member States have either adopted or in the process of adopting national provisions, which aim at regulating online service providers with regard to illegal content and acts online. These include:
    - **Germany**:
        - **Network Enforcement Act** (NetzDG),[389] which aims at combating hate crime, criminally punishable fake news and to improve the enforcement of German criminal law online, notably in terms of deletion of content. Under the law, which came into effect on January 1, 2018, social networks – among other obligations - have to set up a complaints management system for reporting illegal content and must take down or block access to manifestly unlawful content within 24 hours of receiving a complaint. Social networks that fail to set up a complaints management system or do not set one up properly – especially where this means that they do not delete criminal content in full, on time or at all –face fines of up to €50 million. In addition to complying with this operational provision, social media platforms are also obliged to publish bi-annual reports. A revision was adopted in April 2021,[390] providing *inter alia* for detailed reporting obligations in case of detection of child sexual abuse materials.
        - **Draft Act amending the Protection of Young Persons Act**:[391] aims to regulate the dissemination of various forms of media harmful to minors. It provides for the establishment of an obligation for internet services relevant for children and minors to take appropriate and effective structural precautionary measures to protect them from dangerous content, protect their individual rights and their data, and further develop tools for strengthening media literacy. In order to enforce the implementation of the amendments, the draft also includes the restructuring of the Federal Review Board for Media Harmful to Minors into an authority to become the Federal Agency for the Protection of Children and Young Persons in the Media.
    - **France**:
        - **Law aimed at combating hate content on the internet** (Avia law):[392] this law, which was adopted on 13 May 2020, obliges online service providers to remove within 24 hours any content which has been reported by any user (physical or legal person) or by the police as manifestly unlawful (for ex.: material containing incitement to hatred

[389] Additional information on the NetzDG can be found here.
[390] Gesetzespaket zur Bekämpfung der Hasskriminalität | Recht | Haufe
[391] Additional information on the Draft Act can be found here.
[392] Additional information on the Avia law can be found here.

or violence). These obligations are addressed in particular to the big platforms such as Facebook, YouTube and Twitter, the search engines and the websites exceeding a visitor-threshold to be determined by national law. The time-frame to carry out the removal obligations is reduced to one hour – and applies not only to platforms but to any website – where the content has been flagged as terrorist propaganda or child sexual abuse material. Any failure to delete the content or make it inaccessible within these time-limits is punished under criminal law and triggers a fine up to 250.000 euros. Moreover, the law requires the platforms to adopt the organisational and technological measures appropriate to ensure that the flagged contents are examined and removed within the due deadlines. The law grants the French media regulator extensive powers to systematically monitor the levels of compliance with the law. Services under the scope of the law would also be subject to reporting and transparency obligations on their content moderation activities and technical and human means devoted to it. The French regulatory authority would also be granted broad powers of supervision and enforcement, including the issue of binding guidelines. Where the regulator considers that the measures in place are not adequate to the purposes of the law and that the platform has not aligned with its recommendations to mend non-conformity, it can issue fines up to 20 million euros or 4% of the annual turnover, whichever is higher. Although certain provisions of the law were deemed unconstitutional by the French Constitutional Council on 18 June 2020, particular concern has been voiced, across France's political spectrum, about the need to regulate online service providers more strictly. In the meantime, the French law that aims to regulate online hate speech entered into force on 1st July 2020[393].

- **Draft law to regulate online platforms**:[394] would create a new national (administrative) authority equipped for fighting piracy, protecting minors (including combatting the commercial exploitation of the image of children under sixteen years of age on online platforms) or defending the public against disinformation and online hate speech. The new authority would be in charge of enforcing platform rules, including the Digital Services Act. The principle obligations established in the draft relate to (i) cooperation with judicial or administrative authorities, the retention of reported and withdrawn content, and the appointment of a point of contact; (ii) the transparency of the general conditions of use, the moderation system, the conditions for the suspension or termination of the account and the public reporting on their moderation policy; (iii) providing users with

[393] Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, JORF n° 0156 du 25 juin 2020.

[394] Additional information on the draft law can be found here and here.

a mechanism for reporting illegal content and processing said reports promptly; (iv) the establishment of internal processes to combat the withdrawal of content and suspension of accounts; (v) the evaluation and mitigation of systemic risks associated with the service; (vi) an obligation to report periodically to the Conseil Supérieur de l'Audiovisuel (Higher Audio-visual Council) and (vii) possible formal notices and sanctions imposed by the same Conseil Supérieur de l'Audiovisuel in the event of non-compliance with these obligations. The draft aims to broaden the scope of the actors to whom the judicial authorities may prescribe any measures designed to prevent or stop damage caused by an illegal site or illegal content; the injunction of the judge would no longer be limited to hosting or internet service providers, but to "any person" who may contribute to these preventive measures. Among the new tools of the new authority are blacklists of illegal websites (containing a list of so called 'mirror sites' having content, which is identical or equivalent to that of the service covered by a court ruling) and mechanisms to make it easier to block such websites.

- **The Netherlands:**
  - **Draft law on fighting child sexual abuse**:[395] would impose a duty of care on companies to address illegal content proactively. It would also establish a new independent public law administrative body in charge of enforcing the removal of terrorist and child sexual abuse content online. The authority would cooperate with hotlines and law enforcement; have a legal basis to search for child sexual abuse material proactively; have the power to issue notices to hosting service providers, and to apply fines in case of non-compliance (for ex.: if child sexual abuse material is not taken down within 24 hours). A range of administrative instruments will allow action to be taken against communication service providers through whose services store or transmit child sexual abuse material, but who fail to take (voluntary) measures to prevent this. This law will make it possible to issue these providers with a binding order. Hosting service providers would be required to take appropriate and proportionate measures to limit the storage and dissemination of child sexual abuse online. This law also serves to implement a number of motions calling for greater efforts to combat child sexual abuse material online and a stricter approach to providers who fail to cooperate in this or who do not make sufficient efforts.
- **Austria:**

[395] The public consultation and the draft law are accessible here.

- **Draft law on measures to protect users on communication platforms (Communications Platform Act):**[396] On 1 January 2021, the Austrian "Communication-Platforms-Act" entered into force. Operators had until 1 April 2021 to implement it. The law applies to "communication platforms," which are defined as "information society service[s], the main purpose or an essential function of which is to enable the exchange of messages or presentations with intellectual content in written, oral or visual form between users and a larger group of other users by way of mass dissemination.". In principle, all domestic and foreign providers would be affected, provided that that they had more than 100,000 registered users in Austria in the previous quarter and more than 500,000 euros revenue generated in Austria in the previous year. Certain communication platforms are exempt, such as certain media companies that are already covered by specific legal requirements, or online trading platforms and not-for-profit online encyclopedias, even though they have a commentary section. All regulated communication platforms would be required to appoint a "*responsible representative*" to ensure compliance with domestic law and for service of process and cooperation with law enforcement authorities. Depending on the severity of the violation, the financial strength of the platform, the number of registered users and the frequency/repetition of violations, different types of penalties will be imposed.

- **Third countries:**
  - **US.** Since many of the service providers whose cooperation is essential in the fight against child sexual abuse online are headquartered in the US, its national legal framework is also relevant in this context. It includes:
    - **18 U.S. Code § 2258A**[397], which obliges online service providers to report to the National Centre for Missing and Exploited Children instances of child sexual abuse online in their systems that they become aware of.
    - The **PROTECT Our Children Act of 2008**[398], introduced in 2008 by the **current US President Biden**, requires the Department of Justice to develop and implement a National Strategy Child Exploitation Prevention and Interdiction, to improve the Internet Crimes Against Children Task Force, to increase resources for regional computer forensic labs, and to make other improvements to increase the ability of law enforcement agencies to investigate and prosecute child predators.

---

396 Additional information on the draft law can be found here.
397 18 U.S.C. §2258A, Reporting requirements of providers.
398 Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008, S. 1738, 110th Congress, 2008.

- **UK.** The **Online Harms White Paper**[399] covers both illegal and harmful content. It provides for a new regulatory framework establishing a duty of care on companies to improve the safety of their users online, overseen and enforced by an independent regulator. The regulator would have a suite of powers to take effective enforcement action against companies that have breached their statutory duty of care. This may include the powers to issue substantial fines and to impose liability on individual members of senior management. It sets out a programme of action to tackle content or activity that may not cross the criminal threshold but can be particularly damaging to children or other vulnerable users. This includes requiring companies to provide effective systems for child users, and their parents or carers, to report, remove and prevent further circulation of images of themselves which may fall below the illegal threshold, but which leave them vulnerable to abuse.
  Following the consultation on the Online Harms Whilte paper, the draft Online Safety Bill[400], which aims to establish a new regulatory framework to tackle harmful content online, was published on 12th May 2021.

4. International conventions and agreements

- The 1989 **UN Convention on the Rights of the Child**, which establishes the right of the child to be protected from all forms of violence[401].
- **UNCRC General comment No. 25 on children's rights in relation to the digital environment**[402]**,** of 2 March 2021, makes explicit - for the first time - that **children's rights apply in the digital world**, including the protection from child sexual abuse and exploitation. It sets out, among others, that state parties should take all appropriate measures to protect children from exploitation and abuse, including by legislating and enforcing **business sector responsibility**. It also states that digital service provider's compliance can be achieved through **due diligence**, in particular by means of **child impact assessments**. In particular, paragraphs 36-39 (Section I, Children's right and business sector) provide the following:

  36. States parties should take measures, including through the development, monitoring, implementation and evaluation of legislation, regulations and policies, to ensure compliance by businesses with their obligations to prevent their networks or online services from being used in ways that cause or contribute to violations or abuses of children's rights, including their rights to privacy and protection, and to provide children, parents and caregivers with prompt and effective remedies. They should also encourage businesses to provide

399 UK Home Office, Consultation Outcome: Online Harms White paper, updated 15 December 2020.
400 UK Home Office, Draft Online Safety Bill, 12 May 2021.
401 Also of relevance for child sexual abuse in the domestic context is the Council of Europe Convention on preventing and combatting violence against women and domestic violence, CETS No.210, 01.08.2014.
402 United Nations, UNCRC General comment No. 25 (2021) on children's rights in relation to the digital environment of 2 March 2021, CRC/C/GC/25.

public information and accessible and timely advice to support children's safe and beneficial digital activities.

37. States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.

38. States parties should require the business sector to undertake child rights due diligence, in particular to carry out child rights impact assessments and disclose them to the public, with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children. They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

39. In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.

- The 2007 Council of Europe **Convention on Protection of Children against Sexual Exploitation and Sexual Abuse** (Lanzarote Convention)[403], which served as an inspiration for the Child Sexual Abuse Directive.
- The Council of Europe **Convention on Cybercrime** (Budapest Convention)[404]. This 2001 instrument obliges Parties to establish certain criminal offences relating to child sexual abuse material in their domestic law. In addition, the Convention also provides, among others, a framework for mutual legal assistance,

[403] Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.201, 01.07.2010.
[404] Council of Europe Convention on Cybercrime, ETS No.185, 01.07.2004.

and requires parties to ensure the availability of certain procedural powers in relation to the detection, investigation and prosecution of cybercrime offences at both the domestic and international levels. The Parties to the Convention are engaged in negotiations for an additional Protocol to the Convention to enhance existing rules to improve cross-border access to e-evidence[405].

[405] For more information see here.

ANNEX 6: ADDITIONAL INFORMATION ON THE PROBLEM

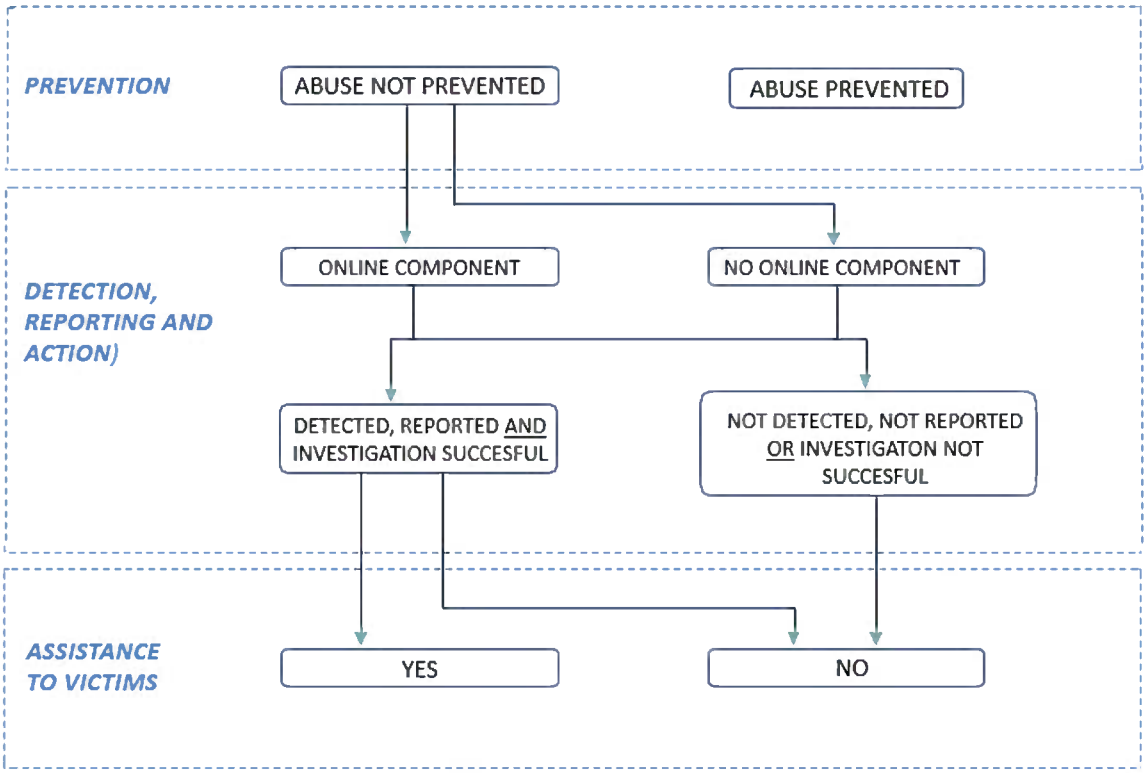
This annex presents additional information on the definition and magnitude of the problem.

1. Definition

The problem is that some child sexual abuse crimes are not adequately addressed in the EU due to insufficient prevention, challenges in their detection, reporting and action, and insufficient assistance to victims.

Figure 1 presents and overview of the different parts of the problem in its broadest form:

Figure 1: overview of the different parts of the problem



1.1. Prevention

There is consensus among practitioners in the fight against child sexual abuse (including law enforcement) that prevention is essential, because it is obviously best for children to protect them from falling victim to the crime rather than acting after the fact. Once the offender commits the crime the victim is harmed, and, even if law enforcement rescues them and stops the abuse, it is already too late to avoid the immediate and long-term negative consequences for victims of the abuse that has already taken place.

There are two main types of prevention efforts[406]:

1. Efforts focused on the **child** and his or her environment and on decreasing the likelihood that a child becomes a **victim**. Examples include **awareness raising**

[406] See here for an overview of international efforts to prevent child sexual abuse: Unicef, Action to end Child Sexual Abuse and Exploitation: A Review of the Evidence 2020, December 2020, p. 77, 143.

campaigns to help inform children, parents, carers and educators about risks and preventive mechanisms and procedures, as well as **training**.

2. Efforts focused on potential **offenders** and on decreasing the likelihood that a person **offends**. Examples include prevention programmes for persons who **fear that they might offend**, and for persons who have already offended, to **prevent recidivism**.

The Child Sexual Abuse Directive[407] requires Member States to put in place **effective prevention programmes**. It requires Member States to ensure that persons who fear they may commit child sexual abuse offences have access to effective intervention programmes or measures designed to evaluate and prevent the risk of such offences being committed[408]. Similarly, Member States are obliged to make effective intervention programmes available at any time during criminal proceedings to prevent and minimise the risks of repeated offences[409]. The 2011 Directive also requires Member States to take action to discourage and reduce the demand that fosters all forms of sexual exploitation of children, to raise awareness and reduce the risk of children becoming victims of sexual abuse or exploitation[410].

The monitoring of transposition into national law of this Directive indicates that Member States struggle with putting in place such programmes[411], of the two types above, where frequently multiple types of stakeholders need to take action. As a result, children and their environment are insufficiently aware of the risks and of means of limiting them, and persons who fear they may offend do not find avenues for support to try to avoid offending.

1.2. Detection, reporting and action

Where prevention fails, the first step to address these crimes is to detect them as early as possible and report them to law enforcement.

Despite the seriousness of these crimes, a long time often passes before they are detected[412], if that ever happens. The lack of detection can have several reasons: frequently, the abuser establishes control over the victim, using secrecy, blame, and threats to prevent the child from disclosing the abuse[413]. The child may also be unable to seek help due to an intellectual or physical disability, or because the child is afraid of the consequences of going against the abuser's will, as the abuser often belongs to the **circle of trust** of the child (**four in five cases**), i.e. **people they know and trust or depend**

---

407 Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011, p. 1–14

408 *Ibid* , Art. 22.

409 *Ibid* , Art. 24.

410 *Ibid* , Art. 23.

411 Member States struggle in particular with the implementation of Articles 22, 23 and 24 of the Directive, focused on prevention. For more details, see the Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, COM/2016/0871 final.

412 McElvaney, R., *Disclosure of Child Sexual Abuse: Delays, Non- disclosure and Partial Disclosure. What the Research Tells Us and Implications for Practice*, 26 June 2013, p. 159-169;
see also The Irish Times, Historic sex abuse victims waiting average of 20 years to come forward, 17 April 2019.

413 Darkness to Light, Child Sexual Abuse Statistics, accessed on 20 April 2021; See also the research on Child Sexual Abuse Accommodation Syndrome, which may explain why children often do not report sexual abuse incidents or withdraw their complaints, Masumova, F., A Need for Improved Detection of Child and Adolescent Sexual Abuse, May 2017.

on[414], including **family members in one in five cases**[415]. Or the child victims simply may be too young to recognise that what is happening to them is abuse[416]. As a consequence, the child may not tell anyone and those close to the child either are not aware of the problem or are accomplices to the crimes[417]. For example, in a recent case in a campsite in Germany, two men sexually abused **32 children, aged between 3 and 14, over 10 years**, including a foster girl that had been trusted to one of the men[418]. In another recent case, a stepfather had been sexually abusing and raping his three stepchildren **for 8 years** until the mother found out by chance[419].

Frequently the only way that these crimes come to the attention of public authorities is when the offenders exchange online the **images and videos** of the abuse or try to approach children online for sexual purposes. For example, in Germany the police rescued a 10 year old boy and a 13 year old girl that had been abused by their father 42 times before an online service provider detected the images of the abuse and reported them to public authorities[420].

Even when the abuse does not occur in the circle of trust, such in the case of **online solicitation of children** where an offender lures or extorts the child into sexual abuse, internet companies (more precisely referred to as online service providers) are often the only ones to be able to detect the crimes. In these cases, the child may not dare to tell anybody for fear of the offender, who often threatens the victims with sharing the images and videos of their abuse with their family and friends if they tell anyone. For example, in a recent case in the UK, an offender who pretended to be a girl online was convicted of abusing **52 children**, **ranging from ages 4 to 14,** after targeting more than **5000 children globally**. He threatened the victims with sharing online the sexual images that he had lured them into producing and forced some of them to abuse younger children and record the abuses. Some victims later tried to kill themselves. The investigation only started after Facebook, the online service he mainly used to find victims, detected the abuse and reported it to public authorities[421].

Reports of child sexual abuse online are both evidence of a crime, as the possession and dissemination of child sexual abuse materials and grooming of children into abuse are in themselves criminal offences, and at the same time often also a lead for uncovering further offences, including at times ongoing child sexual abuse.

Reports from online service providers can contain three main types of abuse:

1. **past abuse**, through the distribution of **known material**, i.e. images and videos that have already been detected before and identified as child sexual abuse;

---

414 This includes in particular children with disabilities living in institutional care.

415 Gewirtz-Meydan, A., Finkelhor, D., Sexual Abuse and Assault in a Large National Sample of Children and Adolescents, 16 September 2019. See also Canadian Centre for Child Protection, Survivor's Survey Full Report 2017, July 2017; and ANAR, Sexual Abuse in Childhood and Adolescence according to the Victims and its Evolution in Spain (2008-2019), February 2021.

416 National Society for the Prevention of Cruelty to Children (NSPCC), What is sexual abuse?, accessed on 9 April 2021.

417 Pereda, N., Diaz-Faes, D.A., Family violence against children in the wake of COVID-19 pandemic: a review of current perspectives and risk factors, 20 October 2020.

418 The Guardian, Two men jailed for decades of child abuse at German campsite, 5 September 2019. DW, Germany: Long jail terms handed out in campsite sex abuse trial, 5 September 2019.

419 Süddeutsche Zeitung , Stiefvater wegen jahrelangen Kindesmissbrauchs vor Gericht, 20 January 2021.

420 Süddeutsche Zeitung, Solinger soll eigene Kinder missbraucht haben, 29 January 2021.

421 UK National Crime Agency, Paedophile who targeted more than 5,000 children globally in child sexual abuse case jailed for 25 years, 10 February 2021.

2. **ongoing abuse**, through the distribution of **new material**, i.e. images and videos of child sexual abuse which had not been detected before;
3. **future abuse**, through the detection of **grooming** (also referred to as online solicitation or enticement), i.e. text-based threats for children in which an adult, frequently hiding its true identity[422], establishes online contact with a child for sexual purposes[423].

These reports have been **instrumental** for years in **rescuing children in the EU from ongoing abuse**. They have led to, for example:

- the rescue of **11 children**, some as young as **2 years old**, who were exploited by a network of abusers in **Sweden**[424];
- the single **largest operation ever** against child sexual abuse in **Denmark**[425];
- the rescue of a **9 year-old** girl in **Romania**, who had been abused by her father for **more than a year**[426];
- the arrest of an offender in **France** who groomed **100 children** to obtain child sexual abuse material from them[427];
- the rescue of **2 girls** in **Czechia**, abused by a 52 year-old man, who recorded the abuse and distributed it online[428];

These reports have also been **instrumental** in **preventing** the abuse of children in the EU, through the detection of **online solicitation**.

Annex 7 contains additional information on sample cases of child sexual abuse in the EU that started with a report from online service providers.

Law enforcement in the EU receives the vast majority of child sexual abuse reports from two **sources**: 1) service providers, through NCMEC; and 2) the public and hotlines, through hotlines[429]:

---

422 Craven, S., et al., Sexual grooming of children: Review of children: Review of literature and theoretical considerations, November 2006.

423 Online solicitation may also reflect ongoing abuse (e.g. when the child is extorted into producing new images and videos).

424 Swedish Cybercrime Centre SC3, Swedish Police.

425 Europol, Internet Organised Crime Threat Assessment, 18 September 2018, p. 32.

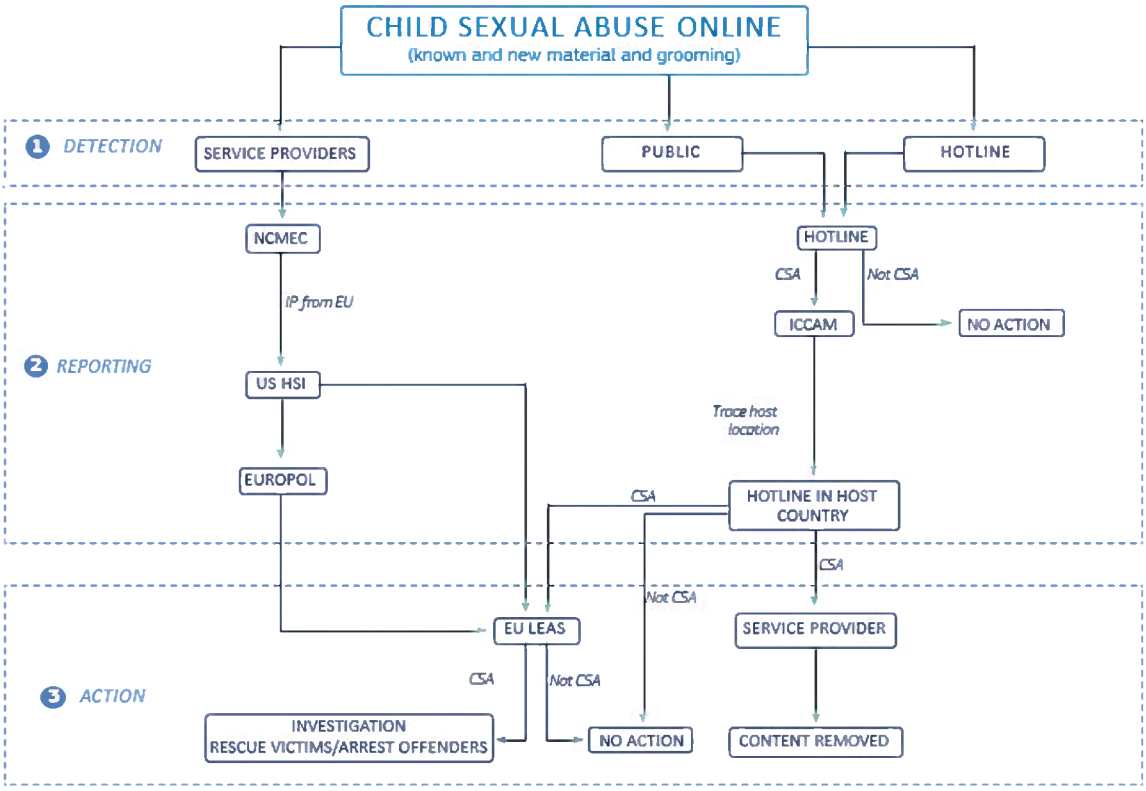
426 Stirile Kanal D, O femeie de 27 de ani, din Bacău şi-a abuzat sexual fetiţa de doar 9 ani pentru a-şi mulţumi iubitul, 9 November 2018.

427 As reported by the French police.

428 As reported by the Czech police.

429 Based upon the median percentage of reports received by law enforcement authorities from each source according to the targeted survey of law enforcement authorities (see Annex 2). Respondents indicated that about 45% of reports originate from providers through NCMEC, while about 10% of reports originate from hotlines in their own jurisdiction or another jurisdiction, representing the largest two external sources.

Figure 2: the two main sources of CSA reports for law enforcement in the EU



From service providers

In a survey addressed to public authorities in Member States, **more than two thirds** of respondents indicated that the largest proportion of leads in child sexual abuse cases were **reports** from **online service providers** about abuse discovered on their systems[430].

1. Detection.

In the detection stage of the process, known CSAM, new CSAM or solicitation is detected by technologies used by the provider. Several types of technologies are currently used by providers and organisations in this stage, many of which are made freely available as a service to qualified users[431]. Technologies for the detection of known CSAM typically make use of a process known as hashing, which generates 'digital fingerprints' of files. By comparing these fingerprints with those of content that has been previously verified as CSAM, new copies of the content can be easily detected[432]. Technologies for the detection of new CSAM are commonly based on artificial intelligence. Using previously-verified CSAM, these technologies are trained to identify whether new material is likely to constitute CSAM[433]. See annex 8 for more details on the detection technologies.

2. Reporting.

---

[430] See Annex 2.

[431] H. Lee et al., Detecting child sexual abuse material: A comprehensive survey, Forensic Science International: Digital Investigation, Volume 34, September 2020, 301022.

[432] Thorn, 'Introduction to Hashing: A Powerful Tool to Detect Child Sex Abuse Imagery Online', 12 April 2016.

[433] Thorn, 'How Safer's detection technology stops the spread of CSAM', 13 August 2020.

In the reporting stage, content that has been flagged as possible CSA online is processed prior to receipt by relevant law enforcement authorities. In this stage, the service provider may perform additional verification, such as human review, of flagged content to confirm that the content constitutes CSA online. In addition, the provider blocks access to the CSA online and makes a report to NCMEC. US law obliges service providers **to report** to NCMEC child sexual abuse online in their services where they become aware of the abuse (i.e. it does not make providers subject to an obligation **to detect** such abuse).

NCMEC verifies in some cases that the reported content constitutes CSA online, in accordance with the relevant definitions under US law, and attempts to determine the relevant jurisdiction(s). Where the report relates to an EU Member State, the report is forwarded to the US Department of Homeland Security Investigations (HSI) for onward transfer, either to Europol or directly to the relevant EU law enforcement authorities[434]. Europol cannot receive information directly from private parties, including NCMEC (or service providers)[435], hence the intermediary role of US HSI.

Reports which are received by Europol are cross-checked and forwarded to the relevant Member States[436].

3. Action.

In the 'action' stage, reports are received by the competent law enforcement authorities in Member States. Those authorities then review the reports in accordance with national law, confirming that the report relates to possible criminal activities and commencing a criminal investigation.

Based upon the information contained in the report, law enforcement authorities take steps to identify and rescue victims from ongoing or imminent abuse, and to identify, investigate and ultimately arrest suspects. Where necessary, authorities engage further with the service provider to obtain further information relevant to the investigation, and, in limited cases, to provide feedback to providers on their reports in order to improve quality in future.

Box 1: challenges in cross-border access to electronic evidence

In many cases, additional information is needed by law enforcement authorities from service providers when investigating child sexual abuse, with those service providers often being located in another Member State, or in a third country. Significant and longstanding challenges exist regarding processes to obtain access to e-evidence across borders. Indeed, e-evidence is relevant in about 85% of criminal investigations, and in two thirds of these investigations a request to service providers in other jurisdictions is needed[437].

---

434 Europol channels NCMEC reports to 18 EU Member States. The rest of the Member States receive reports directly from NCMEC through a secure (VPN) channel set up by HSI.

435 Impact Assessment accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation of 9 December 2020, SWD/2020/543 final.

436 The proposal for a revision of Europol's mandate includes the possibility for Europol to receive personal data from private parties. See Proposal for a Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation of 9 December 2020, COM(2020) 796 final.

437 See the Impact assessment for the proposals on cross-border access to e-evidence SWD/2018/118.

While several mechanisms exist for access to such evidence, each has significant difficulties. Judicial cooperation between the public authorities of different countries (for example, through mutual legal assistance channels or European Investigation Orders) is typically slow and resource intensive. Direct cooperation between service providers and public authorities is possible in some cases, however in general it is unreliable, inconsistent and lacks transparency and accountability.

In general, less than half of all requests to service providers are fulfilled, and two-thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted[438]. There are currently several initiatives which seek to address challenges related to e-evidence at the Union level and internationally[439].

From the public and hotlines

About 10% of the reports that law enforcement in the EU receives come from hotlines, which in turn receive reports from either the public or other hotlines[440].

1. Detection.

In the detection stage, suspected child sexual abuse online is encountered either by a member of the public, who makes a report to the national hotline in their country, or by a hotline searching proactively for child sexual abuse online.

2. Reporting.

In the reporting stage, the hotline reviews the suspected child sexual abuse in accordance with national law. Where the reported content does not constitute CSAM, no further action is taken. Where the hotline concludes that the content does constitute CSAM, the hotline adds hashes to INHOPE's ICCAM database, and attempts to determine the jurisdiction in which the content is hosted.

If the content is hosted in the same jurisdiction as the hotline, the hotline sends a report to the relevant law enforcement authorities for investigation. The hotline also sends a notice-and-takedown request to the relevant service provider, alerting the provider of the abusive content on their service and responsibility to remove the content under the eCommerce framework. The hotline then monitors and confirms the service provider's compliance.

If the content is determined to be located in another jurisdiction, the hotline forwards the report to the national hotline in that jurisdiction, if one exists. The hotline in the host

---

438 *Ibid.*

439 Proposal for a Regulation and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters of 17 April 2018, COM/2018/225 final; and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings of 17 April 2018, COM/2018/226 final.
Negotiations on an EU-US e-evidence agreement: Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 9114/19.
Negotiations on a Second Additional Protocol to the Convention on Cybercrime: Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 9116/19.

440 Sum of median percentages of reports of child sexual abuse online received by law enforcement authorities from hotlines in their own jurisdiction or another jurisdiction, as a percentage of the total number of reports received. Source: Targeted survey of law enforcement authorities (see Annex 2).

country re-examines the reported content in accordance with the national law of that jurisdiction and, if the reported content is confirmed to constitute child sexual abuse under the applicable law, forwards the report to the relevant law enforcement authorities and service provider for action, as above.

In cases where the content is found to be hosted in another jurisdiction which does not have a national reporting hotline, the hotline forwards the report to Interpol for action.

3. Action.

In the action stage, reports are received by the competent law enforcement authorities in the jurisdiction where the reported content is hosted, and notice-and-takedown requests are received by the service providers hosting the content.

Under the eCommerce framework, providers' exemption from liability for illegal content ceases to apply if they do not act promptly once they are made aware of the content's presence on their services. Upon receipt of a notice-and-takedown request, the provider take steps to remove the reported content from their services in accordance with their legal obligations, while the hotline monitors and confirms that the content is removed.

Reports received by law enforcement authorities are reviewed in accordance with national law in order to confirm that the report relates to possible criminal activities, and a criminal investigation is launched. Due to the nature of reports received from hotlines, which are sourced by members of the public and hotlines themselves from the open web, reports typically contain only limited information.

Based upon the information contained in the report, law enforcement authorities take steps to identify and rescue victims from ongoing or imminent abuse, and to identify, investigate and ultimately arrest suspects. Where necessary, authorities engage further with the service provider to obtain further information relevant to the investigation.

Box 2: regulatory challenges and the effectiveness of hotlines

The operation of hotlines is not explicitly provided for in Union law, and is provided for by national law in only five Member States. Hotlines also lack an explicit and uniform legal basis for the exchange of CSAM and data related to CSAM with other hotlines, service providers and law enforcement authorities[441]. EU hotlines usually operate based on co-regulation and self-regulation frameworks, leading to legal uncertainty with gaps in relation to the legality of processing of reports and related data. This, in turn, significantly restricts the activities that can be undertaken by EU hotlines[442].

While the importance and effectiveness of proactive searches for CSAM by hotlines has been demonstrated, the lack of a clear legal basis for EU hotlines to undertake such searches means that currently just one EU hotline can do so, and only to a limited extent[443].

Also, the lack of a clear and consistent legal framework for notice-and-takedown requests significantly complicates the work of hotlines. Many EU hotlines are unable to send notice-and-takedown requests to providers, while the lack of harmonised monitoring, sanctions and definitions of prompt removal undermine compliance[444]. Similarly to

441 *Ibid.*

442 European Commission, *Study on framework of best practices to tackle child sexual abuse material online*, 2020.

443 *Ibid.*

444 *Ibid.*

reports from US service providers, differences between definitions of CSAM in different jurisdictions, including between different Member States, can create difficulties: content that is classified as illegal by the hotline that receives a public report may not be illegal in the jurisdiction where the content is hosted. Consequently, such reports must be assessed by multiple hotlines, leading to delays or even resulting in the content being left online[445].

1.3. Assistance to victims

Victims of child sexual abuse need **tailored and comprehensive assistance**[446], **immediately and in the long-term**[447].

An example of **immediate** assistance is the **support** of victims during **criminal investigations and proceedings**, to prevent that they suffer additional trauma (e.g. by setting specific standards for interviews with child victims)[448].

An example of **long-term** assistance is the support of victims to **stop the sharing and distribution** online of the **images and videos** depicting their abuse, which **perpetuates the harm**. Victims have to live with the knowledge that the images and videos showing the worst moments of their lives are circulating and anyone, including their friends or relatives, may see them[449].

The **Child Sexual Abuse Directive** introduced measures to support victims of child sexual abuse, including measures to prevent that victims suffer additional trauma through their involvement in criminal investigations and proceedings[450], to ensure that assistance and support are available as soon as there are reasonable grounds to suspect an offence[451], and that special protection is assured for children reporting abuse committed within the family[452].

The monitoring of transposition into national law of the Directive indicates that Member States are incurring **delays** to fully implement these articles concerning assistance and support to victims before, during and after criminal proceedings[453]. In addition, as noted in the EU strategy for a more effective fight against child sexual abuse, the efficiency and

---

445 *Ibid.*

446 Unicef, Action to end Child Sexual Abuse and Exploitation: A Review of the Evidence 2020, December 2020.

447 Victims' testimonies, which may help understand victims' need for assistance, are available at The Truth Project, Experiences Shared, accessed on 20 April 2021; Royal Commission into Institutional Responses to Child Sexual Abuse, Narratives, accessed on 20 April 2021.

448 Canadian Centre for Child Protection, Survivor's Survey Full Report 2017, July 2017;
ANAR, Sexual Abuse in Childhood and Adolescence according to the Victims and its Evolution in Spain (2008-2019), February 2021.

449 See related victims testimonies at The New York Times, 'If Those Were Pictures of You, You Would Understand', 9 November 2019.

450 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *OJ L* 335, 17.12.2011, Art. 20. L 335, 17.12.2011, p. 1–14

451 *Ibid,* Art. 18.

452 *Ibid,* Art. 19.

453 For more details, see the Report from the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography of 16 December 2016, COM/2016/0871 final.

effectiveness of efforts to assist victims is limited as these do not systematically make use of existing best practices and lessons learned in other Member States or globally[454].

Also, although not explicitly required by the Directive, no Member State has put in place measures to support victims in **ensuring removal** of child sexual abuse materials circulating online. Victims are unable to take action themselves as they would be committing a crime when searching for child sexual abuse images.

As figure 2 indicated, even if the abuse is detected and the investigation is successful, there are situations in which the victim does not receive the necessary assistance.

2. Magnitude

It is not possible to determine **exactly** the number of crimes that cannot be effectively addressed in the EU due to insufficient prevention, challenges in their detection, reporting and action, and assistance to victims. Data at this level of detail is **not collected** by public authorities.

In addition, these crimes appear to be significantly **underreported**. Studies show that whereas about **one in five girls** and **one in ten boys** become a **victim** of child sexual abuse[455], **one in three victims will never tell anyone** and at least **four in five child sexual abuse cases are not reported directly to public authorities**[456] (i.e. by the victims or people close to the victims).

There are indications that the **COVID-19** crisis has exacerbated the problem[457], especially for **children who live with their abusers**[458]. In addition, children are **spending more time online than before, possibly unsupervised**.[459] While this has allowed them to continue their education and stay in touch with their peers, there are signs of increased risk of children coming into contact with **online predators**[460]. With more offenders isolated at home, the **demand for child sexual abuse material** has increased[461] (e.g. by 25% in some Member States[462]), which in turn leads to increased demand for new material, and therefore **new abuses**[463].

---

454 EU Strategy for a more effective fight against child sexual abuse COM(2020) 607 final.

455 M. Stoltenborgh, M.H. van IJzendoorn, E.M.Euser, M.J. Bakermans-Kranenburg, A global perspective on child sexual abuse: Meta-analysis of prevalence around the world, 2011, pp. 79-101. This study, based on 331 independent samples and almost 10 million individuals, found an overall prevalence rate of 13%, with the rate for girls being more than twice that of boys (18% vs. 8%, respectively). These numbers concur with those of another study involving more than 10 000 individuals, which found a prevalence of 7.9% of males and 19.7% of females: Pereda N, Guilera G, Forns M, Gómez-Benito J, The prevalence of child sexual abuse in community and student samples: a meta-analysis, 2009.

456 Gewirtz-Meydan, A., Finkelhor, D., Sexual Abuse and Assault in a Large National Sample of Children and Adolescents, 16 September 2019; Martin E, Silverstone P: How much child sexual abuse is "below the surface", and can we help adults identify it early, May 2013.

457 Europol, Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.

458 WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children and UNESCO, COVID-19 and its implications for protecting children online, April 2020.

459 Europol, European Union serious and organised crime threat assessment, 12 April 2021.

460 *Ibid.*

461 NetClean, 'NetClean Report – COVID-19 Impact 2020', accessed 14 April 2021.

462 Europol, Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.

463 The number of child sexual abuse reports globally quadrupled in April 2020 (4.1 million reports) compared to April 2019 (around 1 million), as reported to the US National Centre for Missing and

With regard to the **victims**:

- a majority are **female** (girls are more than twice as likely to be abused than boys)[464];
- one of every seven victims of sexual violence reported to law enforcement agencies is **under 6 years**[465];
- **three out of four** victims depicted in the images and videos is younger than 13 years old[466];

With regard to the **offenders**:

- Although prevalence data is scarce, studies indicate that around **3%** of the male population could have a paedophilic disorder[467];
- Estimates suggest that only **50%** of child sexual abusers have a sexual orientation towards children (paedophilia or hebephiliac)[468];
- Studies suggest that up to 32% of high-risk offenders who view child pornography **may re-offend**[469].
- 99.6% of people convicted in the US in 2019 for non-production CSAM (e.g. distribution) were men, with an average age of 41[470].

2.1. Data on reporting by online service providers

Amount of reports

The past few years have seen a **strong increase** in reports of child sexual abuse online submitted by online service providers globally: from 1 million reports in 2010 to **over 21 million in 2020**:

Exploited Children, CNN, The pandemic is causing an exponential rise in the online exploitation of children, experts say, 25 May 2020.

464 Collin-Vézina, D., et al., Lessons learned from child sexual abuse research: Prevalence, outcomes, and preventive strategies, 18 July 2012, p. 6. See also : SVSolutions - Preventing Sexual Violence Against Children - Together For Girls, which analysed available data from 24 countries (primarily in high- and middle-income countries) and found that sexual violence in childhood ranged from 8% to 31% for girls and 3% to 17% for boys.

465 Gewirtz-Meydan, A., Finkelhor, D., Sexual Abuse and Assault in a Large National Sample of Children and Adolescents, 16 September 2019, p.2.

466 INHOPE, Annual Report, 2019, p. 31.

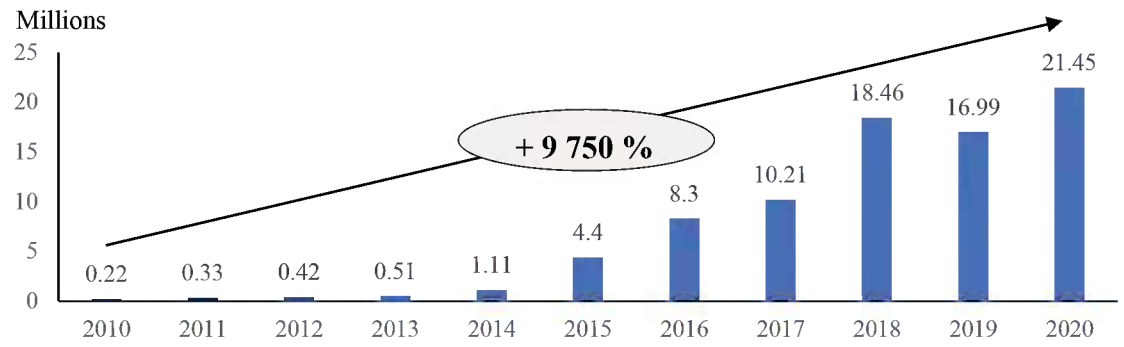
467 In a self-report survey with a sample of 1,978 young adult males from Sweden, 4.2 % reported they had ever viewed child sexual abuse material (Seto, et al, 2015). In another self-report survey with a sample of 8,718 adult males in Germany, 2.4% of respondents reported using that material (Dombert, et al, 2016).
Not all offenders have a paedophilic disorder (other motivations to offend include exploitation for financial gain), and not everyone who has a paedophilic disorder ends up being an offender (some people seek support in dealing with their paedophilia).

468 Fast,E., Paedophilia and sexual offending against children: Theory, Assessment and intervention by M. Seto, 2010.

469 Eke, A., Seto, M., Williams, J., Examining the criminal history and future offending of child pornography offenders, 2011. Link between those who view Internet child pornography and those who commit CSA unclear. Nonetheless, it appears that for high-risk CSA offenders, pornography increases the risk of offending in a study of 341 offenders, according to Kingston, D., Pornography Use and Sexual Aggression: The Impact of Frequency and Type of Pornography Use on Recidivism Among Sexual Offenders, 2008.

470 United States Sentencing Commission, Federal Sentencing of Child Pornography (non-production offences), June 2021.

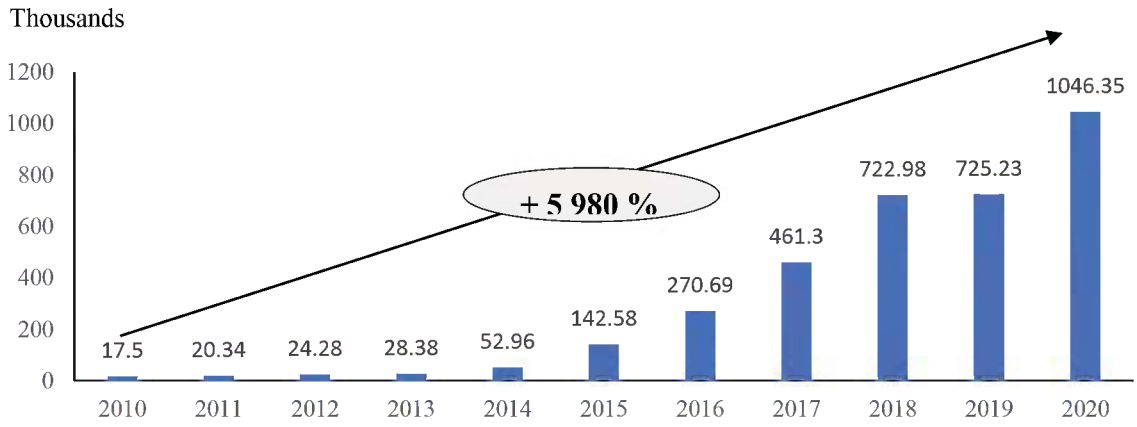
Figure 3: total reports submitted by online service providers, 2010-2020



These reports included more than **65 million images and videos**[471]. A report can contain multiple files, of various types (e.g. images, videos and text), and can concern one or several types of abuse (e.g. known material, new material, and grooming).

A similarly stark increase has occurred with reports concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.): from 23 000 in 2010 to **more than 1 million in 2020:**

Figure 4: EU-related reports submitted by online service providers, 2010-2020



These reports contained more than **4 million images and videos**[472].

Breakdown by company

A single company, **Facebook**, submitted **95% of the reports** in 2020. Five companies (Facebook, Snapchat, Google, Microsoft and Twitter) submitted 99% of all reports in that year[473].

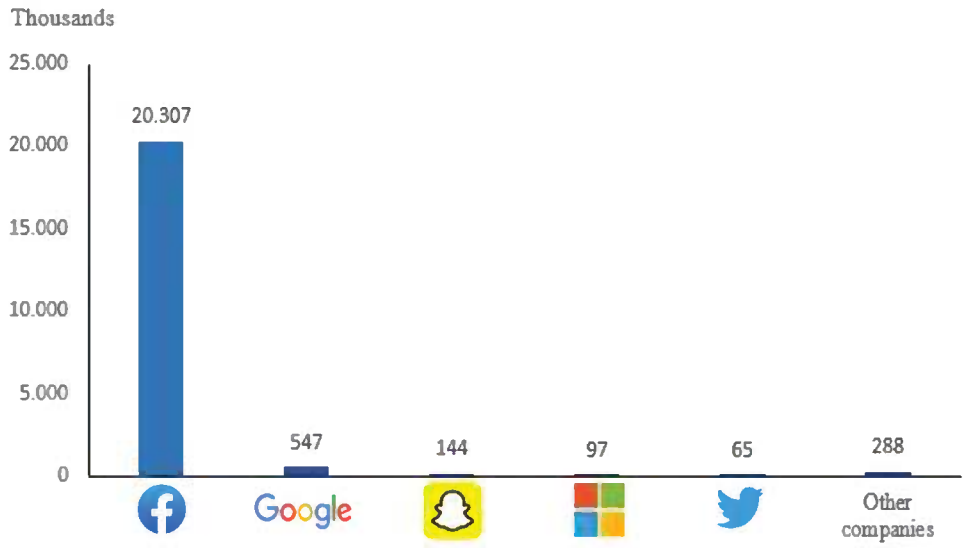
---

471 As reported to the US National Centre for Missing and Exploited Children (NCMEC). Its CyberTipline received a total of 65,465,314 files within reports in 2020.

472 As reported to the US National Centre for Missing and Exploited Children (NCMEC). Its CyberTipline received 4,265,151 files in the reports that resolved to the European Union Member States.

473 National Centre for Missing and Exploited Children (NCMEC), 2020 Reports by Electronic Service Provider (ESP), accessed 20 April 2021. In 2019 the number was similar, 94%.

Figure 5: breakdown of reports submitted by online service providers in 2020



There are currently **1630** companies registered to report to NCMEC. In 2020, NCMEC received reports from 167 service providers, meaning that approximately 88% of providers registered with NCMEC made no reports at all. Of these 167 providers, around 80% made fewer than 100 reports.

There is no evidence that 95% of the current cases of child sexual abuse in online service providers occur in Facebook. In fact, experts suggest that **comparable levels of abuse** occur in **similar services** from other companies, and the difference in detection levels is rather due to the **different intensity** of detection efforts[474]. This means that there is a **substantial amount** of child sexual abuse online that **remains undetected**.

Content of reports

The most reported content is known material, followed by new material and grooming[475]:

Table 1: content of EU-related reports from online service providers in 2020[476]

Type of child sexual abuse online		**2020**
All material (images and videos)		4 265 151
Known material (images and videos)		3 736 985
New material	Images	436 754
	Videos	91 412
Grooming		1 453

[474] The New York Times, Tech Companies Detect A Surge in Online Videos of Child Sexual Abuse, 7 February 2020; The Verge, As platforms get better at detecting child sexual abuse videos, they're finding more of them, 7 February 2020.

[475] The amount of new and known videos is unknown. It is possible to determine the exact amount of known images, based on the number of hits with the database of hashes, and through that number estimate the amount of new images. There is not yet a similar database of video hashes at NCMEC, and therefore it is only possible to estimate the amount of videos (known and new) received.

[476] National Centre for Missing and Exploited Children.

Table 1 above describes the content of reports. The number of reports is in general higher because a report can contain multiple types of child sexual abuse online (e.g. known images mixed with new ones, etc), and the same file can be reported multiple times. For example, a set of images of children abused by a group of offenders has been reported to NCMEC almost 900 000 times since 2005. In another example, images of a child abused by a family member has been reported to NCMEC over 1 million times since 2003[477].

The amount of **new images detected increased by more than 10 times** and the amount of **grooming reports increased by more than 5 times** from 2019 to 2020[478]. The **COVID pandemic** may explain these dramatic increases. As both children and perpetrators spent more time at home, the possibilities for **grooming and new abuses** increased, including through the production of **self-generated material.**

*Box 3: **grooming** and **self-generated material** involving children*

Abuse relating to self-generated sexual content/material involving children is **common** and features **increasingly** in investigations[479]. This content includes material that has been created as a result of **grooming** (i.e. an offender lures or extorts the child into producing that material), as well as material which, while originally **voluntarily-produced**, is used or distributed in an exploitative or abusive way[480].

76% of law enforcement authorities report that self-produced material **as a result of grooming** is a **common or very common** feature in investigations[481], while **65%** indicate that this is the case for self-produced material as a result of **sextortion**[482]. **98%** of authorities indicate that such material is increasing[483].

75% of children surveyed in a study in Finland **had been asked to send** explicit pictures of themselves, while almost **80% had been sent** explicit images and more than **1 in 10** experienced grooming on a **weekly basis**[484].

There are also indications that the **COVID-19 pandemic** has significantly affected the frequency of self-generated sexual content/material involving children. In 2020, the Internet Watch Foundation confirmed 68 000 cases of self-generated imagery,

---

477 See the NCMEC's presentation (in particular minute 45:20) in an online event organised by the European Parliament Intergroup on Children's Rights on EU legislation on the fight against child sexual abuse online, on 15 October 2020.

478 *Ibid.* In 2019, in EU-related reports the amount of new images was 39 614. In 2020, it increased by 1003%. The amount of grooming reports was 240, and it increased by 505% in 2020.

479 NetClean, NetClean Report 2018, accessed 26 April 2021.

480 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 28 January 2016.

481 NetClean, NetClean Report 2018, accessed 26 April 2021.
See also Europol, European Union serious and organised crime threat assessment, 12 April 2021; and Internet Watch Foundation, "Grave threat" to children from predatory internet groomers as online child sexual abuse material soars to record levels', 12 January 2021.

482 NetClean, *NetClean Report 2018,* last accessed 26 April 2021.

483 *Ibid.* The same study indicates that live-streaming of self-produced content is also a significant issue. 57% of law enforcement authorities report that induced self-produced live-streamed content is common or very common in investigations, while two thirds (67%) report that captures of what appears to have been voluntarily self-produced content is common or very common. Some respondents noted the difficulty in many cases of determining if an image has been produced voluntarily or if it is as a result of grooming or sexual extortion (for example, 'an image which appears to be voluntarily self-produced can easily be that of sextortion').

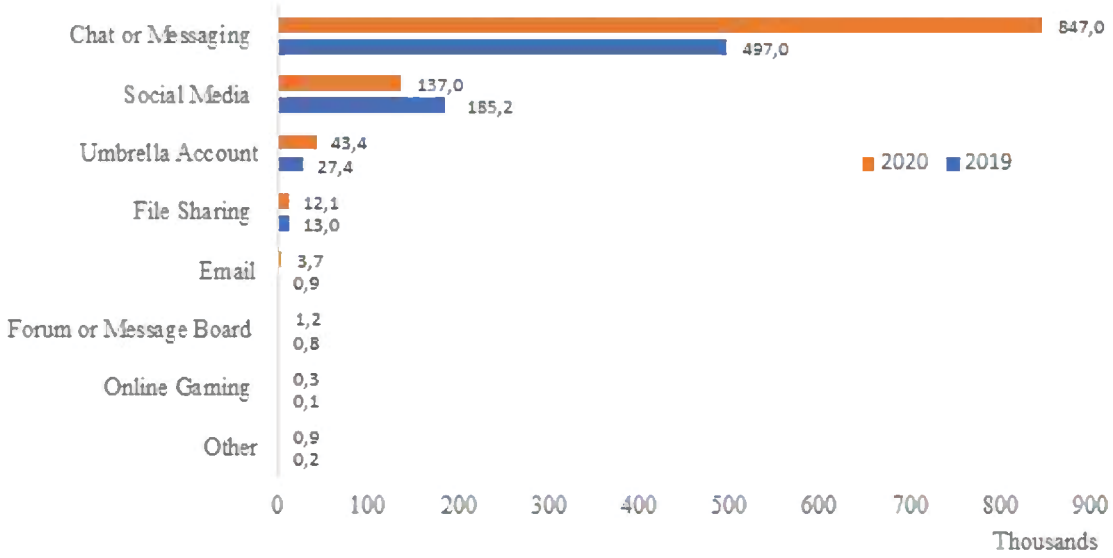
484 Save the Children Finland, 'Osa lapsista saa aikuisilta seksuaalissävytteisiä viestejä viikoittain – ainutlaatuinen selvitys lasten ja nuorten kokemasta groomingista julki', 26 April 2021.

representing **44%** of the imagery on which the IWF took action that year, and an **increase of 77%** in comparison to 2019[485]. In the vast majority of cases (80%), the victims were girls between 11 and 13 years of age[486]. In addition, some law enforcement authorities have seen an increase during the pandemic in young people sharing self-produced material **in exchange for money**[487].

Breakdown by type of service

The vast majority of reports (more than 80% in 2020, up from 69% in 2019) originate in interpersonal communication services (e.g. messenger applications such as Facebook Messenger, and email):

Figure 6: breakdown of reports by type of service in 2019 and 2020[488]



In the case of grooming, 31% of reports in 2020 originated from a chat or messaging service, whereas 68% originated in social media or online gaming platform that had messaging or chat capability.

Figure 7: breakdown of grooming reports by type of service in 2019 and 2020[489]

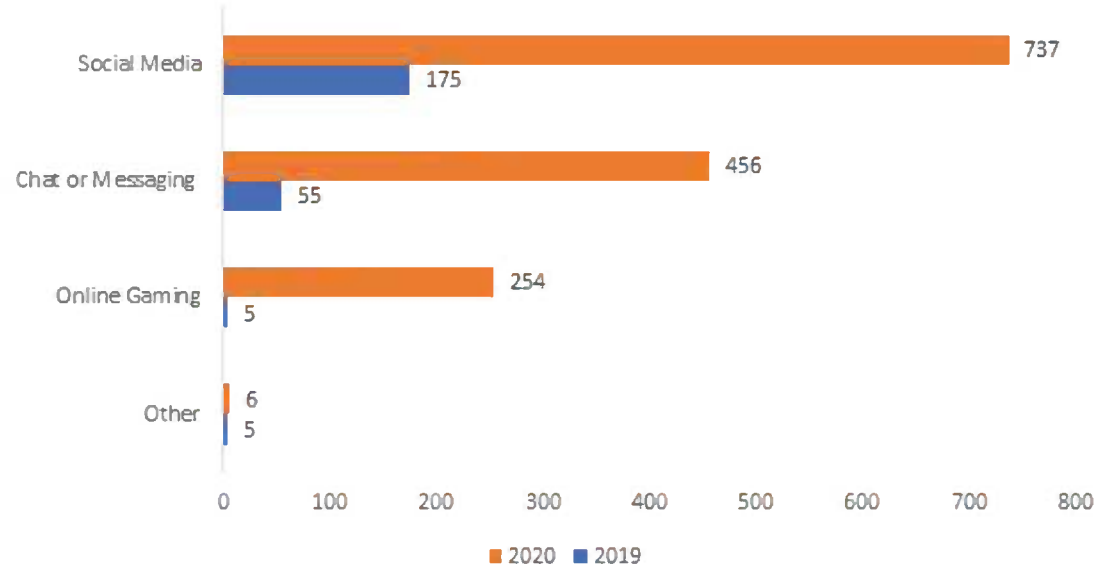
485 Internet Watch Foundation, 'Sexual abusers have never been so social. Self-generated child sexual abuse prevention campaign', last accessed 21 April 2021.

486 *Ibid.*

487 NetClean, *NetClean Report 2020*, last accessed 26 April 2021.

488 The term "Umbrella Account" refers to a company that submits reports on behalf of their multiple products or services (e.g., a company that has file sharing, search engine, and social media products may file all reports under the same name). The term "Other" includes: hosts/providers, marketplace, advertising, adult sites, safety solutions (companies who offer moderation or monitoring services for other platforms).

489 The terms "Social media" and "Online gaming" refer to platforms that have messaging or chat capability. The term "Other" includes: file sharing services, online marketplaces safety solutions (companies who offer moderation or monitoring services for other platforms) or moderations apps.



2.2. *Data on reporting by the **public and hotlines***

The number of reports from the public and hotlines is significantly lower than the number of reports from service providers. For example, in 2020 the 47 members of the INHOPE network of hotlines processed 1 million (1 038 268) URLs, of which 267 192 were unique URLs containing CSAM[490]. In contrast, in 2020 service providers made a total of almost 21.5 million reports to NCMEC[491], as indicated earlier.

According to a 2018 Eurobarometer survey, 6% of EU internet users have encountered CSAM[492]. However, a majority (59%) of users who encountered illegal content online reported that they took no action, while those who did take action were most likely to bring the content to the attention of the provider[493].

In addition to the comparatively low volume of reports made by members of the public, there is also significant variation in the quality of reports. For example, in 2020 Germany's eco Complaints Office found that only **two in five** (40%) public reports relating to child sexual abuse online were justified[494]. In the same year, the Internet Watch Foundation (IWF) found that just 14% of reports of suspected CSAM from members of the public actually constituted CSAM[495]. In 2019 Hotline.ie, the national hotline for Ireland, found that while 85% of reports received were flagged by the reporter as suspected CSAM, just 24% were determined by the hotline's analysts to constitute CSAM[496].

While the majority of hotlines focus solely on receiving reports from members of the public, a small number have begun to **proactively search** for CSAM online in recent years[497]. Proactive searches by hotlines have proven to be highly effective, leading to a

---

490 INHOPE, *Annual Report 2020*, 4 May 2021

491 National Center for Missing and Exploited Children, '2019 Reports by Electronic Service Providers (ESP)', accessed 21 April 2021.

492 European Commission, 'Flash Eurobarometer 469: Tackling Illegal Content Online', September 2018.

493 *Ibid*.

494 eco Complaints Office, *Annual Report 2020*, 13 April 2021.

495 Internet Watch Foundation, *Annual Report 2020*, accessed 4 May 2021

496 Hotline.ie, *Annual Report 2019*, 19 October 2020.

497 Currently, four hotlines search proactively for CSAM: the Internet Watch Foundation (UK), the Canadian Centre for Child Protection, NCMEC (US, through a pilot project), and Švarus internetas

substantially higher quality of reporting than public reports. In 2020, for example, the IWF found that while less than **one in five** (14%) reports of CSAM from members of the public were actionable, over **four in five** (87%) reports resulting from their analysts' proactive search were actionable[498]. As a result, the **overwhelming majority** (87%) of all reports actioned by IWF in 2020 resulted from proactive search[499].

***

Despite the increasing volumes of CSA online reported, it is not possible to determine exactly the actual amount of CSA online that is taking place at the moment. Given the hidden nature of the crime, it is likely that the reported cases are just the tip of the iceberg. To given an indication of the amount of CSAM that circulates, during the arrest of just one child sexual offender in Germany in 2019, the police confiscated 14 terabytes of CSAM, including more than three million photos and 86,000 videos[500]. And the takedown of a single darkweb forum ("Boystown") dedicated to exchange CSAM showed that it had more than 400 000 registered users[501].

(Lithuania, in limited form). See: European Commission, *Study on framework of best practices to tackle child sexual abuse material online*, 2020.

498 Internet Watch Foundation, *Annual Report 2020*, accessed 4 May 2021.

499 *Ibid.*

500 DW, Child sex abuse at German campsite: How authorities failed the victims, 5 September 2019.

501 Europol, 4 arrested in takedown of dark web child abuse platform with some half a million users, 19 November 2021.

ANNEX 7: SAMPLE CASES OF CHILD SEXUAL ABUSE ONLINE IN THE EU

Sample cases in the EU that started with <u>detection of images and/or videos</u>

The following are actual, anonymised sample cases shared by law enforcement agencies in the EU. All the cases started with the detection of child sexual abuse images and/or videos on online services.

<u>Austria</u>

- Case # 1:
  - Austrian law enforcement received in 2019 a report from NCMEC submitted by Facebook alerting of the distribution via **Facebook Messenger** of images and videos of minors performing sexual acts.
  - The investigation led to the identification of a Slovak citizen living in Austria who forced minors through the threat of violence to produce images and videos of themselves performing sexual acts and to send them to him. The material was also distributed online to other users.
  - The report led to the identification of all **30 victims.** The suspect was arrested and convicted to five years of imprisonment.
- Case # 2:
  - Austrian law enforcement received in 2019 a report from **KIK Messenger** alerting of the distribution of child sexual abuse material.
  - The investigation led to the identification of an Austrian citizen.
  - The search of his house and further investigations revealed that he sexually abused his **2 year old daughter,** who was **rescued**.
- Case # 3:
  - Austrian law enforcement received in 2019 a report from **Snapchat** alerting of the distribution of child sexual abuse material.
  - The investigation led to the identification of an Austrian citizen who had forced several female minors to produce nude images of themselves and provide them to him, under the threat of making publicly available images and videos he made in the bathroom of a soccer field while acting as a referee.
  - The report led to the identification of a **large number of victims**.

<u>Bulgaria</u>

- Law enforcement in Bulgaria received in 2018 a report from the National Child Exploitation Coordination Centre alerting of the distribution of child sexual abuse material through **KIK Messenger**.
- The report led to a criminal investigation in which two mobile phones from a suspect were seized, containing 517 video files with child sexual abuse material.
- The material included videos with **brutal scenes of child sexual abuse** with a child around **2 years old**.

Czech Republic

- Law enforcement in the Czech Republic received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**, initiated by **Google**.
- The report led to a criminal investigation in which a 52 year old man was arrested following a house search, where additional child sexual abuse material was found.
- This person had abused **2 girls** and recorded the abuse. The 2 girls were identified and rescued.

Denmark

- Case # 1:
    - Following reports from KIK alerting of the distribution of child sexual abuse material through **KIK Messenger**, Danish authorities arrested, a Danish national in his forties with no criminal record.
    - During preliminary examination of his mobile phone, Danish police found several recordings of himself abusing his **10 year old daughter**.
    - The **10 year old victim was rescued** and the suspect is undergoing criminal proceedings.

- Case #2 - Operation Umbrella[502]:
    - Facebook reported to the National Center for Missing and Exploited Children (NCMEC) the distribution of videos via **Facebook Messenger**[503] depicting a Danish boy and a girl who were engaged in sexual activity.
    - NCMEC forwarded the case to Denmark via Europol.
    - Over 1000 people had distributed the videos to one or more people via Facebook Messenger and were charged for distribution of child pornography.
    - This operation, still ongoing, is the single **largest operation ever** against child sexual abuse in Denmark.

Estonia

- Law enforcement in Estonia received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The report led to a criminal investigation in which a person was arrested for exchanging and possessing child sexual abuse material.

France

- Case # 1:

---

502 Europol, Internet Organised Crime Threat Assessment, 18 September 2018, p. 32.
503 The case was also reported in the media (in English).

- French police received in 2018 a NCMEC report submitted by Facebook alerting of the distribution of child sexual abuse material via **Facebook Messenger**.
- The investigation revealed that the offender provided **PlayStation codes** to young boys in exchange of child sexual abuse material.
- The offender was arrested. There were around **100 victims**.

- Case # 2:
  - French police has received a number of cases from NCMEC submitted by KIK alerting of the distribution of child sexual abuse material via **KIK Messenger.**
  - The cases typically involve multiple offenders (up to **20 offenders** per case).
  - The cases have led to **multiple arrests**.

Germany

- German Federal Police received a NCMEC report in July 2019 submitted by Facebook alerting of the distribution via **Facebook Messenger** of material showing the sexual abuse of a very young girl.
- The NCMEC report also indicated that the material could have been recently produced.
- The report led to a criminal investigation and a house search in which a suspect was incriminated with abusing **his 4 year old daughter, and his 10 year old son**, who were **rescued and safeguarded**.

Greece

- Greek police received two NCMEC reports submitted by Yahoo! informing about a user who exchanged child sexual abuse material via **Yahoo!'s messenger** service.
- The house search of the offender revealed that he was also in contact, via Skype, with individuals (mothers of underage children) in the ASEAN region and was sending money to them so they would send him indecent pictures of their underage children.
- The ASEAN authorities were notified of all the details.

Ireland[504]

- Law enforcement in Ireland received in 2013 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The material was detected by Microsoft when Matthew Horan used a **Gmail** account to send child sexual abuse material to an email address on **Microsoft's** platform.
- The report led to an investigation in which it was discovered that Horan had been sexually exploiting children.
- Irish police identified **six victims** in Ireland as a result of the investigation.

[504] The case was also reported in the media.

Romania[505]

- Romanian police received in 2016 a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
- The investigation revealed that a mother had been abusing her **9 year old daughter** for more than a year and sent the material generated in the sexual abuse to her boyfriend (not the father of the girl) in England.
- The mother was arrested and **her daughter was rescued**.

Sweden

- Case # 1:
  - Swedish police received a NCMEC report alerting that one person had shared two child pornographic images on **Facebook Messenger** of material known to the police.
  - Swedish police carried out a search at the suspect's home and found child sexual abuse material in hard drives.
  - The material included the suspect **abusing his stepdaughter**, who was **rescued** in the operation.
  - The suspect was sentenced to nine years in prison for, among other things, gross rape against children.
- Case # 2:
  - Swedish police received a report from the National Child Exploitation Coordination Centre in Canada in which a person was sharing child sexual abuse material through **KIK Messenger**.
  - A house search was conducted in which child sexual abuse material was found.
  - Thanks to the investigation, **nine Swedish children** were identified.
  - The suspect was sentenced to four years in prison for different child pornography offenses.
- Case # 3:
  - Swedish police received a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
  - The investigation revealed that a female suspect was producing child sexual abuse material with the children of her romantic partners and sharing it with another male.
  - Further investigation revealed a network of two other female producers and three male consumers of child sexual abuse material.
  - **11 victims** were identified and rescued, ranging from ages 2 to 14 when the crimes occurred, out of more than 50 victims in total.

[505] The case was reported in the media, see here and here.

Spain

- Law enforcement in Spain received a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The investigation by law enforcement in Spain led to the arrest of one person, who actively shared online with other child sex offenders the child sexual abuse material he produced.
- The person arrested produced that material by abusing children within his family circle.
- Given the gravity of the situation, law enforcement focused on locating the victims, eventually **rescuing 2 children** within the family circle.

Sample cases in the EU that started with detection of online solicitation

The following are actual, anonymised sample cases of online solicitation in the EU that service providers reported to NCMEC.

Austria

- An adult man enticed an 11-year-old female child via an online chat service to produce and share sexually explicit images.
- An adult man enticed a 12-year-old female child via an online chat service to produce and share sexually explicit images. Chat logs submitted with the report showed the man threatened the child he would notify police if she did not send explicit images and videos. Fearing this threat, the child produced additional content and sent it to her exploiter.
- A 45-year-old man enticed a 13-year-old male child via online private messaging to engage in sexual activity. Chat logs submitted with the report showed the man was talking to the child about leaving the country and making plans to meet the same weekend the report was made to NCMEC. The man was in a position of authority as a coach and talked about wanting to adopt and marry the child.

Belgium

- A 21-year-old man enticed a 14-year-old female child via an online private messaging service to produce and share sexually explicit images. Chat logs submitted with the report indicated the man previously had enticed the child to meet in person so that he could exploit her by engaging in sexual activity.

Bulgaria

- A 15-year-old used an online platform to traffic his 9-year-old girlfriend for sexual abuse exploitation. His reported profile stated:

  *"I'm looking for a pedophile who wants to **** my 9 year old girlfriend and want her to paw him "*

- An adult man used an online chat feature to entice six female children and sent them graphic images of himself engaged in sex acts. At least one of these children

was enticed to create and send an explicit image of herself to the man who then demanded she produce and send more images. When she declined, the man threatened to harm her, saying he "knows where she lives".

- A 51-year-old man used a messaging service to entice a 13-year-old male child to produce and share sexually explicit content of himself. Chat logs submitted with the report indicated the man was the child's uncle, had direct access to him, and discussed specific sexual acts with the child. The chat also indicated the uncle was offering the child money in exchange for sending sexually explicit files.

Croatia

- A 48-year-old man used an online chat service to entice a 14-year-old female child to produce and share sexually exploitative images of herself. The man also enticed her to sexually abuse her 11-year-old sister and said he wanted to meet in person to abuse her. Chat logs provided with the report show the child victim disclosing that she used force to abuse her younger sister, specifically stated the following:

"She screamed"

"It did, but I had to do it by force. She was fighting me....she cried"

Cyprus

- An adult man used the chat function on an online gaming platform to engage in sexually exploitative conversation with another adult gamer about his 13-year-old daughter. The man provided the other adult gamer with his daughter's screenname on another chat platform so the other man could contact the child to "seduce" her.
- A 41-year-old man from Cyprus enticed a 15-year-old child victim from Moldova to produce and send sexually exploitative imagery of herself. Chat logs submitted with the report indicated the man previously had enticed the child to travel to Cyprus so he could exploit her through sexual activity.

Czech Republic

- A 29-year-old man used a private messaging platform to entice a 14-year-old female victim to produce and share sexually exploitative images of herself. Chat logs submitted with the report indicated the man previously had enticed the child to meet in person so he could sexually exploit her. The man lived close to the child and was making plans to meet her so he could continue to sexually abuse her.
- A 29-year-old man enticed five child victims between the ages of 8 and 12 years old. The man enticed two of the children to engage in sex acts, including bestiality, with each other. He enticed another victim to sexually abuse her 3-year-old sibling. Chat logs submitted with the report indicated the man offered money or expensive gifts to the victims to entice them into producing and sharing the sexually exploitative images.

Denmark

- An adult man used a platform's chat function to send sexualized messages about

children to another adult. Chat logs submitted with the report indicated the man planned to sexually abuse his 13-year-old daughter who was intoxicated at the time.

- A 41-year-old man in the United States enticed multiple children under the age of 13 to produce and send sexually exploitative imagery of themselves. This man was communicating online with a 20-year- old man from Denmark and the two men discussed trading sexually exploitative images. At least one child, a 9-year-old female child, was coerced to engage in sexual activity over a video call after being threatened that she would be publicly exposed if she refused.

Estonia

- An adult male created and used multiple online accounts to entice over 12 children, some as young as 9-years-old, to produce and share sexually exploitative imagery. Chat logs submitted with the report indicated that in some cases the man offered to pay the children in exchange for initial images and then coerced to send additional images by threatening to publicly expose their images online.

Finland

- An adult enticed numerous child victims in Finland, Lithuania, Norway, the United Kingdom, and the United States to produce and send sexually exploitative imagery of themselves. After obtaining initial images, this adult would blackmail the children by threatening to send the images to the children's families unless they continued producing and sending additional images. Chat logs submitted with the report indicated the adult also was sharing child sexual abuse material with other adults online.
- An adult man used an online messaging service to engage in sexualized conversations about children with another adult. The man made multiple statements indicating he had sexually abused his young daughter on multiple occasions and had shown her pornography since she was an infant. Chat logs submitted with the report detailed the man's plans to continue sexually abusing his daughter.

France

- A 46-year-old man enticed a 15-year-old female child to meet in person for sexual activity. The man also disclosed he was sexually molesting his minor daughter.
- A 36-year-old man used a platform's messaging service to entice a 14-year-old female child to engage in sexual activity. Chat information provided with the report indicated the man was the child's uncle and had direct access to her.
- A 38-year-old man in a position of trust as a youth football coach used a platform's messaging service to entice a 13-year-old female child to meet for sexual activity. Chat logs submitted with the report indicated the man was a friend of the child's father and had frequent access to her during weekend visits.
- A 48-year-old man enticed a female child to meet for sexual activity. Chat information submitted with the report indicated the man was the child's stepfather

and provided the child with a location where they could meet in secret so that he could sexually exploit her.

- A 28-year-old man enticed a 14-year-old female child to meet for sexual activity. Chat logs submitted with the report indicated the man was the child's half-brother and had direct access to the child victim.
- An adult man enticed several female children between the ages of 14 and 17 to produce and share sexually explicit images. After the suspect coerced the children to produce images, he blackmailed them to produce and send additional content by threatening to publicly expose the initial images he had received. Chat logs provided with the report included the following statements showing the severe distress of the children as the man blackmailed them to produce increasingly egregious content:

"... you really want to ruin my life"
"I've already tried to commit suicide please don't start again"
"It's going to destroy my life"
"I want to die"
"I'm going to kill myself"

- A 42-year old man used a platform's private chat function to entice a 12-year-old female child to engage in sexual activity. Chat logs submitted with the report indicated the man was in a relationship with the child's mother, had direct access to the child, and already had exploited her by forcing her to engage in painful sexual activity:

"I can't anymore with your mom... your Mom and I are done ok"
"We should do it softer... it causes some bleeding usually the first time"
"Wait mom is up... erase everything"

- A 36-year-old man used a platform's messaging service to entice a 14-year-old female child. Chat logs submitted with the report indicated the man was a school teacher in a position of trust and with access to children. Chat logs submitted with the report indicated the man already had met and sexually abused the child and was trying to make plans for future meetings.
- A 46-year-old man used a platform's messaging service to entice a 13-year-old male child to produce and share sexually explicit content. Chat logs provided with the report indicated the man was the child's uncle, had direct access to the child, and had sexually molested the child on multiple occasions. Chat logs also indicated the man was coercing the child to meet him in isolated areas of the home so he could sexually exploit him when no one else was home.

Germany

- A 42-year old man used a private messaging service to entice a 13-year old female child to engage in sexual activity. Chat logs submitted with the report indicated the man had previously enticed the child to meet and had sexually abused her.
- A 32-year-old man used a platform's messaging service to entice a 13-year-old male child to produce and share sexually explicit content. Chat logs submitted with the report indicated the man had enticed the child to sexually abuse his 9-year old

brother and directed him to continue the abuse as indicated by the following statements:

"Go to him in the room"
"Tell him he should open your pants"
"So you don't want to take the virginity of your brother"
"Tell him to give you a blowjob"
"Come on dare to take your brother's virginity and then you were the first who had"

- A 32-year-old man used multiple online personas to entice female child victims to engage in sadistic sexual conversations and produce and share sexually explicit imagery of themselves. Chat logs provided with the report indicated the man also was communicating with an 18-year-old woman who he paid to produce imagery of her sexually abusing her infant child.

Greece

- A 50-year-old man enticed a 14-year-old male child to produce and send sexually exploitative imagery. Chat logs submitted with the report indicated the man had enticed the child to meet in person on previous cases and had sexually abused him. The man also referred to having made videos of himself sexually abusing the child.

Hungary

- A 29-year-old man used a platform's messaging services to entice a 13-year-old female child to engage in sexual acts. Based on the report, it appeared the man had previously enticed the child to meet and sexually abused her and the two lived in close proximity to one another.
- A 40-year-old man used a platform's messaging service to entice a minor female child to meet for sexual activity. Information submitted with the report indicated the man lived in close proximity to the child and knew the child as a friend of her family.
- A 41-year-old man used a platform's messaging service to entice a 12-year-old female child to produce and share sexually explicit content. Chat logs submitted with the report indicated that after coercing the child to send initial images, the man began to blackmail her to produce and send additional content. The man threatened to spread the child's images online if she did not comply and threatened that she had no options but to send more images:

"I have already saved it on my phone so if you don't obey I post it on the web"
"If you do what I say I won't spread your photos on the internet"
"Oh and you can forget about threatening me with the police, I don't care"
"I'm not afraid of the police, I will upload your photos 1000 times by the time the hearings end"

Ireland

- A 29-year-old man used a platform's messaging service to entice a 15-year-old female child to meet and engage in sexual activity. Chat logs submitted with the report indicated the man lived in close proximity to the child and previously had

enticed her to meet in person and sexually abused her. The man also sent several messages to the child urging her to keep their relationship secret because he would go to jail if her parents found out.

Italy

- A 27-year-old man enticed a 12-year-old female child to produce and share sexually exploitative imagery. After the man obtained initial images from the child, he blackmailed her to create and send additional content by threatening to expose her images publicly. Information provided by the reporting company also indicated the man had direct access to children, including his minor daughter.

Latvia

- An adult used a platform's chat room service to entice three children between the ages of 8 to 15 years old. Chat logs submitted with the report referred to the victims appearing nude and the adult's desire to meet the children in person.

Lithuania

- An adult male who used a platform's chat feature to entice a 12-year-old male child for sexual activity. Chat logs submitted with the report detailed the man pressuring the child to expose himself in various degrees of nudity and to engage in sexual acts on camera for the man.

Luxembourg

- The parent of a 15-year-old child in Luxembourg reported that their child was being enticed into a sexual relationship by an adult man in the United States using a social media platform's chat feature.
- An adult used a platform's messaging service to entice a 15-year-old female child to produce and share sexually explicit images of herself.

Malta

- A 20-year-old man used a platform's chat service to entice a child to produce and send sexually exploitative images. The child disclosed the following information: *"we started chatting, he pretended to be a girl. then he started sending live pics of this girl. he is actually a boy so this was all false. then he insisted I send him nudes with my face and threating to release my other nudes. I sent him one and now he has my nudes is is threating to send them to everyone I know. please help me as soon as possible."*
- A 30-year-old man used a platform's messaging services to entice a 15-year-old female child to produce and share sexually explicit content. The man threatened the child:

"You have to do as I say if you don't want to get exposed"
"Otherwise I will show everyone your nudes"

Netherlands

- A 61-year-old man used a platform's messaging service to entice multiple male children to produce and share sexually explicit imagery. Chat logs provided with the report spanned several years and information provided in the report indicated the man was a school teacher and therapist in a position of trust with direct access to children. The man coerced the victims to engage in specific sexual acts, including anally penetrating themselves with foreign objects and also asked several victims if they had access to younger siblings. The man at times groomed the boys by pretending to be a teenage girl or a football recruiter assessing the children's physical fitness by requesting images:

"Do you see your brother of 12 ever naked?"
"1. Everything we talk about, so the fact that I'm going to scout you stays between us. It stays between us as long as I or another scout is coming to visit you at a match. So no telling trainer, parents or friends. You have to promise that... 2. We try a cam session where I interview you and do a body check and different tests. You have to be in a room alone. Is that possible?"
"Show semen in front of the cam"

Poland

- An 18-year-old man used a platform's messaging services to entice an 11-year-old female child to create and share sexually exploitative images. After the man enticed the child to create the initial explicit images, he continued to coerce and threaten the child to create additional images by threatening to publicly expose her.

Portugal

- A 56-year-old male used a platform's messaging service to entice a 15-year-old female child. Chat logs submitted with the report indicated the man asked the child if she enjoyed having sex and whether she performed oral, vaginal, and anal sex. Additional information submitted with the report indicated the man lived in close proximity to the child and had been trying to entice her over chat to meet in person so he could sexually abuse her.
- A 43-year-old man used a platform's messaging service to entice a 16-year-old male child to produce and share sexually explicit content. Chat logs submitted with the report indicated the man had enticed the child to sexually abuse and produce exploitative images of his 12-year- old brother. Chat logs submitted with the reports indicated the man was a success coach in a position of authority and with direct access to children.

Romania

- A 23-year-old woman in Romania used a platform's chat service to coordinate transporting a 13-year- old child victim to an 83-year-old man in Germany so the man could sexually abuse the child in exchange for financial compensation. Chat logs submitted with the report indicated that the woman had access to multiple female children between the ages of 10 and 16 years old, but the 13-year-old child

victim was selected because she was still a virgin:

"parents to the 13-Year-old virgin wants me to give them money before don't trust to give up the girl without giving them money"
"I have the virgin is the 13 year old girl her parents want 5000"
"5000 for the girl and you give us and new a credit ok because the girl is virgin you can do with take whatever you want"

Slovakia

- A 21-year-old Austrian man enticed multiple female children in Slovakia to produce and send sexually exploitative images of themselves over several years. After the man obtained initial images, he would threaten to publicly expose the child to coerce them to create and send additional, and often more egregious, sexual images. One child was coerced to record video of her sexually abusing a younger sister. Two other children expressed suicidal thoughts due to their severe distress while being blackmailed. The man also threatened the children not to disclose the exploitation to trusted adults or law enforcement by telling them he would have them institutionalized or taken away from their families:

"just so you know, I told them that you suffer from mental illness and that you offered me sexual services and that parents cannot take care of you, you will go into kids shelter"

Slovenia

- A Slovenian man used the chat service on an online gaming platform to send sexually exploitative messages regarding children, including that he had sexually molested a child and raped "little kids."

Spain

- A 22-year-old Spanish man enticed a 14-year-old female child in Chile to produce and send sexually exploitative images of herself. After the man obtained the images, he blackmailed the child to produce and send additional exploitative images by threatening to "ruin her life" and disseminate her sexually explicit images publicly. Chat logs submitted with the report indicated the enticement and blackmail caused the child severe distress, and she stated multiple times that she would kill herself if the images were released.
- Two apparent adult women used a platform's chat service to engage in sexualized conversations about children. One of the women disclosed she had sexually molested her 10-year-old daughter on multiple occasions and provided details of the abuse at the request of the woman she was chatting with.

Sweden

- A 31-year-old man used a platform's private messaging service to entice a 14-year-old female child to engage in sexual activity. Chat logs submitted with the report indicated the man already had enticed the child to meet in person and had sexually abused her and also indicated the man had produced a child sexual abuse video by recording his exploitation of her.

ANNEX 8: TECHNOLOGIES TO DETECT CHILD SEXUAL ABUSE ONLINE

This annex provides additional information on technologies to detect child sexual abuse online, i.e. known material, new material and grooming[506].

The examples given below are some of the most widely used, and this is not intended to be an exhaustive listing. Many of these tools are made available to service providers, law enforcement and other organisations where a legitimate interest can be shown. Typically, these tools are combined with human review to ensure the maximum possible accuracy.

General considerations

- These technologies answer the question "is this content likely to be child sexual abuse, yes or not?" not the question "what is this picture about? what is this conversation about?" In other words, the tools look for **specific indicators** of possible child sexual abuse.
- Error rates: given the costs (e.g. human moderation, legal redress) and the reputational risks for service providers, these have an incentive to ensure that the error rate is a low as possible before they use these technologies. High error rates (e.g. incorrectly flagging as child sexual abuse content that it is not), would be quickly detected in the current system by NCMEC and/or law enforcement in the EU as the ultimate recipient of the reports.
- Human moderation: human review reduces the error rate to close to zero. It is already typically in place even for the most accurate technologies such as hashing.

1. Known child sexual abuse material

Technologies used to detect known CSAM are typically based on hashing. **Hashing technology** is a type of digital fingerprinting. Many variations and implementations of hashing technology exist, including Microsoft's PhotoDNA[507], which is the most widely used tool of this type.

PhotoDNA has been in use for more than 10 years and it was developed by academics at Dartmouth College in cooperation with Microsoft. While the original PhotoDNA detects known CSAM in images, a version for detecting CSAM in videos is also available[508].

PhotoDNA works as follows[509]:

1) Detection:
   - The tool first identifies images above a certain size.
   - The tool focuses on images only and ignores text, i.e. it does not read the body of the email or extract any other information transmitted in the one-to-one message (it does not recognise faces in the images, or other contextual information). In

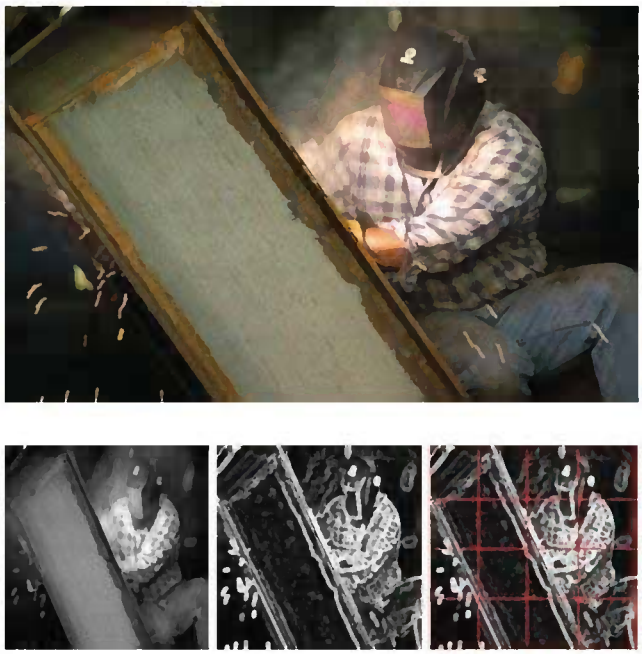
[506] See here for a visual explanation of how these technologies work (minute 24:28) by Professor Hany Farid, who lead or co-lead the creation of Microsoft's PhotoDNA to detect known images and of Microsoft's grooming detection tool.
[507] Microsoft, PhotoDNA, accessed on 14 May 2021.
[508] Microsoft, How PhotoDNA for Video is being used to fight online child exploitation, September 2018.
[509] See here for a visual explanation on how PhotoDNA works.

other words, it does not answer the question "what is this message about?" but the question "is this image known?"

2) Creating a unique digital signature (known as a "hash") of the image (see figure below)[510], through the following process:
   - Convert a full-resolution color image (top) to grayscale and lower resolution (bottom left);
   - Use a high-pass filter to highlight salient image features (bottom center); and
   - Partition the high-pass image into quadrants from which basic statistical measurements are extracted to form the PhotoDNA hash (bottom right).

   This hash is unique and irreversible (the image itself cannot be re-created from the hash).

Figure 1: hashing process



3) Matching:
   - The hash is compared with those in a database of hashes of known child sexual abuse material. If the image hash is not recognised, no information is kept.
   - The main and largest database of hashes (around 1,5 million) is held by the National Center for Missing and Exploited Children, a public-interest, non-governmental organisation established by US Congress in 1984 to facilitate detection and reporting of child sexual abuse material.
   - The criteria for an image to be converted into a hash added to the database of the National Center for Missing and Exploited Children is the following:
     - Children (prepubescent or pubescent) engaged in sexual acts.
     - The sexual contact may involve the genitals, mouth, or digits of a perpetrator; or it may involve contact with a foreign object.

[510] Farid, H., Reining on online abuses, *Technology and Innovation*, 2018.

- An animal involved in some form of sexual behaviour with a pre-pubescent child.
- Lewd or lascivious exhibition of the genitalia or anus of a pre-pubescent child.
- Images depicting pubescent children contain children that have been identified by law enforcement (therefore ensuring that they are actually minors).

- Every hash has been viewed and agreed upon as being child sexual abuse material by two different experts at the National Center before it is included in the database.

PhotoDNA has a high level of accuracy[511]. PhotoDNA has been in use for more than 10 years by over 150 organisations globally[512] including service providers (Microsoft, Facebook, Twitter, Apple[513]), NGOs (e.g. NCMEC, Internet Watch Foundation) and law enforcement in the EU (e.g. Europol, DE, SE and others). In these 10 years, the tool has been used daily and analysed hundreds of billions of images without any accuracy concerns being identified.

Other examples of hashing technology used for these purposes, and operating on similar principles, include YouTube CSAI Match[514], Facebook's PDQ and TMK+PDQF[515]. In addition to these implementations of hashing technology used specifically to detect known CSAM, other variations are used in a range of applications, including the detection of **malware**[516] and **copyrighted content**[517].

2. New child sexual abuse material

Technologies currently used for the detection of new CSAM include **classifiers and artificial intelligence** (AI). A classifier is any algorithm that sorts data into labelled classes, or categories of information, through **pattern recognition**.

Examples of classifiers include those that can detect nudity, shapes or colours. Classifiers need data to be trained on and their accuracy improves the more data they are fed.

---

511 The rate of false positives is estimated at **no more than 1 in 50 billion**, based on testing (Testimony of Hany Farid, PhotoDNA developer, to House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, 16 October 2019).

512 Microsoft provides PhotoDNA for free. Organisations wishing to use PhotoDNA must register and follow a vetting process by Microsoft to ensure that the tool is used by the right organisations for the exclusive purpose of detecting child sexual abuse material. The tool can be used to detect child sexual abuse material in various services (e.g. hosting, electronic communications) and devices (e.g. by law enforcement to detect known child sexual abuse material in a suspect's device).

513 More information is available here.

514 YouTube CSAI Match

515 Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer

516 Sikorski, Michael and Honig, Andrew, Practical Malware Analysis, February 2012; Kapersky Daily, 'The Wonders of Hashing', 10 April 2014.

517 TechCrunch, 'How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff)', 30 March 2014.

Thorn's Safer tool[518] is one example of industry's ability to detect child sexual abuse material. Safer can be deployed by a company as a modular solution to identify, remove, and report child sexual abuse imagery. A company using Safer can utilize the tool's hash matching technology to identify known CSAM, and can choose to expand detection by utilizing the tool's machine learning classification model that can detect both known and potentially new, unreported CSAM. This classifier, developed by Thorn and integrated into Safer, returns a prediction for whether a file is CSAM and has been trained on datasets totalling hundreds of thousands images. It can aid in the identification of potentially new and unknown CSAM.

Thorn's CSAM Classifier can be set at a 99.9% precision rate[519]. With that precision rate, 99.9% of the content that the classifier identifies as CSAM is CSAM, and it identifies 80% of the total CSAM in the data set. With this precision rate, only .1% of the content flagged as CSAM will end up being non-CSAM. These metrics are very likely to improve with increased utilization and feedback.

Other tools making use of classifier and AI technology to detect previously new CSAM include Google's Content Safety API[520], and Facebook's AI technology[521].

In some cases, the search for new CSAM is undertaken if known CSAM has been found with that user. In this case, once the known CSAM is identified on an account, it uses classifiers to assess the content of the account to identify if it has a high probability of containing CSAM.

In other cases, the search for new CSAM with classifiers is undertaken in parallel to the search of known CSAM[522].

3. Grooming (solicitation of children for sexual purposes)

Tools for the detection of grooming in text-based communications make use of technologies solely to detect patterns, which point to possible concrete elements of suspicion of online child sexual abuse without being able to deduce the substance of the content. While not identical in function, these tools use technology similar to the one used in spam filters[523].

Tools of this type include the tool developed under Microsoft's Project Artemis[524], developed in collaboration with The Meet Group, Roblox, Kik and Thorn.

The technique is applied to text-based chat conversations. Conversations are rated on a series of characteristics and assigned an overall probability rating, indicating the

---

518 Thorn's Safer tool.

519 Data from bench tests.

520 Fighting child sexual abuse online

521 See here and here for more information on Facebook's tool to proactively detect child nudity and previously unknown child exploitative content using artificial intelligence and machine learning.

522 See for example, How WhatsApp Helps Fight Child Exploitation. Examples of behavioural classifiers used are the speed/amount of users that join and leave a group, the frequency of group name change, or whether the group contains members previously banned.

523 For more information about content spam filters see here and here and for other spam filters see here, here and here. Spam filters are usually run with the receiving end-user's consent. Some spam filters look only at the subject line of the email.

524 Microsoft shares new technique to address online grooming of children for sexual purposes

estimated probability that the conversation constitutes grooming. These ratings can be used as a determiner, set by individual companies, to address flagged conversations for additional review.

Microsoft has reported that, in its own deployment of this tool in its services, its **accuracy is 88%.**

ANNEX 9: ENCRYPTION AND THE FIGHT AGAINST CHILD SEXUAL ABUSE

1. Overview

This annex provides further information on the role of encryption in the dissemination of child sexual abuse materials and the grooming of children, to explain the rationale behind the measure obliging companies to detect child sexual abuse (CSA) regardless of technologies employed, including encryption. It outlines the different instances where encryption is encountered in the context of the fight against child sexual abuse, and the challenges it may pose to detecting instances of child sexual abuse and combating this crime. This annex informs of developments in the EU and more broadly and gives an understanding of the work of the Commission on the different aspects of the problem.

The shift towards greater interactions and activities in the online space resulted in the widespread and increasing use of different forms of encryption to safeguard web browsing, interpersonal communications, live streaming video chats and private messaging, and to safeguard data in online and offline storage solutions. Encryption has become an indispensable tool for the protection of fundamental rights, including privacy, confidentiality of communications and personal data[525]. It provides a secure means of communication for journalists, dissidents and vulnerable groups[526] and is essential is securing digital systems and transaction[527]. All this puts encryption at the heart of digital security, fuelling developments in this area of technology and others that are reliant on it.

However, if used for criminal purposes, it can mask the identity of offenders, hide the content of their communications, and create secure channels and storage for perpetrators where they can hide their actions, including the trading of images and videos of illegal content. During a high-level dialogue, law enforcement and the judiciary noted[528] that encryption has pervaded the vast majority of their caseload and has impacted the ability to gain lawful access to electronic evidence in between 25% and 100% of their cases- depending on the crime area. They estimated that the use of encryption technology by criminals, will continue to increase. Europol's 2020 internet Organised Crime Threat Assessment (iOCTA)[529] highlighted encrypted communication as the biggest issue that has frustrated police investigations in recent years.

Children are vulnerable to multiple risks whilst online, including grooming and being coerced into producing self-generated imagery for the abuser's consumption and blackmailed to meet in person with abusers. Material produced, is often re-shared and utilised as currency by perpetrators to join online abuser platforms.

---

525 Existing European Union legislation specifically refers to the use of encryption as a possible measure to ensure an appropriate level of security for the protection of the fundamental rights and strengthening cybersecurity: Article 32(1a), 34(3a), 6(4e), recital (83) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; recital (60), article 31(3a) of the Law Enforcement Directive; recital (20) in conjunction with article 4 of the ePrivacy Directive 2002/58/EC; recital (40) of Regulation (EU) 2019/881 (Cybersecurity Act).

526 Carnegie, Moving the Encryption Policy Conversation Forward, 10 September 2019.

527 EU Strategy to tackle Organised Crime 2021-2025

528 Information gathered from a high-level stakeholder dialogue on encryption with prosecutors. Held with the European Judicial Cybercrime Network (EJCN) at Eurojust on 13th November 2019.

529 Europol's Internet Organised Crime Threat Assessment (IOCTA) 2020 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Offenders perpetrating crimes of child sexual abuse are generally quite sophisticated in their use of technology and technical capabilities including effectively exploiting various types of encryption and anonymity[530]. Law enforcement has noted an increase and broader use of encryption to store and distribute child sexual abuse material (CSAM) with impunity. The increase in use of digital technologies, including encryption, has allowed offenders from around the globe that would have probably never known each other in pre-Internet times to chat and exchange materials freely in digital safe havens. Perpetrators actively encourage offline abuse for the purpose of producing new 'high-value' material and normalise this crime.

Encryption of data "at rest" and "data in motion":

Encryption technology can be used to safeguard both **data "at rest"** i.e. data that is stored on devices, external hard-drives and thumb drives in the offline environment and online, e.g. in cloud storage sites, and **data "in motion"** – data that is safeguarded whilst being transferred from one device to another, normally with end-to-end encryption (E2EE). These two different facets of criminals' use of encryption raise their own unique concerns.

1. Encryption of data "at rest":

Encryption of data "at rest" is relevant for the purposes of the present initiative when it is offered by relevant service providers, such as cloud hosting providers. These providers may offer encrypted storage space to customers, either retaining access to the stored content or only granting access to the user. The use of encryption is particularly relevant for image and video storage, as it allows the storage of CSAM in an online folder which can be accessible to several individuals, making it a popular choice for the sharing of CSAM without having to send materials.

2. Encryption of data "in motion":

End-to-end encryption (E2EE) is used to safeguard data "in motion" and gives rise to a different set of challenges. A number of interpersonal communications service providers already make E2EE available by default or by choice on their services. The impact on the possibility to detect child sexual abuse is significant.

E2EE safeguards communications by preventing third parties, as well as the online service providers themselves, from having access to the messages. Messages are encrypted by the sender's device, sent to the recipient's device, and decoded by the recipient using a set of public and private cryptographic keys known only to the devices involved in the communication. It is possible to intercept messages, however, they cannot be viewed or monitored by the service provider, law enforcement or any other third party. While E2EE implemented in communications services therefore provides increased privacy protections, as a consequence, it may also prevent companies from effectively detecting conduct that goes against their terms of service, as well as illegal activities such as the sharing of CSAM among offenders and grooming and coercion of children for the purpose of sexual abuse including the self-generation of CSAM. The tools currently used by industry to reliably detect known child sexual abuse materials do not work in E2EE electronic communications.

While some service providers have created other tools to attempt to limit CSA on their services, the use of E2EE limits the available evidence, so that even where a service provider

[530] Europol, Internet Organised Crime Threat Assessment, 5 October 2020; Independent Inquiry into Child Sexual Abuse, The Internet Investigation Report 2020 March 2020; Virtual Global Taskforce Online Child Sexual Exploitation, accessed 29 April 2021.

suspects that CSA is happening on their services, sufficient evidence will usually not be available to report and thus allow law enforcement to investigate.

This becomes evident when comparing two of the most widely used messaging services, Facebook Messenger and WhatsApp, which are both part of Facebook and subject to the same overall company policy of zero tolerance for child sexual abuse. Facebook Messenger, which is currently unencrypted, is at the origin of more than half of total reports to NCMEC in 2019, with more than 11 million reports.

WhatsApp, on the other hand, is end-to-end encrypted. Detection efforts on WhatsApp are therefore based on a triangulation of unencrypted metadata and behavioural analysis to detect anomalies that may signal harmful behaviour. It is supported by information extracted from unencrypted data e.g. names of the group chat and public profile pictures and users' reports. Facebook states that, using this approach, WhatsApp detects and bans over 300 000 accounts per month[531] on suspicion of sharing child sexual abuse material e.g. use of CSAM in profile pictures or a group name that references CSA. In most of these cases, there is insufficient suspicion of CSA to generate a report to NCMEC, and as a result, in 2020 the company made only 400,000 reports to NCMEC, which amounts to 11% of instances of banned accounts.[532] However, the mere banning of accounts leaves victims without any hopes of receiving help, as no law enforcement organisation is informed of the abuse and the problem is simply pushed off the platform. This example shows that current solutions for the detection of child sexual abuse in encrypted environments are not yet up to the challenge of reliably detecting child sexual abuse in a way that can also result in support for the child victim.

This development has created concerns also beyond the European Union. The United Kingdom, United States, Australia, Canada, India, Japan and New Zealand raised concerns about the growing trend toward E2EE in electronic communications, and its impact on child safety, in an international statement on "end-to-end encryption and public safety[533]". The statement mentions the significant challenges E2EE poses to public safety, especially to children who are vulnerable to exploitation and called on companies to ensure that deployment of E2EE is not done in a way that undermines companies' abilities to identify and respond to violations in their terms of service including on the sexual abuse of children. They are supported by a coalition of child protection organisations who called for actions to ensure that measures to increase privacy, including the use of E2EE does not come at the expense of children's safety[534].

At the same time, finding solutions is not evident. The **consultation process** underpinning this impact assessment to prepare a proposal for a regulation on combating the sexual abuse and sexual exploitation of children yielded a variety of different viewpoints with respect to the issue of encryption. Stakeholders warned against introducing flaws into the E2EE set-up that could create vulnerabilities that jeopardise the privacy and security of communications for all citizens. They agreed that technology, including encryption has an integral part to play in solutions that keep children safe. A number of stakeholders rejected the concept that there has to be a binary choice between maintaining privacy and protecting children, advocating for

---

531 Figures obtained from a position document that Facebook sent to the European Commission, in response to efforts taking place in a Commission-led expert process to identify technical solutions that could help companies detect child sexual abuse in end-to-end encrypted electronic communications. Also shared on WhatsApp's FAQ section: *How WhatsApp Helps Fight Child Exploitation.*

532 Wired report: Police caught one of the web's most dangerous paedophiles. Then everything went dark.

533 The United States Department of Justice, International Statement: End-to-end Encryption and Public Safety, 11 October 2020.

534 Letter to Facebook from a coalition of child protection organisations and experts on concerns regarding the company's proposals to implement E2EE across Facebook's messaging services of 6th February 2020.

privacy-preserving solutions that protect of children in encrypted environments. Stakeholders saw the need for frameworks that are inclusive of both existing and emerging techniques to tackle abuse and reflect the varied and dynamic nature of online communications, considering the different properties of companies that offer such services[535]. In aligning these concerns, any measures taken must be rigorously tested and must be proven to be reliable and accurate. Their proportionality, necessity and limitation in scope must be guaranteed[536].

To assess whether solutions were even technically feasible, the Commission set up a technical expert process under the EU Internet Forum, in line with the EU Strategy for a more effective fight against child sexual abuse. This process aimed to map and assess possible technical solutions which could allow companies to detect and report CSA in E2EE electronic communications, in full respect of fundamental rights and without creating new vulnerabilities that criminals could exploit. The process brought together technical experts from academia, industry, public authorities and civil society organisations.

The possible solutions considered would allow for the use of both existing technologies (e.g. matching of unique signatures of material – hashes – to content that has been confirmed as CSAM) to detect CSA as well as upcoming technologies to the extent known at present, whilst maintaining the same or comparable benefits of encryption. The approach used was purely technical with each solution assessed from a technical point of view across five criteria; effectiveness, feasibility, privacy, security and transparency. A number of promising solutions were identified during this process that help to reconcile the specific safeguarding needs of children through detection and reporting of CSA and with the full respect of fundamental rights of privacy and data protection.

The expert process and its outcomes were presented to Justice and Home Affairs Ministers at the EU Internet Forum Ministerial meeting of 25th January 2021[537]. Ministers taking part in the meeting agreed on the need for further efforts to overcome the challenges that E2EE poses to the detection of child sexual abuse on encrypted platforms and noted that this process is a first step in looking for feasible solutions that provide the right balance to help combat and eradicate CSA online and offline. The expert process complements the voluntary efforts that a number of technology companies have already been engaging in and attests to the importance of better alignment and collaborative efforts to safeguard children, whilst providing proof of concept of the existence of possible technical solutions.

The Commission has also announced that it will support research to identify which technical solutions are the most feasible and could be scaled up and feasibly and lawfully implemented by companies and continue to engage with key players in the technology industry who are best placed to pioneer new technologies that can contribute effectively to the fight against CSA.

The relevant sections from the paper summarising the findings of the expert process are reproduced in the following section. The paper summarises the technical views of the experts and has not been formally endorsed by the Commission.

---

[535] Digital Europe- response to open public consultation on upcoming legislation to fight child sexual abuse: detection, removal and reporting of illegal content online.

[536] EDRi- general views, open public consultation on upcoming legislation to fight child sexual abuse: detection, removal and reporting of illegal content online.

[537] Press Release: EU Internet Forum Ministerial- Towards a coordinated response to curbing terrorist and child sexual abuse content on the Internet, 26 January 2021.

2. Technical solutions to detect child sexual abuse in end-to-end encrypted communications

Scope

This paper covers the **proactive detection**[538] **by companies** of images, videos and **text-based**[539] child sexual abuse such as grooming or sextortion. The scope of the paper is limited to one specific type of online service, **electronic communications**, and one specific type of illegal content, **child sexual abuse (CSA).**

The focus on electronic communications is due to the fact that a large proportion of reports to the National Centre for Missing and Exploited Children (NCMEC) of instances of CSA (around 2/3 of the 16.9 million reports received in 2019, more than 700k of which concerned the EU) originate in this type of online service. These include one to one instant messaging services and email.

This paper:

- **defines the problem** of the detection of CSA content in end-to-end encrypted (E2EE) communications; and
- presents a number of possible **technical solutions** that could allow the detection of CSA in E2EE communications.

A possible solution is one that allows the detection of CSA in E2EE electronic communications using **existing technologies** (e.g. hashing), as well as upcoming technologies, to the extent that these may be known today.

The paper aims to provide **a first technical assessment** to help identify possible solutions. **Substantial additional work**, beyond the scope of this paper, is likely to be needed to further evaluate and eventually develop, and deploy the technical solutions across the companies' infrastructure.

Approach

The approach of the paper is purely **technical**. It aims to reflect in **non-technical language** the input from internationally recognised technical experts from academia, industry and public authorities from around the world, who have kindly contributed with their time and knowledge to help make progress on this matter.

---

538 The document focuses on detection as a first step to tackle this complex problem. The reporting of child sexual abuse after it has been detected is not covered in this document at the moment but it is of course of utmost importance to ensure that actionable and valuable information is provided to law enforcement on a timely basis. Also, the document covers proactive detection by companies, not lawful access by law enforcement with a warrant. The document currently does not cover either the process to develop the technical solutions (e.g. data to train and test the tools, the preparation and maintenance of the database of hashes, etc), also of key importance. Also, the document focuses on solutions that work on real time detection, rather than detection of CSA in messages that have already been sent to the recipient.

539 The technologies and approaches required to detect text-based threats are in general different from those required to detect images and videos. At the moment, the detection of text-based threats is more difficult and presents a higher number of false positives than image and video detection. It is therefore not easy to bundle the assessment and recommendations for text, image and video detection. The assessment of the solutions and the recommendations presented in the paper focuses mostly on image and video detection.

The paper maps possible technical solutions and assesses them from a technical point of view across five criteria (the order does not reflect any considerations on relative importance):

1. **Effectiveness**: how well does the solution **detect and report** known and unknown CSA (images, videos and text-based threats)?[540]
2. **Feasibility**: how ready is the solution and how easily can it be implemented, in terms of **cost, time and scalability**?[541]
3. **Privacy**: how well does the solution ensure the **privacy of the communications**?[542]
4. **Security**: how vulnerable is the solution to be **misused** for other purposes than the fight against CSA, including by companies, governments or individuals?[543]
5. **Transparency**: to what extent can the use of the solution be documented and be **publicly reported** to facilitate **accountability** through **ongoing evaluation and oversight** by policymakers and the public?[544]

2. PROBLEM DEFINITION

The problem that this paper aims to address is the following: given an E2EE electronic communication, are there any technical solutions that allow the detection of CSA content while maintaining the same or comparable benefits of encryption (e.g. privacy)?

In addition to the technical aspects of the problem, which are the focus of this paper, the problem has important **policy** aspects, as it lies at the core of the debate over the privacy, cybersecurity and safety implications and trade-offs. Some voices on the safety side of the debate push for forbidding E2EE altogether or require the existence of generalised exceptional access mechanisms, whereas some voices on the privacy side would reject any solution that allows the detection of CSA in E2EE communications, as they would put the privacy of communications above anything else.

This document aims at mapping possible solutions that could ensure the privacy of electronic communications (including the privacy of children) **and** the protection of children against sexual abuse and sexual exploitation. The solutions explored are purely technical in nature, and this paper does not take a position on the related policy aspects.

---

[540] This includes the ability to report to law enforcement sufficient information to enable the rescue of children from ongoing abuse and the prosecution of the offenders, as well as the ability of companies to proactively stop the abuse of their infrastructure to commit CSA related crimes. A solution is also considered more effective if it allows for the detection of CSAM through multiple technologies (e.g. image and video hashing, Artificial Intelligence based tools, etc).

[541] User experience (e.g. no reduction of performance) also determines how ready the solution is to be implemented.

[542] This refers solely to the ability of the technical solution to ensure that neither the company, nor any actor other than the sender and the receiver has access to the content of the communication.

[543] This includes, e.g., the misuse by companies to detect other types of content; the misuse by governments for mass surveillance; the misuse by individuals to cause damage exploiting possible weaknesses that the solution may inadvertently introduce in the infrastructure; and the misuse by individuals to compromise the integrity of the solution to detect CSA and modify it so that it would not work as intended. It is important to note that tech-savvy offenders (who may compromise the solution) are unlikely to use systems that allow the detection of CSA.

[544] Carnegie Endowment for International Peace, *Moving the Encryption Policy Conversation Forward*, Encryption Working Group, September 2019, p14.

3. POSSIBLE SOLUTIONS

0) Baseline solutions

These are immediate solutions that require little or no technical development. They provide reference points for comparison to the other technical solutions.

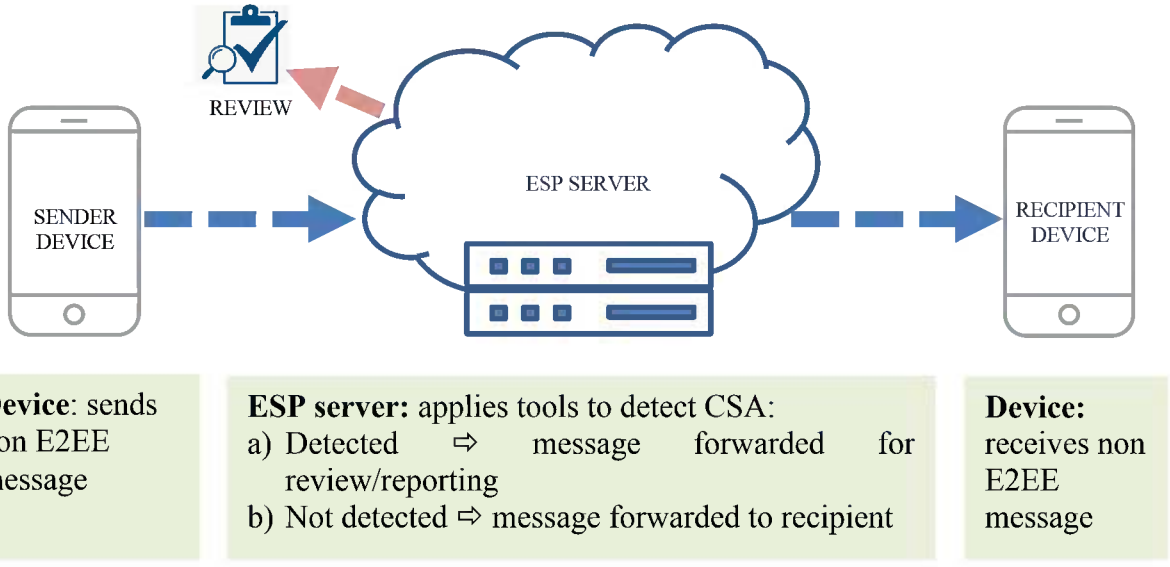
a. Non-E2EE communications

In communications that are not end-to-end encrypted (but which may be encrypted with other client to server protocols such as https), the electronic service provider (ESP) has the ability to apply various tools to detect CSA (images, videos or text) on its server. The most common ones are:

- Hashing tools[545]: they convert the image (or video) into a unique alphanumeric sequence (hash), which is compared with a database of hashes of known images and videos identified as CSA material (CSAM).
- Machine-learning tools: they are trained to detect features indicating that an image or video is likely to constitute CSAM.
- Text-based tools: they detect keywords or text patterns that indicate possible CSA (e.g. grooming or sextortion).

If the tools identify possible CSA, the message is flagged for manual review by a content moderator or reported directly to the authorities.

Figure 1: detection of CSA in communications that are not end-to-end encrypted



Assessment:

- Effectiveness:
  - High: highly effective in detecting and reporting known CSAM and text-based threats (i.e. as effective at detecting and reporting new CSAM as the current technology to detect it allows).

[545] The most widely used hashing tool is PhotoDNA, developed by Microsoft and Professor Hany Farid in 2009. See here for more information on how PhotoDNA works.

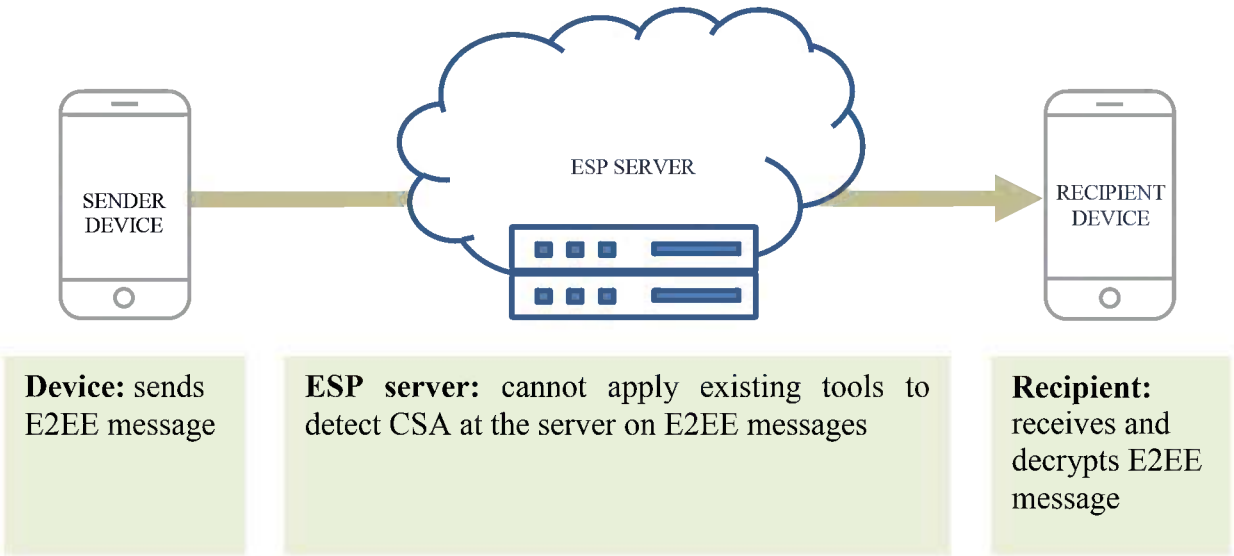
- Feasibility:
  - High: already in use, frequently as the default option.
- Privacy:
  - Low: the content of the communication could in principle be accessed by the ESP at any point (from a technical point of view).
- Security:
  - Medium/medium-low: The communication is relatively secure from unauthorised access by governments and individuals (given the use of e.g. client-server encryption). However, companies can access the content of the communication for other purposes than the detection of CSA.
- Transparency:
  - Medium: whereas the use of tools to detect CSA can be publicly reported (i.e. reports sent to NCMEC), it is not always clear whereas these or similar tools are used to detect other types of content, illegal or not, as oversight mechanisms not always exist.

b. End-to-end encrypted communications[546]

In end-to-end encrypted communications the sender and recipient utilize a public key protocol to agree on a secret session key, which no passive observer including the ESP can determine.

As such, without additional mechanisms, the server is not able to apply the tools to detect CSA, since it does not have the private decryption key and thus no access to the content in clear.

Figure 2: detection of CSA in end-to-end encrypted communications



Assessment:

- Effectiveness:

[546] This baseline solution does not include device, server and encryption related solutions, which will be analysed in the rest of the document.

- None, as it is not possible to detect at the server CSA (images, videos and text-based threats) included in the content of the communication.

➢ Feasibility:
- Not applicable (detection of CSA is not possible).

➢ Privacy:
- High: the content of the communication can only be accessed by the sender and the recipient of the message[547].

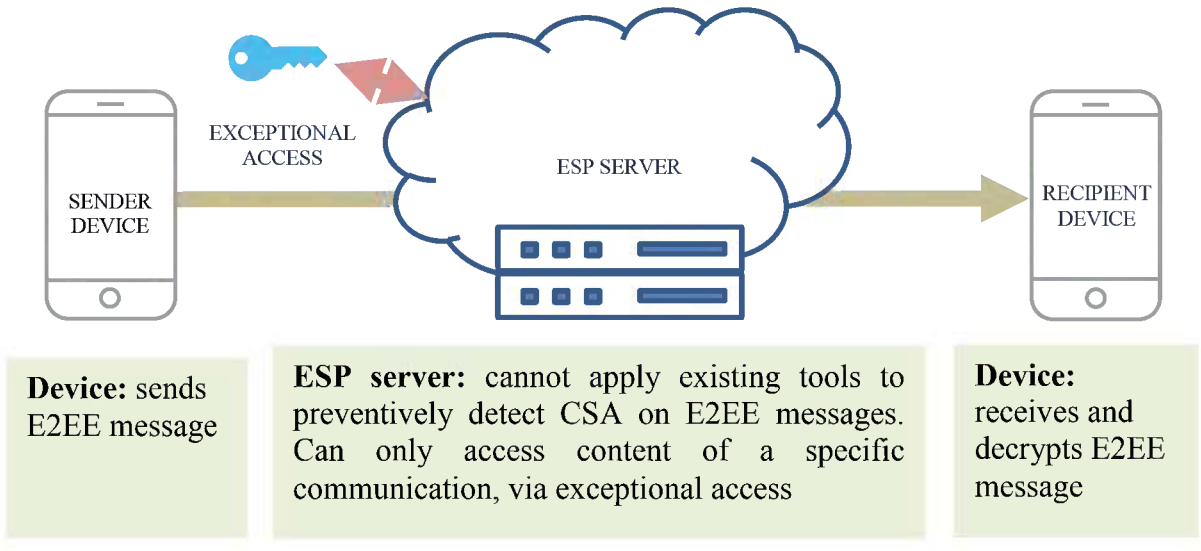
➢ Security:
- Not applicable, since there is no solution to detect CSA that can be compromised.[548]

➢ Transparency:
- Not applicable, since the detection of CSA is not possible.

c. End-to-end encrypted communications with exceptional, targeted access

In this type of solutions, the electronic communications system includes the possibility of exceptional access for the company and law enforcement (e.g. with a warrant), i.e. the possibility to decrypt the content of the communication as the ESP has the encryption keys:

Figure 3: detection of CSA in E2EE communications with exceptional, targeted access



Assessment:

➢ Effectiveness:
- Low: preventive detection (i.e. to reduce the proliferation of CSA and report to law enforcement for action as needed) is not possible. Detection of CSA is only possible for a specific communication, via exceptional access.

➢ Feasibility:

[547] The only part of the communication that is not private, as in all the other solutions discussed in this document, is the fact that the sender sent a message to the recipient (metadata/traffic data).

[548] The 'not applicable' rating is in relation to the definition of security used in this paper, i.e. the security of solutions that allow for the detection of CSA in E2EE communications. End-to-end encryption in itself offers a high level of security to the communication.

- Low: the solution can only be used on the basis of a warrant, where suspicion exists that an individual is committing crimes related to online CSA. It is infeasible for the continuous detection of CSA at scale.

- Privacy:
  - Low: all the content of the communication could in principle be accessed by the ESP at any point (from a technical point of view) using the exceptional access mechanism.
- Security:
  - Medium/Medium-Low: a reasonable expectation for a standard design is to be able to prevent unauthorised access, i.e. prevent hacking the server-side implementation or cryptographically impersonating the ESP. That said, it could be difficult to decide who gets the exceptional access and who does not.
- Transparency:
  - Medium: the authorised use of the exceptional access could be reasonably documented and be publicly reported.

****

There are three basic elements in an end-to-end encrypted communication: device, server and encryption type (see figure 2). These basic elements also determine the three possible types of technical solutions beyond the baseline ones: 1) **device** related, 2) **server** related, and 3) **encryption** related solutions, which the following sections will analyse.[549]

1) Device related solutions[550]

This type of solutions consists in moving to the **device** some or all of the operations done at the ESP server in communications that are not end-to-end encrypted.

The solutions where the device is involved could work both with the sender's device as well as with the recipient's device. Setting the solutions up on the sender's side helps limit the distribution of illegal material, whereas setting them up on the recipient's side helps with detecting grooming. Also, implementing detection solutions on both the sender and receiver's device might mitigate the risk of offenders modifying their apps to defeat the detection mechanisms.

a. All detection done on-device

In this solution, operations for the detection of CSA, i.e. hashing and matching for images and videos, and matching for text, are moved to the device, and applied on the message before it is encrypted. If the tools detect CSA, the message is sent for manual review (or reporting). If they do not, the message is end-to-end encrypted and sent to the recipient:

---

549 Some of these solutions refer to the use of hashes. Hashes can be cryptographic (a small change in the image generates a new hash) or perceptual/robust (a small change in the image does not change the hash). Perceptual hashing has higher effectiveness but somewhat lower feasibility, as the hash set size is larger and more space is needed for the matching process. Cryptographic hashes would reduce effectiveness but be more feasible. The assessment assumes perceptual hashing unless stated otherwise.

550 The detection tools could in principle be incorporated either at the app or the operating system level (although in the latter it could be more technically complex). It might be easier for the ESP to check against manipulation of the detection tools before allowing the operation if they are incorporated at the app level but incorporating the solutions in the operating system may be more effective and efficient to implement.

Figure 4: all detection done on-device

Device: applies tools to detect CSA (e.g. hashing of images and matching with a database of known CSAM). If CSA is:
a) not detected ⇨ encrypts message end-to-end and sends to recipient
b) detected ⇨ sends message for review and/or reporting

ESP server: cannot apply existing tools to detect child sexual abuse on end-to-end encrypted messages

Device: receives and decrypts message

Assessment:

- Effectiveness:
  - Medium: it would allow the detection of known CSAM. Depending on the type of device, the list of hashes may need to be limited to work properly.[551] Updating the hashset with new hashes is slower and thus less effective than a model where the hashset is in the ESPs cloud.
- Feasibility:
  - Medium-low: it could be implemented relatively easily but it would require significant storage space in the device with the current technology[552]. Updating the dataset regularly would also use computational capacity.
- Privacy:
  - Medium: user data is not exposed to the ESP. The possible security issues (compromise and manipulation of detection tools) may introduce vulnerabilities that could decrease the privacy of the communication.

[551] That said, in the case of PhotoDNA, the additional time needed to compare hash databases of increasing size scales logarithmically, not linear. In other words, doubling the size of the database requires one extra comparison, not twice as many.

[552] For example, PhotoDNA hashes could be between 1 to 4 million, which could take around 30MB. Adding video hashes would take even more storage space. Feasibility may be increased by limiting the hash database to include only hashes of the most commonly encountered content or manage the dataset on a device/operating system level.

- Security[553]:
  - Low: the solution could be easily subverted and compromised/reverse engineered to not detect or report CSA (in particular in devices without trusted execution environments) or to detect content other than CSA. It could also be manipulated to introduce false positives to inundate the reporting systems (e.g. NCMEC) with them. The possible leak of detection tools (e.g. hashing algorithm, hash list, keywords list), could reduce the effectiveness of similar detection tools elsewhere.
- Transparency:
  - Medium-low: the possible security issues could limit the reliability of public reporting on the use of the solution and therefore the accountability.

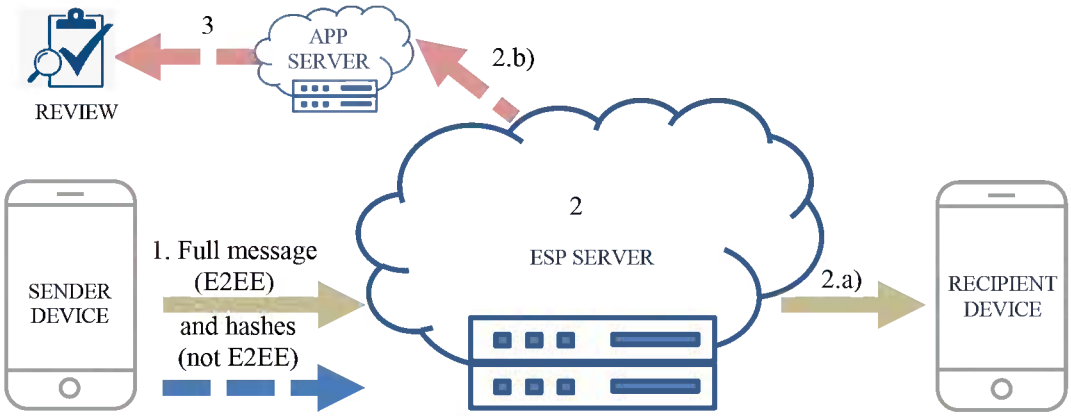
b. On-device full hashing with matching at server

In this solution, the device converts the images and videos in the message into hashes, encrypts the message and sends the (client to server encrypted) hashes and the full message encrypted to the server. The server compares these hashes with those in the database of hashes of confirmed child sexual abuse (matching).

If there is a hit at the server, it instructs the app server to send the full image (or video) for manual review (or reporting). If there is no hit, the server forwards the E2EE message to the recipient.

[553] The security of all solutions that make use of a hashing algorithm could be increased if that algorithm is updated/modified periodically, to reduce the risk of reverse engineering. Ideally, an open-source hashing algorithm very difficult to hack would be best, but it remains to be developed.

Figure 5: on-device hashing with matching at server



1. **Device**: converts the images and videos into hashes before the message is encrypted, encrypts the full message and sends the hashes (client to server encrypted) and the E2EE full message to the server.

3. **App server:** sends full image/video for review if there is a match in the server and/or reporting

2. **ESP server:** compares hashes received from the device with those in the database of hashes of confirmed CSA (matching)
1) No match ⇨ forwards E2EE message to recipient
2) Match ⇨ asks app server to send image/video to review and/or reporting

Device: receives and decrypts E2EE message

Assessment:

- Effectiveness:
  - Medium-high: it would allow the detection of known CSAM only. It would not be applicable to text-based threats (not possible to detect with hashing). No need to limit the hash list, as it will be located at the server.
- Feasibility:
  - High: it could be implemented relatively easily. An open-source version of the solution could be created to be used by smaller companies who may not have enough resources to obtain and maintain a proprietary tool.
- Privacy:
  - Medium-low: user data (hashes) are visible to the ESP. The possible security issues (compromise and manipulation of detection tools) may introduce vulnerabilities that could decrease the privacy of the communication.
- Security:
  - Medium-low: the hashing algorithm in the device could be subverted and compromised/reverse engineered to not detect or report child sexual abuse (in particular in devices without trusted execution environments). It could also be manipulated to introduce false positives to inundate the reporting systems (e.g.

NCMEC) with them. Also, the hash database in the ESP server could be manipulated to introduce non-CSAM hashes. The possible leak of detection tools (e.g. hashing algorithm), could reduce the effectiveness of similar detection tools elsewhere. Also to consider is the possibility that tech-savvy offenders (who may compromise the solution) would not use any system that allows the detection of CSA. These solutions are more likely to be used by non tech-savvy offenders (as is the case of most CSA detected and reported today).

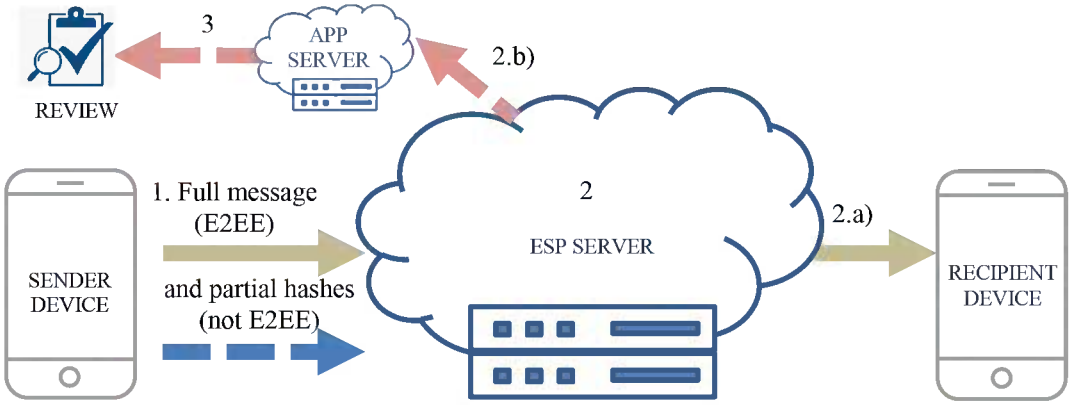
- Transparency:
  - Medium: the possible security issues could limit the reliability of public reporting on the use of the solution and therefore the accountability.

c. On-device partial hashing with remaining hashing and matching at server

This solution is the same as the previous one (1.b.) but in this case part of the hash is generated at the device and the rest at the server, where the matching also takes place[554]. This hybrid approach makes the process lighter and more secure:

[554] The process to create a hash has several steps: downsize the image, convert it to greyscale, etc… (see here for an illustration of the process). In this solution, the first steps to generate the hash are executed at the device and the remaining steps at the server.

Figure 6: on-device partial hashing with remaining hashing and matching at server



1. **Device**: converts the images and videos into partial hashes before the message is encrypted, encrypts the full message and sends the partial hashes (client to server encrypted) and the E2EE full message to the server.

3. **App server:** sends full image/video for review and/or reporting if there is a match in the server

2. **ESP server**: finalises the partial hashes received from the device, and compares the now full hashes with those in the database of confirmed CSA (matching)
a) No match ⇨ forwards E2EE message to recipient
b) Match ⇨ asks app server to send image/video to review and/or reporting

Device: receives and decrypts E2EE message

Assessment:

- Effectiveness:
  - Medium-high: it would allow the detection of known CSAM only. It would not be applicable to text-based threats (not possible to detect with hashing). No need to limit the hash list, as it will be located at the server.
- Feasibility:
  - Medium: proof of concept was done and it could be already in use. Depending on the size of the partial hash (which would determine the payload and upload time), this solution may be faster than 1.b. as it would lift some of the hashing burden from the device. The exact implementation details are important (e.g. to maximize performance) and remain to be defined.
- Privacy:
  - Medium-low: user data (hashes) are visible to the ESP and more information about the image is exposed to the ESP through the partial hash. The possible security issues (compromise and manipulation of detection tools), although improve by exposing the hashing algorithm only partially to, still may introduce vulnerabilities that could decrease the privacy of the communication.
- Security:

- Medium: the device contains only part of the hashing algorithm, which limits the risks of reverse engineering and manipulation. This risk could be further mitigated through obfuscation techniques to scramble pixels without affecting the creation of the hash to ensure that the hash is not reversible.

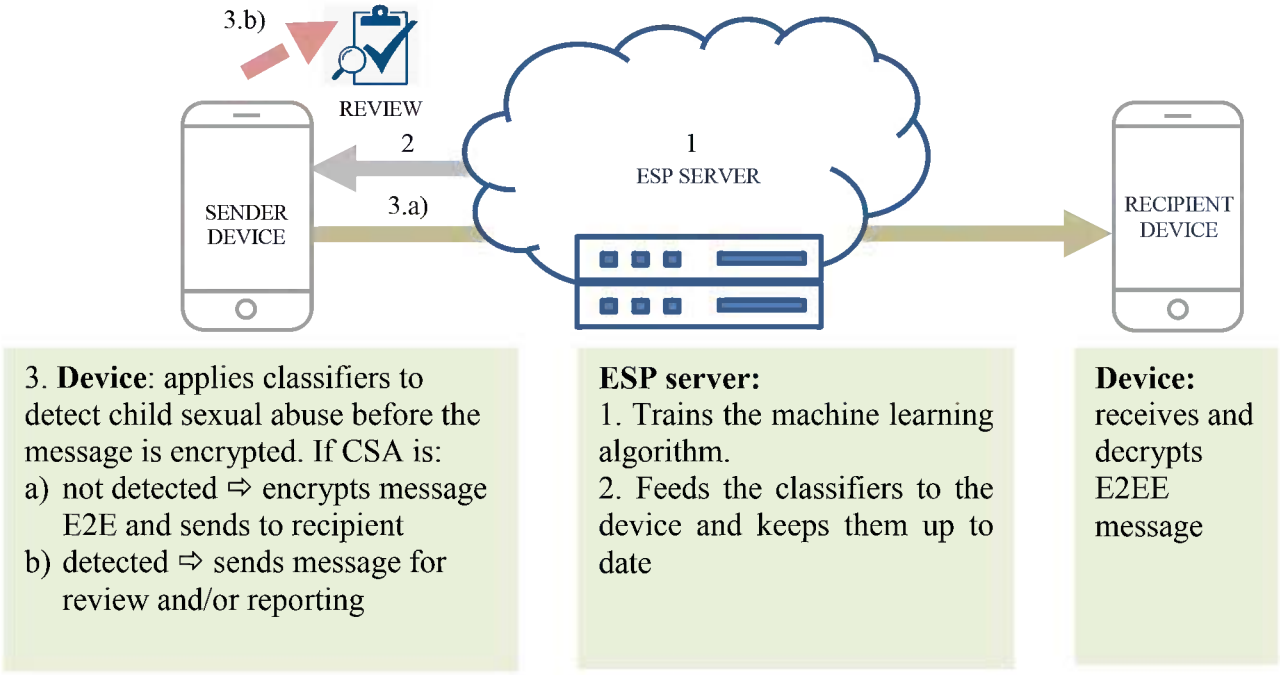
➢ Transparency:

- Medium-low: the possible security issues could limit the reliability of public reporting on the use of the solution and therefore the accountability.

d. On-device use of classifiers

In this solution, the server produces classifiers to identify child sexual abuse (images, videos and/or text) using extensive labelled data of verified child sexual abuse and non-child sexual abuse to train the machine learning system. A classifier is a set of characteristics that can determine whether the contents of a message are child sexual abuse related. The classifiers are then fed to the sender's device, which uses them to determine whether a message should be sent for review or reporting.

Figure 7: use of machine learning classifiers



Assessment:

➢ Effectiveness:

- Medium-low: it is basically the only solution that allows the direct detection of unknown content[555] (in addition to known content). That said, detecting child sexual abuse images and videos using machine learning is still not sufficiently developed and generates relatively high error rates (e.g. compared to hash matching). The machine learning algorithms require well-labelled data on an

[555] Hashing can also indirectly lead to the identification of new content as the known images are usually found together with new ones, which are confirmed as CSA during the manual review of the detected content.

ongoing basis to make sure that the models are kept up-to-date. They also require constant feedback on the quality of the classification, which is particularly difficult to consistently provide in the detection of child sexual abuse in an end-to-end encrypted system. This may result in the algorithms getting outdated relatively soon if they are not updated regularly.

- Feasibility:
  - Medium-low: image classifiers are already in use in cloud services by companies (e.g. to recognize commonly occurring faces in photos or doing automatic grouping of images) and they are also used to detect CSA. That said, significant development is still required, in particular for the detection of images and videos and on the possibility of running classifiers on the client side, given the size and complexity of the models and the need for frequent updates.[556] Classifiers for the detection of text-based threats (e.g. grooming) would be more feasible.
- Privacy:
  - Medium-low: the possible security issues (compromise and manipulation of classifiers) may introduce vulnerabilities that could decrease the privacy of the communication. In the particular case of behavioural classifiers, which determine possible instances of child sexual abuse based on metadata from the user, the privacy intrusion is higher than other tools such as hashing. In addition, a possibly higher rate of false positives could result in user data (not child sexual abuse) being reported / processed / reviewed. Also the classifiers could be misused to identify a range of non-CSA activities.
- Security:
  - Medium-low: the classifiers in the device could be compromised and manipulated to avoid detection (i.e. introduce false negatives), introduce false positives to inundate the reporting systems (e.g. NCMEC) (or even be used by offenders to crawl the web to search for CSA). This kind of attack could be based on sophisticated adversarial machine learning techniques that could defeat any classifier. Being able to detect new child sexual abuse threats exposes the system to be more vulnerable to adversarial attack.
- Transparency:
  - Medium: the use of the solution could be documented and be publicly reported to facilitate accountability, but how the solutions works would be more difficult to document than e.g. 1.c.

2) Server related solutions

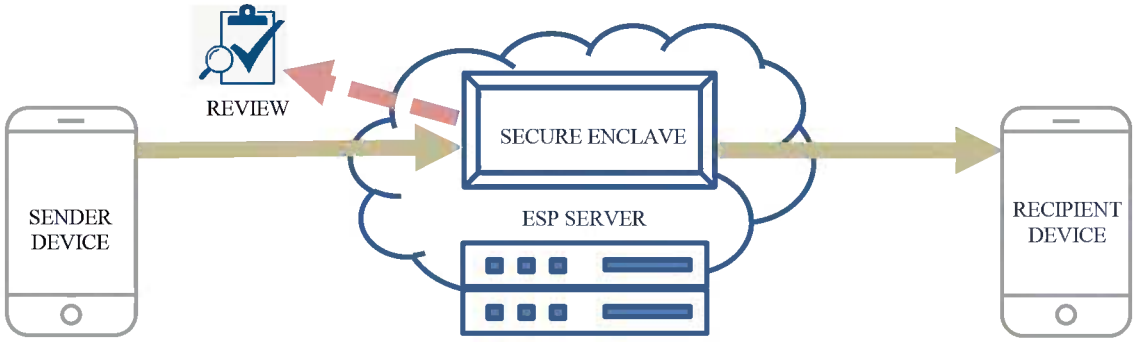
This type of solution consists in **moving to secure enclaves in the ESP server or to third party servers** some or all of the operations done at the ESP server in communications that are not end-to-end encrypted (e.g. client-to-server encrypted).

[556] Current image classifier models can range from 16 to 70 MB, whereas the maximum acceptable size of an app running on the device would be 4-5 MB. Implementation in their current state could have a negative impact on the functionality and costs for persons using lower-end handsets or in lower-bandwidth/high data-cost environments.

a. Secure enclaves in the ESP server

In this solution, the ESP server contains a "secure enclave" that allows compute intensive operations to happen on the cloud, for example in closed off trusted execution environments. The enclave can decrypt the user info and perform the same operations and checks as done in communications that are not end-to-end encrypted (see figure 1), while protecting the sensitive information inside the enclave:

Figure 8: secure enclaves in the ESP server



Device: sends encrypted message to the enclave in the ESP server.	**Secure enclave in the ESP server:** decrypts the message and applies tools to detect child sexual abuse. If CSA is: a) detected ⇨ forwards message for review and/or reporting b) not detected ⇨ encrypts message end-to-end and forwards it to recipient	**Device:** receives and decrypts E2EE message

Assessment:

- Effectiveness:
  - Medium-high: it could allow the detection of known and new CSAM. No need to limit the hash list, as it will be located at the server. This solution also opens up possibilities to develop new technologies to detect child sexual abuse.
- Feasibility:
  - Medium-low: on one hand, it is a solution that simplifies the detection process and similar systems are already in use today for other applications (e.g. Intel's SGX or Software Guard Extensions, in Microsoft's Cloud[557], and other trusted execution environments). On the other hand, only a few companies have access at the moment to the hardware and software required in this solution, given its operational complexity[558] (although the technology may become more accessible in a few years in particular if it is offered as a service by the cloud providers).

[557] Microsoft has recently announced the availability of Azure virtual machines running on SGX hardware that allows the users to write their own code to run in a secure enclave to which the service provider does not have access.

[558] For example, on SGX systems there is a cost every time data is moved from the main memory into the enclave memory so it is necessary to consider the amount of data and number of times that it goes back and forth in and out of the enclave.

Also, there are compatibility issues to address in the design of the solution (i.e. the processor in the client side needs to be able to communicate with that in the enclave, and the enclaves need to be able to communicate among themselves).

- Privacy:
  - Medium-low: As the secure enclave would have access to the full content of communications, privacy would depend strongly on the ability to trust that the enclave, as implemented by the ESP, is secure and effective. User data (hashes or the message) are not visible to the ESP nor are the operations to detect child sexual abuse. The possible security issues (e.g. compromise of third-party server by state actors) could affect the privacy of the communication.
- Security:
  - Medium-low: the solution fully relies on trusting that the secure enclave works as intended and it has not been compromised (some vulnerabilities in this type of systems have already been found). The company making the enclave would be the only one having the key to the inner workings of the enclave and could become a target of bad actors, and if successful, a compromise would have a broad impact on the security of the system and give access to the encryption keys for the communications between the sender and recipient. By accessing the enclave, bad actors would also have access to the decryption keys for the communications between the sender and the recipient. That said, it could be possible to attest that the code running in the enclave has not been modified from the time it was deployed and that the user has connected to the right enclave, carrying out the right processes, although this feature has been compromised in the past.[559] In addition, the check could remotely check the code but not the hashes used.
- Transparency:
  - Medium-low: it is unclear how the use of the secure enclave could be documented and be publicly reported to facilitate accountability through ongoing evaluation and oversight by policymakers and the public. The wider user community will have to rely on a trustworthy and technically competent entity to confirm the workings of the secure enclave.

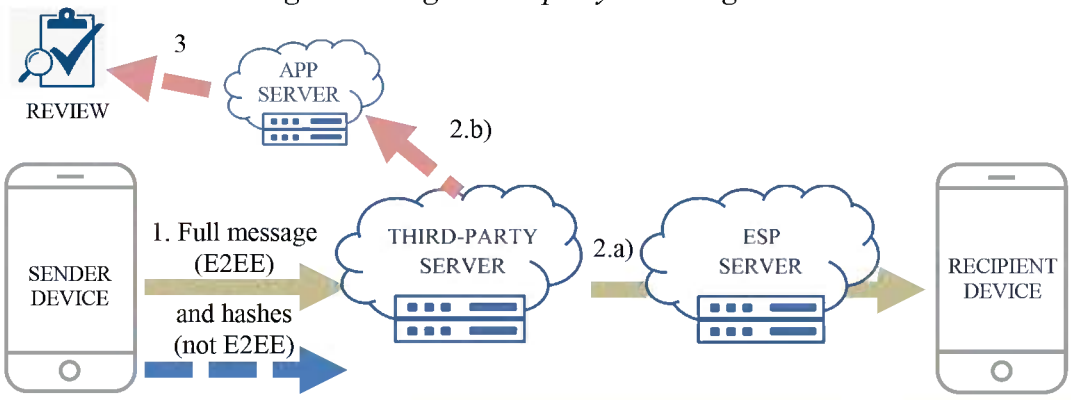
One possible way to mitigate some of the above concerns (in particular on security and transparency) could be to send to the secure enclave the hashes not E2EE for matching. This would e.g. eliminate the risk of leaking the private E2EE keys if the enclave is compromised. In this case the trust in the secure enclave would be limited to protecting the hashing algorithm and its parameters.

b. Single third-party matching

This solution is the same as 1.b. (on device full hashing with matching done at server), but with the matching done at a trusted third-party server instead of at the ESP server:

[559] See here.

Figure 9: single third-party matching



1. **Device:** converts the images and videos into hashes before the message is encrypted, encrypts the full message and sends the hashes (client to server encrypted) and the E2EE full message to the third-party server.

3. **App server:** sends full image/video for review if there is a match in the third-party server.

Third-party server:
2. Compares hashes received from the device with those in the database of hashes of confirmed child sexual abuse (matching)
a) No match ⇨ forwards E2EE message to recipient
b) Match ⇨ asks app server to send image/video to review and/or reporting

Device: receives and decrypts E2EE message

Assessment:

- Effectiveness:
  - Medium-high: it could allow the detection of known CSA[560]. No need to limit the hash list, as it will be located at the third-party servers.
- Feasibility:
  - Low: scalability could be an issue, although this could be a service for a smaller companies offered on top of the cloud infrastructure of larger ESPs. It requires a combination of code running on the sender's device and (third party) server and therefore certain interdependence, which would influence e.g. the latency of message transmission.
- Privacy:
  - Medium-low: user data (hashes) are not visible to the ESP and no operations to detect CSA would occur at the ESP server. The possible security issues (e.g. compromise of third-party server by state actors) could decrease the privacy of the communication. That said, it is likely that the third party would have to work very closely with or be effectively part of the ESP that provides the communication service, which may raise privacy concerns. If the third party does not work in real time (i.e. analysing the message at the time it is sent) and instead analyses the

[560] The use of classifiers is in principle possible with single third parties but it would be part of a different solution.

message after it has been sent, the dependence on the ESP could be lower[561]. Also, the third party could be part of the client provisioning, which could reduce the privacy concerns.

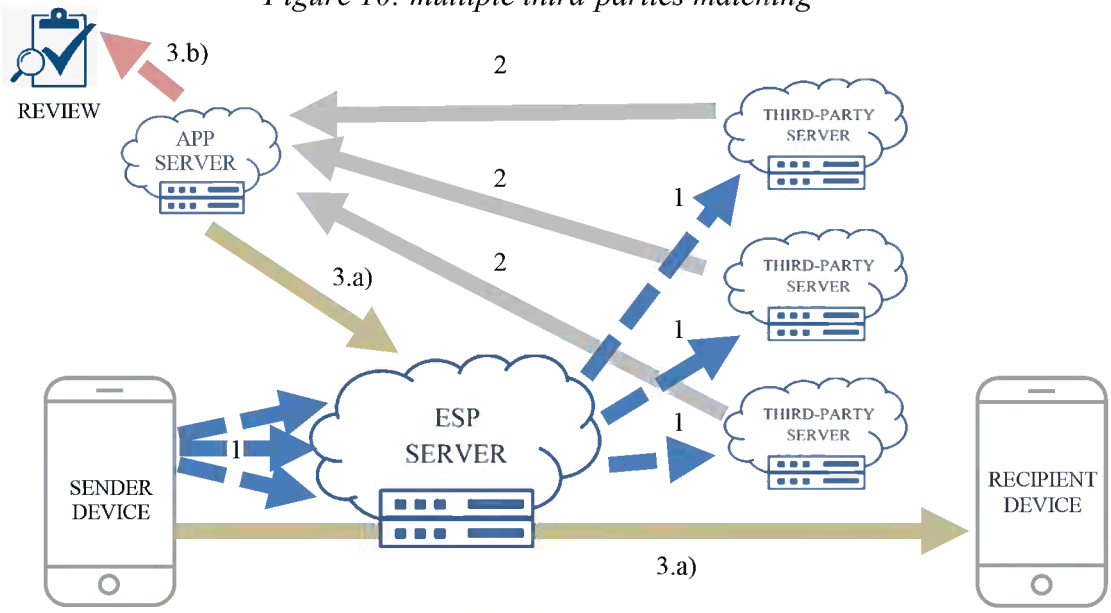
- Security:
  - Medium-low: in addition to the security concerns of 1.b) (on-device full hashing with matching at the server), e.g. risk of manipulation of the hashing algorithm, the third-party server could be compromised by state or individual actors.
- Transparency:
  - Medium-low: the possible security issues could limit the reliability of public reporting on the use of the solution and therefore the accountability.

c. Multiple third-parties matching

In this solution, based on **multi-party computation** (MPC), the device converts the image (or video) into a hash, breaks it into parts, encrypts them with the third party keys and sends these parts to multiple third-parties for partial matching through the ESP server (which does not have access to the encrypted partial hashes). The app server compiles the responses from the third-parties and determines whether a match has occurred. If there is a match, the app server sends the full image (or video) for review/reporting. If there is no match, the ESP server forwards the E2EE message to the recipient:

[561] The processing of messages after they have been sent to the recipient (i.e. batch processing with some timescale) could be applied to other solutions as well (see footnote 1 on the scope of the solutions).

Figure 10: multiple third-parties matching



1. **Device:** converts the images and videos into hashes before the message is encrypted, breaks them into parts, encrypts them with the third-party keys and sends them through the ESP server to multiple third-parties for partial matching and sends the E2EE full message to the third-party server.

3. **App server:** compiles the responses from the third-parties and determines whether a match has occurred:
a) No match ⇨ asks server to forward E2EE message to recipient
b) Match ⇨ sends message for review and/or reporting.

Third party servers:
2. Do partial matching of the multiple hash parts and sends info back to device.

ESP server:
No action beyond routing the hashes to the third parties.

Device: receives and decrypts E2EE message

Assessment:

- Effectiveness:
  - Medium-high: it could allow the detection of known CSA[562]. No need to limit the hash list, as it will be located at the third-party servers.
- Feasibility:
  - Low/medium-low: the multiple round-trip requests between the device and the servers before the message can be sent could slow performance, in particular with slow internet connections. It requires a combination of code running on the

[562] The use of classifiers is in principle possible with single third parties but it would be part of a different solution.

sender's device and (third party) server. A similar technology is already in use by Google and online merchants[563] but further research would be required to see how it could be applied in this situation (in particular on scalability) and what would be the costs, including computational overhead.

- Privacy:
  - Medium: user data (content and hashes) are not visible to the ESP and no operations to detect child sexual abuse would occur at the ESP server. The possible security issues (e.g. compromise of third-party server by state actors) could decrease the privacy of the communication. That said, the solution could offer better privacy than solution 2.b) (single third party matching): if at least one of the parties is trustworthy the hash will remain private. On the other hand, it is possible that the larger companies, which also offer electronic communication services, turn themselves into the third parties of this solution for the smaller companies, which may generate some privacy issues.
- Security:
  - Medium: in addition to the security concerns of 1.b) (on-device full hashing with matching at the server), e.g. risk of manipulation of the hashing algorithm, the third-party servers could be compromised by state or individual actors. That said, compared to solution 2.b) (single third-party matching), the risk will be lower as bad actors would need to compromise multiple servers instead of one.
- Transparency:
  - Medium: the possible security issues could limit the reliability of public reporting on the use of the solution and therefore the accountability.

****

Another possible server related solution would be to use **classifiers running on the server**, feeding on **metadata**. This seems to be the approach taken by **Facebook**[564] as it plans to switch to E2EE by default in its Messenger service[565] but the technical details remain unclear.

3) Encryption related solutions

This type of solutions consists in using **encryption protocols** that allow the detection of CSA in encrypted electronic communications.

a. On-device homomorphic encryption with server-side hashing and matching

In this solution, images are encrypted using a carefully chosen partially homomorphic encryption scheme (this enables an encrypted version of the hash to be computed from the encrypted image). The encrypted images are sent to the ESP server for hashing and matching

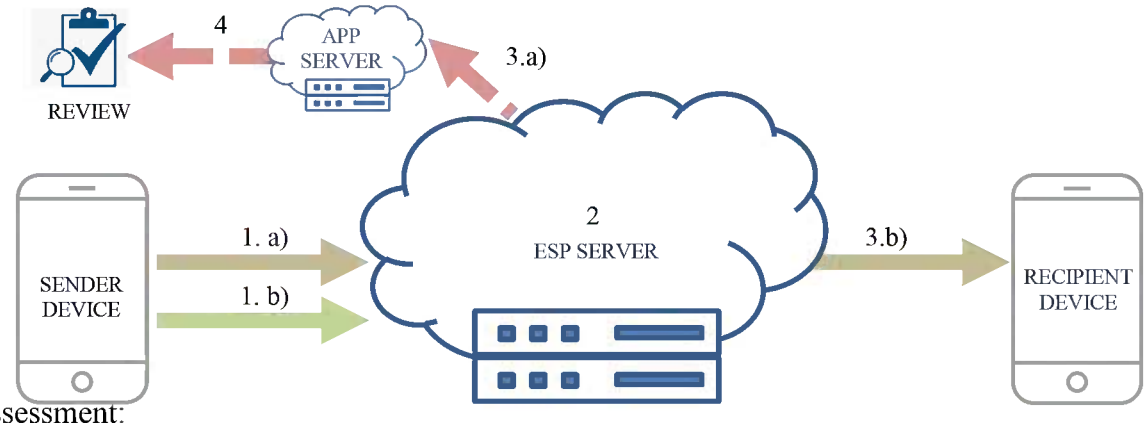
[563] See here and here. The technology allows Google and online merchants to compute certain profile information on internet users (.g. the average age of buyers of a certain watch) without sharing all the data they have about those users.

[564] As indicated here.

[565] As announced in March 2019.

against an encrypted version of the hash list[566] (the server does not have the homomorphic decryption keys):

Figure 11: on-device homomorphic encryption with server-side hashing and matching



Assessment:

1. **Device:** sends to the ESP server
   a) full message, E2EE, and
   b) images/video homomorphically encrypted

4. **App server**: sends full image/video for review if there is a match in the ESP server.

ESP server:

2. Operates on the homomorphically encrypted images/videos to compute an encrypted hash.
3. Compares the encrypted hash with the database of encrypted hashes of known CSAM. If:
   a) detected ⇨ instructs the app server to send the message for review
   b) not detected ⇨ forwards to recipient E2EE message

Device: receives and decrypts E2EE message

- Effectiveness:
  - Medium: it could allow the detection of known child sexual images[567]. It would not be applicable to videos (too slow) or text-based threats. No need to limit the hash list, as it would be located at the server.
- Feasibility:
  - Low: proof of concept for images exists but additional research and development is needed to reduce processing times (currently at around 15 seconds per image on mobile).[568] No comparable commercial applications on electronic communications

[566] See paper by H. Farid (reference 1 of encryption related solutions in annex 2), which shows that it is possible to build perceptual hashes on encrypted images that have about the same efficacy in terms of false positives and detection rate as PhotoDNA, but taking longer time (about 10-15 seconds per image, without doing any optimization to reduce the time, versus the one thousandth of a second that PhotoDNA currently takes). This could also be a type of privacy homomorphism.

[567] The use of classifiers is in principle possible with partial homomorphic encryption but it would be part of a different solution.

[568] See table II on execution times in Tarek Ibn Ziad, M., et al., *CryptoImg: Privacy Preserving Processing Over Encrypted Images*, University of California, Los Angeles, 2019.

exist. At the moment, the computational power required on the server would render this solution expensive.

- Privacy:
  - Medium-low: Hashes of user data are visible to the ESP. Similar privacy as solution 1.b.
- Security:
  - Medium: no risk of leaking of hash database, or hashing and matching algorithm on the client side, as all these calculations would take place at the server. The solution does not prevent the possibility that the database of hashes could be tampered with at the server, as the other solutions with hash lists on the server.
- Transparency:
  - Medium-high: the use of the solution could be documented and be publicly reported to facilitate accountability.

****

Another possible encryption related solution would be to use machine learning and build **classifiers** to apply on **homomorphically encrypted** data for instant classification. Microsoft has been doing research on this but the solution is still far from being functional[569].

[569] More information on Microsoft's work on homomorphic encryption is available here.

4. OVERVIEW

The table below summarises the above assessments and classifies the possible solutions into 3 groups: top 3 (i.e. most promising, although some research may be needed), needs research (i.e. it could be considered but substantial research is still needed), and to be discarded (i.e. currently not worth pursuing at this point if there is a need to prioritise, but could still be of interest in the future):

Type	Solution	Effectiveness	Feasibility	Privacy	Security	Transparency	Overall
3. Baseline	a. Non-E2EE communications	★★★★★	★★★★★	★	★★	★★★	N/A
	b. E2EE communications	N/A	N/A	★★★★★	N/A	N/A	N/A
	c. Encrypted communications with exceptional access	★	★	★	★★	★★★	N/A
4. Device related	a. All detection done on-device	★★★	★★	★★★	★	★★	Needs research
	b. On-device full hashing with matching at server	★★★★	★★★★★	★★	★★	★★★	Top 3
	c. On-device partial hashing with remaining hashing and matching at server	★★★★	★★★	★★	★★★	★★	Top 3
	d. On-device use of classifiers	★★	★★	★★	★★	★★★	Needs research
5. Server related	a. Secure enclaves in ESP server	★★★★	★★	★★	★★	★★	Top 3
	b. Single third-party matching	★★★★	★	★★	★★	★★	Discard
	c. Multiple third-parties matching	★★★★	★	★★★	★★★	★★★	Needs research
6. Encryption related	a. On-device homomorphic encryption with server-side hashing and matching	★★★	★	★★	★★★	★★★★	Needs research

5. RECOMMENDATIONS

On possible solutions:

- Immediate: on-device hashing with server side matching (1b). Use a hashing algorithm other than PhotoDNA to not compromise it. If partial hashing is confirmed as not reversible, add that for improved security (1c).
- Long term:
  - Invest in research on secure enclaves in ESP server to make the technology more accessible (2a).
  - Invest in research on multiple third-parties matching, leveraging existing applications (2c) and identifying possible third parties.
  - Invest in research on classifiers to supplement hashing and matching, but not replace it (1d).
  - Invest in homomorphic encryption research with regard to image matching (3a).

Other considerations:

- PhotoDNA update: PhotoDNA, the hashing technology most widely used, is more than 10 years old and it may require an update now and then periodically every few years to keep up with the latest developments (and make it less vulnerable to manipulation, including by modifying the images to avoid detection).
- Quality and integrity of hash databases: a number of solutions rely on the detection of child sexual abuse through hashing technology. The quality of this detection (and therefore the effectiveness of those solutions) depends on the quality and integrity of those databases.
- Industry standards for detection: the creation of industry standards for the detection tools (e.g. image and video hashing) could facilitate the development and deployment of coherent and interoperable solutions across industry.
- Open source tools: open source tools could also facilitate the development and deployment of solutions across industry. However, substantial research may be required to produce open source tools that cannot be manipulated to reduce their effectiveness or be misused. At this moment, all solutions considered are based in part on "security by obscurity", that is, it is required for the security and effectiveness of the solution that the opponent does not know the full details of the scheme. The scientific state of the art is not yet sufficiently mature for open tools.
- Open competition: an open competition with a substantial prize[570], could encourage not only the development of open source tools and industry standards, but also the development of new possible solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications.
- Reporting mechanisms: when describing the solutions, the paper does not analyse in detail what happens after child sexual abuse is detected, i.e. review and reporting

[570] For example, similar to the open competitions organized by NIST on cryptography or by the EU-funded projects NESSIE and ECRYPT (eSTREAM).

mechanisms. These mechanisms depend on national legal obligations. These can have an influence on the effectiveness of some solutions (e.g. training of machine learning classifiers, which rely on a stream of well-labelled material to remain effective).

- Industry standards for reporting and transparency: when using hash databases, it would be useful to know not only the total number of reports sent to relevant statutory bodies from matches, but also the matches not sent to statutory bodies but removed based on the terms of service, and matches not sent to statutory bodies nor removed.
  The effectiveness of a hash database is currently only known to the company using it. It could be useful to have a third party perform regular testing/auditing using a sample non-CSAM match similar to the EICAR test file in the anti-virus industry.
- Safety by design: the development of technical solutions that could strike a balance between ensuring the privacy of electronic communications (including the privacy of children) and the protection of children against sexual abuse and sexual exploitation is facilitated when that balance is aimed at from the start, from the design stage.

REFERENCES

General

1. Preneel, B., *The Never-Ending Crypto Wars*, presentation, imec-COSIC KU Leuven, 16/09/2019.
2. Snap Inc., Snap Inc. Response to Sen. Blackburn, 17/07/2019.
3. Weaver, N., *Encryption and Combating Child Exploitation Imagery*, Lawfare, 23/10/2019.
4. WhatsApp , *WhatsApp Encryption Overview, Technical white paper*, 4/4/2016.
5. Pfefferkorn, R., *William Barr and Winnie The Pooh*, Center for Internet and Society, 7/10/2019.
6. Stanford Internet Observatory, *Balancing Trust and Safety on End-to-End Encrypted Platforms,* 12/09/2019 (Stanford workshop).
7. Stanford Internet Observatory, *Mitigating Abuse in an End-to-End World*, 11/01/2020 (New York workshop).
8. Stanford Internet Observatory, *Mitigating Abuse in an End-to-End World*, 17/02/2020 (Brussels workshop).
9. Bursztein, E; Bright, T.; DeLaune, M.; Elifff, D.; Hsu, N.; Olson, L.; Shehan, J.; Thakur, M.; Thomas, K.; *Rethinking the Detection of Child Sexual Abuse Imagery on the Internet*, Proceedings of the 2019 World Wide Web Conference (WWW '19), 13-17 May, 2019, San Francisco, CA, USA.
10. Levy, I.; Robinson, C.; *Principles for a More Informed Exceptional Access Debate*; Lawfare, 29/11/2018.
11. Farid, H.; *Facebook's plan for end-to-end encryption sacrifices a lot of security for just a little bit of privacy;* Fox News, 16 June 2019.
12. Carnegie Endowment for International Peace; *Moving the Encryption Policy Conversation Forward*; Encryption Working Group, September 2019.
13. Millican, J.; *E2EE for Messenger: goals, plans and thinking*; Facebook; Real World Crypto 2020, January 8-10, 2020.
14. Dalins, J.; Wilson, C.; Boudry, D.; *PDQ & TMK + PDQF - A Test Drive of Facebook's Perceptual Hashing Algorithms*; Australian Federal Police and Monash University; December 2019.
15. Harold Abelson, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner, *Keys under doormats*. Commun. ACM 58(10): 24-26 (2015).

Device related solutions

1. Mayer, J., *Content Moderation for End-to-End Encrypted Messaging;* Princeton University; 6 October 2019,
2. Callas, J., *Thoughts on Mitigating Abuse in an End-to-End World;* 14 January 2020,

3. Portnoy, E., *Why Adding Client-Side Scanning Breaks End-to-End Encryption*, Electronic Frontier Foundation, 1 November 2019,
4. Green, M., *Can end-to-end encrypted systems detect child sexual abuse imagery? – A Few Thoughts on Cryptographic Engineering*, 8 December, 2019.
5. Green, M., *Client-side CSAM detection: technical issues and research directions,* presentation at Stanford Internet Observatory event in New York, 11/01/2020.
6. Weaver, N., *Some Thoughts on Client Side Scanning for CSAM*, presentation at Stanford Internet Observatory event in New York, 11/01/2020.
7. Stamos, A., *Written testimony before U.S. House of Representatives Committee on Homeland Security on "Artificial Intelligence and Counterterrorism: Possibilities and Limitations"*, June 25, 2019.

Server related solutions

- Makri, E., Rotaru, D., Nigel P. Smart, N.P., Vercauteren, F., *EPIC: Efficient Private Image Classification (or: Learning from the Masters)*; KU Leuven, Belgium; Saxion University of Applied Sciences, The Netherlands; University of Bristol, UK; 2017,
- Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M., Wernsing, J.; *CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy;* Princeton University, Microsoft Research; 2016.
- Liu, J., Lu, Y., Juuti, M., Asokan, N., *Oblivious Neural Network Predictions via MiniONN transformations;* Aalto University; 2017.
- Juvekar, C., Vaikuntanathan, V., Chandrakasan, A., *GAZELLE: A Low Latency Framework for Secure Neural Network Inference;* MIT; 2018.
- Riazi, M. S., Songhori, E. M., Weinert, C., Schneider, T., Tkachenko, O., Koushanfar, F., *Chameleon: A Hybrid Secure Computation Framework for Machine Learning Applications;* UC San Diego and TU Darmstadt, Germany; 2017.
- Riazi, M. S., Samragh, M., Lauter, K., Chen, Hao., Koushanfar, F., Laine, K., *XONN: XNOR-based Oblivious Deep Neural Network Inference*; UC San Diego and Microsoft Research; 2019.
- Portnoy, E., *Azure Confidential Computing Heralds the Next Generation of Encryption in the Cloud;* Electronic Frontier Foundation; 18 September 2017.
- Frankle, J. et al.; *Practical Accountability of Secret Processes*; Massachusetts Institute of Technology; Proceedings of the 27th USENIX Security Symposium; August 2018.
- Hastings, M.; *General purpose frameworks for Secure Multi-Party Computation;* University of Pennsylvania; Real World Crypto 2020, January 8-10, 2020.
- Damgård, I, Nielsen J.B., Cramer, R., *Secure Multiparty Computation and Secret Sharing*, Cambridge University Press, 2015.

Encryption related solutions

1. Farid, H., Singh, P., *Robust Homomorphic Image Hashing*, Dhirubhai Ambani Institute of Information and Communication Technology, University of California, Berkeley and Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, Gujarat, India, 2019,
2. Iliashenko, I., *Optimisations of fully homomorphic encryption*, KU Leuven, 2019,
3. Minelli, M., *Fully homomorphic encryption for machine learning*, PSL Research University, 2018.
4. European Commission, *Putting privacy at the heart of biometric systems*, 2011.
5. Yakoubov, S., *A Gentle Introduction to Yao's Garbled Circuits*, Boston University, 2017.
6. Tarek Ibn Ziad, M., et al., *CryptoImg: Privacy Preserving Processing Over Encrypted Images*, University of California, Los Angeles, 2019.
7. Gentry, C. *Fully Homomorphic Encryption Using Ideal Lattices*. In the 41st ACM Symposium on Theory of Computing (STOC), 2009.

ANNEX 10: EU CENTRE TO PREVENT AND COUNTER CHILD SEXUAL ABUSE

In the **EU strategy for a more effective fight against child sexual abuse**, the Commission committed to work towards the creation of a European centre to prevent and counter child sexual abuse to enable a comprehensive and effective EU response against child sexual abuse **online and offline**[571]. The purpose of this annex is to comprehensibly screen and assess in detail all possible options for the Centre, and determine the preferred one to be incorporated in the options of the report. It also provides additional information on the Centre as a measure.

First, it explains the part of the problem and the relevant problem drivers in the impact assessment that a centre would address, followed by its added-value and specific objectives. Then, the annex analyses the various possibilities to set up the centre: what are the **implementation choices**? (section 3); what are the **impacts** of each choice? (section 4); how do the choices **compare**? (section 5).

Finally, the annex discusses the **preferred implementation choice** resulting from the previous analysis: what are the advantages, disadvantages and trade-offs of this choice? (section 6). The preferred choice is then integrated into the policy options considered in the report.

1. RELEVANT PROBLEM DRIVERS

The Centre is relevant to all the problem drivers identified in the impact assessment:

*1. **Voluntary action** by online service providers to detect online child sexual abuse has proven **insufficient***

Box X in section 2.1.1. of the report lays out the current system to detect and report CSA online in the EU, which relies on the action of a private entity in a third country (NCMEC in the US), and on US legislation requiring service providers to report to NCMEC CSA online that they may become aware of in their systems, rather than to law enforcement directly.

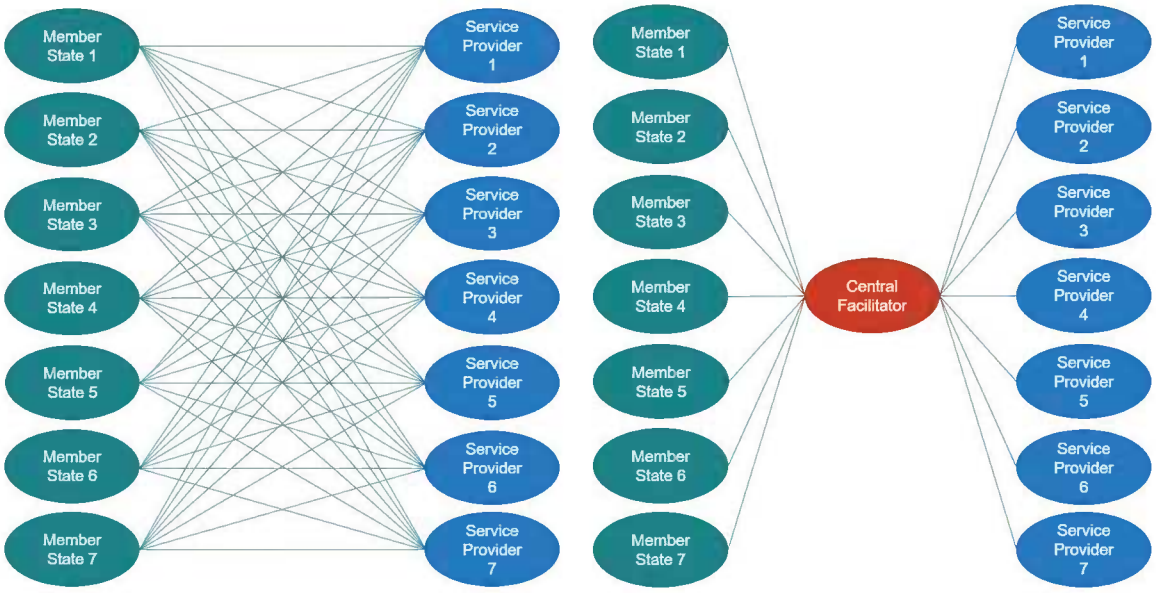
Section 2.2.1. describes how (lack of) voluntary action by service providers in the EU drives part of the problem. At the moment, there are no obligations in EU law for service providers to detect, report or remove CSA online. Neither there is an EU Centre that would be recipient of the reports from service providers or that could serve as a **facilitator** of the detection and removal processes.

***2. Inefficiencies** in **public-private cooperation** between online service providers, civil society organisations and public authorities **hamper** an effective fight against CSA*

First, when setting up channels for the reporting of suspected child sexual abuse from service providers to Member States' authorities, and for the information about what is illegal from Member States' authorities to service providers**, direct connections between**

[571] EU strategy for a more effective fight against child sexual abuse, COM(2020) 607, 24 July 2020, p14.

each Member State and each provider are not efficient. It is more efficient to pass through a central point, as is evident from the following diagram:



Rather than requiring a number of connections that is equal to (Member States*Service Providers), as shown on the left, the creation of a central facilitator reduces the number of connections to (Member States + Service Providers), a significant efficiency gain. In addition, there are also security considerations to take into account here, given that the information to be transmitted is of highly sensitive data. A reduction in the number of connections and in complexity reduces the possibilities for data leaks and the attack surface.

Secondly, it would not be efficient for each Member State to provide **its own information to each service provider about what is illegal** on their territory. There are large overlaps across all Member States because of the harmonised definitions on child pornography created by Directive 93/2011/EU. There may be some additional aspects, such as the provocative posing of children or the criminalisation of drawings or cartoons depicting child sexual abuse, where Member States may differ, but these are very limited in number.

Third, while each provider and each Member State could be required to provide transparency reporting and make available its processes and data for auditing, it is much more difficult to create a robust overview of the entire system in this way. For example, "known" CSAM is often detected on several platforms, yet it would not be possible to trace the spread of one image across service providers without a central overview of which image is reported. Such information would be helpful both in devising effective responses, and in learning about the functioning of the criminal networks behind.

These three issues are relevant here because they are **difficult to address through measures solely targeting service providers or Member States** and their authorities. There are limits to a pure "network approach", in particular when it comes to ensuring **coordination and transparency**.

While a US Centre already exists which provides some of these services for US authorities (NCMEC), the EU cannot rely on this for support to its own authorities, especially when expanding detection and reporting within the EU where it would not be appropriate to require reporting to a third-country entity.

*3. Member States' efforts to **prevent** child sexual abuse and to **assist victims** are **limited, lack coordination** and are of **unclear effectiveness***

When it comes to prevention and assistance to victims, the Commission has taken measures to facilitate the exchange of information between Member States and to foster an evidence-based approach. However, experience has shown that such **networks do not grow into effective exchanges on their own**; rather, to be truly successful, they require a central facilitator to support and structure the exchange, make available a repository of best practices, organise meetings, and provide translations.

Member States face challenges in providing an effective system, a number of which are linked to a **lack of resources and insufficient evidence** as to the effect of a given measure. An EU centre proposed by the initiative would provide an expertise hub to support efficient spending of limited resources and to foster an evidence-based approach in Member States' policies on prevention and victim support measures and programmes.

An EU centre facilitating the exchange of best practices can help Member States make better use of resources: they could apply solutions already existing in other Member States, and take advantage of existing research, instead of developing their own research and solutions from scratch. The aim of the centre would be to become a platform where Member States can exchange experiences. Its role would be **facilitation** of Member States' action, and it would allow Member States to tackle operational issues together.

The centre as a hub for disseminating knowledge would also provide scientific evidence, informing policy makers. Such evidence would allow obtaining high-level commitment, which could help assigning greater resources to this type of activities, including awareness raising, education and work with offenders. It would serve to overcome the tendency to approach the issue of child sexual abuse only from law enforcement angle.

2. SPECIFIC OBJECTIVES

In light of the problem drivers set out above and the general objective of the initiative (improve identification, protection and support of victims of child sexual abuse, ensure effective prevention, and facilitate investigations), the Centre would have three specific objectives:

1. **Help** ensure that victims are rescued and assisted as soon as possible and offenders are brought to justice by **facilitating detection, reporting and removal** of CSA online.
    - The centre would work with service providers and law enforcement agencies in the EU to ensure that victims are identified and assisted as soon as possible and that offenders are brought to justice, by facilitating detection, reporting and removal of CSA online:
        - **Detection**: the centre would support companies by maintaining a **single database** in the EU of indicators of **known CSAM, new CSAM and grooming,** to facilitate its detection in companies' systems, in compliance with EU data protection rules.
        - **Reporting**: it would support Member States by receiving reports in relation to child sexual abuse in the EU from companies **offering their**

services in the EU, ensure the accuracy and relevance of such reports, and forward these to law enforcement for action.

- **Removal**: the centre would also support law enforcement by facilitating the work of **hotlines** on the **notice and takedown** of child sexual abuse material. In particular, it would notify service providers of the existence of child sexual abuse material in their services, and these would be required to remove it within a short time.

To be able to carry out these functions, the centre would need the appropriate **legal basis** to allow it to process **personal data and child sexual abuse material**, as well as the necessary **human and technical resources**. In particular, the centre must be able to implement **strong security measures** to avoid any data breaches. The legal basis should also allow it to cooperate closely with entities **in the EU and beyond**, in particular with regard to **data exchanges**.

- The centre would ensure **accountability and transparency** in the process of detection, reporting and removal of child sexual abuse online. This would include the collection of data for transparency reports; providing clear information about the use of tools and its effects; supporting audits of data and processes; the centre would help to ensure that there is no erroneous takedown of legitimate content, or abuse of the search tools to report legitimate content (including misuse of the tools for purposes other than the fight against child sexual abuse); and possibly support users who feel that their content was mistakenly removed. The roles of the centre ensuring accountability and transparency of the detection and reporting process make it a **fundamental component** of the new legislation.

Box 1: independence of the centre

The centre would serve as a key **facilitator** of the work of service providers in detecting, reporting and removing the abuse (including by ensuring transparency and accountability), and of the work of law enforcement in receiving and investigating the reports from service providers.

To be able to play facilitator role, it is essential that the centre be independent from potentially overriding private and political interests. Even a perception of partiality could undermine the goals the centre would set out to achieve. Therefore is crucial that the centre is **not directly linked** to:

- **service providers**, as the centre would serve both as the source of reliable information about what constitutes CSA online, providing companies with the sets of indicators on the basis of which they should conduct the mandatory detection, and as a control mechanism to help ensure transparency and accountability of service providers, including possibly helping to resolve complaints from users; and
- **law enforcement**, as the centre must be neutral to be able to play the role of facilitator and ensure that it maintains a fair and balanced view of all the rights at stake, in particular between the fundamental rights of children and those of the rest of internet users.

2. **Support Member States** in putting in place usable, rigorously evaluated and effective **prevention** measures to decrease the prevalence of child sexual abuse in the EU.
   - The results of the monitoring of the implementation of the Child Sexual Abuse Directive indicate that Member States face challenges to put in place prevention measures. These challenges occur at all stages: before a person offends for the first time, in the course of or after criminal proceedings, and inside and outside prison. Building on the work of the prevention network of researchers and practitioners[572], the centre would 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, taking into account differing vulnerabilities of children according to their age, gender, development and specific circumstances.
   - The centre would provide support and faciliate Member States action on the various types of prevention efforts, both those focused on the **child** and his or her environment and on decreasing the likelihood that a child becomes a **victim,** as well as those focused on potential **offenders** and on decreasing the likelihood that a person **offends.**
   - It would facilitate **coordination** to support the most efficient use of resources invested and expertise available on prevention across the EU, **avoiding duplication** of efforts. A **hub for connecting, developing and disseminating research and expertise**, it would facilitate the exchange of best practices **from the EU and globally**, and encourage dialogue among all relevant stakeholders and help develop **state-of-the-art research and knowledge, including better data**. To perform that hub function effectively, the centre would be able to cooperate closely in this areas with entities in the EU and beyond, including through **partnership agreements and joint initiatives**. It would also **provide input to policy makers** at national and EU level on prevention gaps and possible solutions to address them.

3. **Support Member States** to ensure that **victims** have access to **appropriate and holistic support**, by **facilitating** efforts at EU level.
   - The centre would work closely with national authorities and global experts to help ensure that **victims** receive **appropriate and holistic support**, as the Child Sexual Abuse Directive and the Victims' Rights Directive[573] require[574]. In particular, the centre would facilitate the **exchange of best practices** from the EU and globally on protection measures for child victims and serve as a **hub of**

---

572 This prevention network is another initiative of the EU strategy for a more effective fight against child sexual abuse, COM(2020) 607, 24 July 2020, p9.

573 Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, OJ L 315, 14.11.2012. This Directive complements with general victims' rights the specific provisions for victims of child sexual abuse contained in the Child Sexual Abuse Directive.

574 To ensure a coherent approach to EU victims' rights policy, the centre could also cooperate with the Victims' Rights Platform set up under the EU Strategy on victims' rights (2020-2025), COM/2020/258 final.

expertise to **help coordinate** better and avoid duplication of efforts. To perform that hub function effectively, the centre would be able to cooperate closely in this area with entities in the EU and beyond, including through **partnership agreements and joint initiatives**.

- It would also **carry out research** (e.g. on short and long-term effects of child sexual abuse on victims) to **support evidence-based policy** on assistance and support to victims.
- The centre would also **support victims in removing their images and videos** to safeguard their privacy, including through **proactively searching** materials online and notifying companies, in cooperation with civil society organisations such as the INHOPE hotlines.
- The centre would also serve to ensure that the voices of child victims are heard and taken into account in policymaking at EU and national level, **raising awareness** of children's rights and of child victims' needs.

***

The specific objectives for the Centre are coherent with the intervention logic of the larger initiative that the impact assessment focuses on, including the problem, problem drivers, and the general and specific objectives. As set out above for the problem drivers, the related objectives are difficult to attain through measures targeting Member States and service providers alone, given the limits in efficiency, security, and accountability.

The problem drivers in the impact assessment basically indicate that service providers are not doing enough (problem driver 1), Member States are not doing enough (problem driver 3), and that Member States and service providers (and NGOs) are not cooperating well in what they are doing (problem driver 2). There is therefore a clear need to 1) do more (i.e. help make and make new efforts), and 2) do it more efficiently (i.e. cooperate/coordinate better on existing efforts). And the specific objectives for the centre are to help do more and help do it more efficiently on detection, reporting and removal of child sexual abuse online and on prevention and assistance to victims.

Considering the above, Table 1 below shows the intervention logic for the centre as a retained measure within the intervention logic for the larger initiative. In particular, it shows the specific objectives for the centre and the implementation choices to achieve those objectives.

Table 1: intervention logic for the Centre as a measure within the larger initiative

Problem	Problem drivers	General objective	Specific objectives	Specific objectives (Centre)	Implementation choices (Centre)			
					Non-legislative	Legislative		
					A	B	C	D
Some child sexual abuse crimes are **not adequately addressed** in the EU due to challenges in their **detection, reporting and action**, as well as **insufficient prevention** and **assistance to victims**	1. **Voluntary action** by online service providers to detect online child sexual abuse **has proven insufficient** 2. **Inefficiencies** in **public-private cooperation** between online service providers, civil society organisations and public authorities hamper an effective fight against child sexual abuse 3. Member States' efforts to **prevent** child sexual abuse and to **assist victims** are **limited**, **lack coordination** and are of **unclear effectiveness**	Improve **identification, protection and support of victims** of child sexual abuse, ensure **effective prevention**, and **facilitate investigations**	4. Ensure the effective **detection, removal and reporting** of online child sexual abuse where they are **currently missing** 5. Improve **legal certainty, protection of fundamental rights, transparency and accountability** 6. Reduce the **proliferation and effects** of child sexual abuse through **increased coordination** of efforts	1. **Help** ensure that victims are rescued and assisted as soon as possible and offenders are brought to justice by facilitating **detection, reporting and removal** of CSA online 2. **Support Member States** in putting in place **usable, rigorously evaluated** and effective **prevention** measures to decrease the prevalence of child sexual abuse in the EU 3. **Support Member States** to ensure that **victims** have access to **appropriate and holistic support**, by **facilitating** efforts at EU level	Set up an EU Centre focused on **prevention and assistance to victims** through **practical measures**	Set up an EU Centre to prevent and counter child sexual abuse as an **independent EU body (decentralised agency)**	Set up an EU Centre to prevent and counter child sexual abuse **with some functions in Europol and others in an independent organisation under Member State law**	Set up an EU **Centre** to prevent and counter child sexual abuse **within FRA**

3. IMPLEMENTATION CHOICES

3.1. What is the baseline from which implementation choices are assessed?

The baseline from which implementation choices are assessed is the **baseline that corresponds to the subset of issues** outlined above, i.e. those problem drivers and objectives where measures targeting Member States or service providers alone would not prove efficient.

In this baseline scenario:

- with regard to **detection, reporting and removal of CSA online**, the inefficiencies in the cooperation between public authorities, service providers, and civil society organisations would likely continue, or increase, given the expected continued growth of online interactions. Even if legal obligations to detect, report and remove are imposed on service providers, it is unclear to where they would need to report, what would be the conditions under which the detection would take place, and whether there would be any entity helping ensure transparency and accountability of the process. The ability of law enforcement authorities to investigate crimes and rescue victims will not significantly improve in the baseline scenario. In addition, the legal fragmentation in the internal market would likely continue to increase as Member States take their own measures to deal with the increasing challenge;
- with regard to **prevention**, the network announced in the EU Strategy for a more effective fight against child sexual abuse would continue to develop and expand. Its activities could contribute to foster exchange of good practices and lessons learned and enable coordination between initiatives in Member States and third countries. As the prevention network grows, it would become more and more difficult to manage without dedicated resources. At the moment the network is at an incipient stage and is managed as part of the activities of a policy unit in the European Commission (DG HOME, D4). This is not sustainable in the long run given the resources required to motivate, encourage, structure and support meaningful network exchanges. As the network grows, its management could be outsourced to a contractor, e.g. as in the Radicalisation Awareness Network, with periodic calls for proposals to renew the outsourcing contract. However, this would not ensure long-term sustainability of the activities of the network. Furthermore, the scope of the activities that the network could carry out would be limited (included limited coordination of efforts, leading to potential gaps and duplication of efforts), given the limited dedicated resources that such a set up would allow;
- with regard to **victims' assistance**, Member States would continue to enforce or implement the corresponding provisions of the Child Sexual Abuse Directive and the Victims' Rights Directive[575]. In addition, the EU Strategy on victims' rights[576] (2020-

[575] Directive 2012/29/EU of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, *OJ L* 315, 14.11.2012. This Directive complements with general

2025) will set up a Victims' Rights Platform bringing together all EU level actors relevant for victims' rights. However, it is unlikely that these measures would avoid the **duplication of efforts** and the **existence of gaps** across Member States in the support of victims of child sexual abuse. No additional EU-level action on victim support would mean that the quality and accessibility of victim support is not expected to improve significantly. In particular, it is unlikely that victims of child sexual abuse would be able to receive the necessary assistance to have the images and videos of their abuse removed swiftly to reduce the negative impact on their wellbeing.

Baseline costs

In the baseline scenario, no action would be taken, and no new structures established. Hence, no additional costs would be incurred. However, no EU action means that there would be **no additional efforts to achieve greater efficiency and cost savings**.

On prevention and assistance to victims, action would continue to be taken independently by Member States, academic institutions and civil society institutions. These actions may contribute to the reduction in relevant offences and better support for victims. However, if no action is taken to facilitate the flow of information between stakeholders, pooling resources and avoiding overlaps, these efforts are likely to continue to be fragmented, duplicating existing research and actions while insufficiently covering other areas.

The use of EU funds in the form of project grants (union actions and national actions) would not be significantly improved. This could lead, for example, to duplication of projects across the EU.

The baseline option would not address the limited nature, lack of coordination and unclear effectiveness of Member States' current efforts to prevent child sexual abuse and assist victims. As a result, the overall negative economic impact of child sexual abuse ia not expected to improve.

3.2. Overview of all choices analysed

Given the above considerations, it **became evident that a central entity was needed**, as the existing entities or networks thereof could not be expected to address the problem drivers and meet the specific objectives.

The process to determine the implementation choices started with a **mapping** of existing entities and their present functions in order to identify **possibilities to build on existing structures** and make use of existing entities, or simple use them as possible references or benchmarks. For the mapping purposes, the examples were divided in two main types, depending on whether they required specific legislation to be set up:

1) entities that **do not require specific legislation** to be set up:

c) Centre embedded in a unit in the European Commission (DG HOME, e.g. Radicalisation and Awareness Network, RAN).

---

victims' rights the specific provisions for victims of child sexual abuse contained in the Child Sexual Abuse Directive.

[576] EU Strategy on victims' rights, 24 June 2020, COM/2020/258 final.

d) Entity similar to the EU centre of expertise for victims of terrorism.

2) entities that **require specific legislation** to be set up:

c) Centre **embedded** in an **existing entity**:
   - EU body:
     - Europol
     - FRA
   - Other:
     - National or international entity (public or private such as an NGO, e.g. a national hotline or INHOPE network of hotlines).

d) Centre set up as a **new entity**:
   - EU body:
     - Executive agency (e.g. European Research Executive Agency, REA, European Education and Culture Executive Agency (EACEA))
     - Decentralised agency (e.g. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), European Institute for Gender Equality (EIGE), European Union Intellectual Property Office (EUIPO)).
   - Other:
     - National entity:
       - Foundation set up under national law (e.g. Academy of European Law (ERA), set up under German law);
       - Member State authority (e.g. new Dutch administrative authority to combat CSA and terrorist content online, under preparation);
     - International entity:
       - Inter-governmental organisation (e.g. European Space Agency (ESA), European Organisation for the Safety of Air Navigation (EUROCONTROL));
       - Joint undertaking (public-private partnership, e.g. Innovative Medicines Initiative, Clean Sky Joint Undertaking).
       - Non-governmental organisation (e.g. CEN/CENELEC, EuroChild).

The mapping also included **combinations of the above**, i.e. with some functions of the Centre under one entity and other functions under another, e.g. a combination of Europol and:

- an independent entity set up under national law;
- FRA;
- a unit in the Commission; or
- and NGO (e.g. a hotline).

Finally, the mapping also included three relevant entities outside of the EU, which carry out similar functions to those intended for the EU centre, and which could provide useful references in some areas (e.g. costs, organisational issues, etc):

- US National Centre for Missing and Exploited Children (NCMEC);
- Canadian Centre for Child Protection (C3P); and
- Australian Centre to Counter Child Exploitation (ACCCE).

The following section presents in detail the above mapping of existing examples of entities that could serve as a reference for the centre, and which will serve as the basis to determine the choices retained for further assessment (described in section 3.3.) and those discarded early (described in section 3.4.). Each reference is analysed in terms of the legal basis, funding, governance, operational capacity, location and estimated time to set up.

1) entities that **do not require specific legislation** to be set up:

a) Centre embedded in **a unit in the European Commission** (DG HOME, e.g. Radicalisation and Awareness Network, RAN[577]).

- Legal basis: no legal personality, administrative decision required to integrate it in an existing unit or create a new unit. In the case of RAN, the Commission announced its creation under objective 2 of the Commission Communication on the Internal Security Strategy (COM [2010] 673).
- Funding: operational expenditure supporting policy implementation + possible a framework contract under ISF to support activities of the unit (as in the case of RAN).
- Governance: RAN is managed by DG HOME, with administration and logistics outsourced to a contractor.
- Operational capacity: a unit in DG HOME could potentially serve as a hub of expertise, offer a platform for national authorities and experts to exchange knowledge and experience, and manage networks, projects and information exchange platforms. In the case of RAN, it organises thematic working groups for frontline practitioners to share their knowledge, experiences and approaches with one another, and peer review each other's work. RAN also produces publications, which are shared with its network of frontline practitioners.
- Location: RAN does not have a physical location, it is overseen by DG HOME, with the contractor based in Brussels.

b) **Entity similar to the EU Centre of expertise for victims of terrorism**[578].

- Legal basis: no legal personality, pilot project set up by the Commission and run by a consortium of victim support associations led by Victim Support Europe.
- Funding: two-year pilot project funded by the European Parliament, implemented by DG JUST under public procurement (EUR 1 million for 2 years).

[577] See here for more information.
[578] See here for more information.

- Governance: Executive committee made of a project manager from the consortium running the project, representatives from DG JUST and HOME, representatives of victim support organisations (in practice the centre is governed like any project funded by the Commission).
- Operational capacity: provides training and handbooks, serves as a hub of expertise. It also offers a platform for national authorities and victim support organisations to exchange knowledge and experience, maintains a database with information on experts in different fields.
- Location: no physical location, overseen by DG JUST/HOME, project coordinator based in Brussels.

2) entities that **require specific legislation** to be set up:

a) Centre **embedded** in an **existing entity:**

- **EU body - Europol**:

- Legal basis: Europol regulation (Regulation (EU) 2016/794) would need to be updated to cover all tasks assigned to the Centre. No separate legal personality for the Centre.
- Funding: financed by the EU budget (around 200 M EUR/year). Funding would need to be topped up by around 25 M EUR/year.
- Governance: through a Management Board with one representative from each EU Member State taking part in the Europol Regulation and one representative from the European Commission. Denmark has an observer status.
- Operational capacity:
    - Around 1300 staff (including staff with employment contracts with Europol, Liaison officers from Member States and third states and organisations, Seconded National Experts, trainees and contractors).
    - Can host databases ensuring data protection.
    - Has the capacity to create specialised Centres that are able to create focused teams; developing good practices for crime prevention; providing training and capacity building measures at national level; build a set of specialised intelligence so that the centres act as knowledge hub per type of crime.
    - Europol provides for notice and takedown services collaborating with online service providers on terrorist content online.
    - For the specialised Centres a Programming Board can be created allowing for collaboration with a specific set of stakeholders that know best a certain type of crime; Europol can cooperate with third countries and other inter-governmental organisations; Europol has the possibility to conclude memorandums of understanding (MoUs) for collaboration with other EU decentralised agencies.
- Location: The Hague (the Netherlands).

- **Fundamental Rights Agency (FRA):**

- Legal basis: FRA's founding regulation would need to be updated to cover all tasks assigned to the Centre. No separate legal personality.
- Funding: financed by the EU budget (around 25 M EUR/year). Funding would need to be doubled (increase by around 25 M EUR/year).
- Governance: through a Management Board with one representative from each EU Member State taking part in the Europol Regulation and one representative from the European Commission. Denmark has an observer status.
- Operational capacity: FRA publishes policy briefs and research in the are of fundamental rights, and serves as an advisor in that area to EU institutions, Member States and other stakeholders.
- Location: Vienna (Austria).

- **Other: National or international (e.g. a national hotlines or INHOPE network of hotlines)**

- Legal basis: INHOPE is an association of hotlines from multiple countries, governed by Articles of Association and Rules and Regulations. The original Dutch version of the Articles of Association (Deed 25th May 2018), only the text of the Dutch notarial deed executed in the Dutch language prevails. Member hotlines have to comply with a Code of Practice.
- Funding: financed by the Commission. Under CEF Telecom in the MFF 2014 – 2020: EUR 76.4 m or approx. EUR 11 m per year. Funding goes via grants (EUR 63.3 m) to the Safer Internet Centres (composed of awareness raising, helpline, Hotline), and via service contracts (MEUR 13.1) to coordination and support providers.
- Governance: Members vote to elect a President who leads an elected Executive Committee, also known as the Board. The Board, which currently consists of six people, is also charged with the management and administration of the Association. Hotlines receive reports on instances of CSAM. If the content is qualified as illegal and is hosted in an EU country, hotlines notify Internet Service Providers for the swift removal of the content, and report the case to the relevant law enforcement agency for victim identification purposes. INHOPE's research role is focused on statistics about the reports it receives and its work.
- Operational capacity: hotlines receive reports on instances of CSAM. If the content is qualified as illegal and is hosted in an EU country, hotlines notify Internet Service Providers for the swift removal of the content, and report the case to the relevant law enforcement agency for victim identification purposes.
- Location: Netherlands. INHOPE brings together 50 hotlines from 46 countries.

b) Centre set up as a **new entity**.

- **EU body: Executive agency** (e.g. European Research Executive Agency (REA), European Education and Culture Executive Agency (EACEA)):
  - Legal basis: Regulation (EC) No 58/2003
  - Funding: dedicated funding from EU budget.
  - Governance: the policy of executive agencies is steered by parent DGs (according to their annual Work Programme). As an executive agency's sole task is to implement EU Programmes, there is no need for direct policy steer/advice from Member States or other relevant actors.
  - Operational capacity: the functions of executive agencies are limited by Regulation (EC) No 58/2003.
  - Location: European Union.

- **EU body: Decentralised agency**

  Possible examples:

  European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)
  - Legal basis: Regulation (EC) 1920/2006.
  - Funding: received stable funding under the Commission's budget (15 million EUR/year). Received funding from IPA for concrete actions (e.g. actions in Balkan countries). It can receive funding from other sources: payments for services rendered, contributions from organisations (international, NGOs, governmental) /third countries. Currently receives donations from Norway and Turkey.
  - Governance: supported by two statutory bodies (Management Board and Scientific Committee) to advise and assist in the decision making process.
  - Operational capacity: staff of 100 people. Provides the EU and its Member States with a factual overview of European drug problems and a solid evidence base, allows sharing best practice and new areas of research. Focused on collecting, analysing and reporting – provides tools such as publication database, statistics compilations, country reports etc. Cooperates with relevant networks, third countries (candidate and potential candidates to the EU, European Neighbourhood Policy (ENP) area countries), and regional and international organisations: as well as with Europol on monitoring of drugs problem.
  - Location: Lisbon, Portugal

  European Institute for Gender Equality (EIGE)
  - Legal basis: Regulation (EC) No 1922/2006.
  - Funding: received stable funding under Commission budget, 8 M EUR/year. It can receive funding from other sources: payments for services contributions from organisations or third countries and Member States.

- Governance: governed by a Management Board: Member States on rotation basis and European Commission. Supported by Experts' Forum as Advisory Body.
- Operation capacity: staff of 45 people. EIGE cooperates with EU, national and international institutions and organisations. It focuses on support to research and policy-making, maintains statistics database.
- Location: Vilnius, Lithuania.

European Union Intellectual Property Office (EUIPO)

- Legal basis: Regulation (EU) 2017/1001.
- Funding: EUIPO does not appear in the EU budget, as its expenditure is covered by a 240 M EUR revenue made yearly. Their main source of income comes from registrations and trade-market design.
- Governance: the governance structure of the EUIPO consists of a Management Board and a Budget Committee, each composed of one representative from each Member State, two representatives from the Commission and one representative from the EP.
- Operational capacity: the EUIPO is responsible for the observatory of the infringement of IP rights. It also assists enforcement authorities with training, awareness raising and tools. They cooperate with DG HOME and have formal service level agreements with 14 DGs and 7 agencies and bodies (Eurojust, Europol, CEPOL, TAXUD, and OLAF). They have seconded staff in Europol for this coordination.
- Location: Alicante, Spain.

- **Other legal forms**

Private entity under national law of an EU Member State: Foundation – Academy of European Law (ERA)

- Legal basis: foundation having legal personality under the German Civil Code, Para.§ 80 to 88. Established at the initiative of the European Parliament.
- Funding:
  - Public foundation supported by donations from EU Member States, regions (e.g. DE Federal States), city of Trier, private entities;
  - Recipient of an operating grant under the Jean Monnet programme;
  - Budget in 2019 – EUR 8,4 million (around 5 million EU contribution).
- Governance:
  - Governing Board (2 members form EU institutions – EP and CJEU, 1 member/MS and relevant associations), Board of Trustees (advisory body), Executive Board;

- The Commission is represented in the Board of Trustees, which provides advice to the main governance bodies of the institution;
- ERA entails Member States' governments as Members of the Governing Board and the Executive board (represents the organisation at international Fora).

- Operational capacity:
  - Delivers training in European law – organisation of conferences, seminars, summer courses
  - Permanent staff (83) deals mostly with organisation, administration, finance and communication. Cooperates with experts in the field to deliver training.
- Location: Trier, Germany

Member State Authority (e.g. new Dutch Administrative Authority, under preparation)

- Legal basis:
  - Legislation establishing the authority is under preparation;
  - Independent public law administrative body;
  - Established to enforce take-down of CSAM, in cooperation with hotlines and law enforcement.
- Funding: provided by the Ministry of Justice.
- Governance: TBC, but the Ministry of Justice will have no influence over the management of the authority, appointment of director.
- Operational capacity (envisaged):
  - Receive notification of CSAM, issue notice of take down to companies and follow-up the removal of CSAM;
  - Enforce administrative fines, issue transparency reports;
  - Conduct proactive search for CSAM;
  - Access to database of hashes.
- Location: the Netherlands.

- **Others: international entity.**

Inter-governmental organisation (e.g. European Space Agency (ESA), European Organisation for the Safety of Air Navigation (EUROCONTROL))

- Legal basis:
  - ESA: ESA Convention.
  - EUROCONTROL: International Convention, to which the EU accessed through Protocol on the accession.
- Funding:
  - Contributions from members and associates, EU funding possible (e.g. annual contribution to ESA);
  - ESA's budget: 6.49 billion EUR; Eurocontrol budget 865 M EUR.

- Governance:
  - ESA: Each Member State is represented in the Council (governing body);
  - EUROCONTROL: the Permanent Commission (high-level State representatives) and the Provisional Council.
- Operational capacity:
  - Can cooperate with a number of stakeholders including the EU;
  - Can handle sensitive data (though not personal data), High level of security.
- Location: European Union.

Joint undertaking (public-private partnership, e.g. Innovative Medicines Initiative, Clean Sky Undertaking)

- Legal basis: Council Regulation based on Article 187 TFEU or on Article 157 TEC (now Article 173 TFEU).
- Funding: contributions from members and EU (contribution set out in the founding regulation, paid the general budget of the Union allocated to the relevant programme).
- Governance: governing Board consisting of founding members.
- Operational capacity: limited to publishing open calls for proposals and managing grants.
- Location: European Union

Non-governmental organization (e.g. CEN/CENELEC, EuroChild)

- Legal basis: registered as non-profit/non-governmental organisation under Member State law (i.e. AISBL- a non-profit international association with legal personality based Belgian Code of companies and associations);
- Funding: donations contributions, sale of goods and services, investments, EU funding possible through project grants).
- Governance: Member States and the EU institutions could not be part of their governance. To avoid questions about their independence, NGOs are unlikely to add other stakeholders in their governance as well.
- Operational capacity:
  - Capacity to conduct reporting activities, e.g. annual data reports;
  - Some NGOs have database hosting capacities.
- Location: European Union

Organisations outside the EU

US National Centre for Missing and Exploited Children (NCMEC)

- Legal basis: not-for-profit corporation, with specific roles recognised under US federal law (18 U.S. Code § 2258A).

- Funding: budget of approximately 26 M EUR/year, over half of it covered by US Federal Government funding, with the remainder coming from private contributions and other sources.
- Governance: board of Directors (including public representatives, industry members, ex-law enforcement).
- Operational capacity:
    - US companies are obliged by law to **report** instances child sexual abuse to NCMEC;
    - NCMEC serves as clearinghouse, receiving, filtering and forwarding reports to relevant law enforcement in the US and globally.
- Location: Alexandria (Washington D.C), USA

Canadian Centre for Child Protection

- Legal basis: Registered as national charity under Canadian law.
- Funding: large part of donations are from international foundation (Oak Foundation, Children's Investment Found Foundation). Some funding comes from private donors, very limited funding from the private sector, subject to strict conditions to avoid conflict of interests.
- Governance: the Board of Directors is composed of volunteers from a variety of disciplines, including law enforcement, education, psychology, medicine, law, finance, and public service.
- Operational capacity:
    - The Canadian Centre offers crisis assistance, works with survivors, prepares educational and prevention materials;
    - It receives reports of CSAM via cybertipline, and runs Project Arachnid – web crawler and platform to reduce the availability of CSAM;
- Location: Winnipeg, Manitoba, Canada

Australian Centre to Counter Child Exploitation (ACCCE)

- Legal basis:
    - Australian Federal Police tasked with creating a hub of expertise and specialist skills needed to detect, disrupt, prevent and investigate child exploitation;
    - Coordinates and support to Australia's law enforcement efforts, supports investigations. Brings together key stakeholders, allows cross-pollination of resources, knowledge and skillsets between stakeholders.
- Funding: Funded from the federal government's budget - AUS$68.6m (approx. 44 M EUR) over 2018-2022.
- Governance: Board of Management consists of representatives of federal and state police, Office of the eSafety Commissioner, Australian Criminal Intelligence Commission, Department of Home Affairs.
- Operational capacity:

- Reporting – provides a platform to report inappropriate, harmful or criminal activities that have occurred to children online, including CSAM, grooming but also cyberbullying and other.
- Triage of reports of child exploitation.
- Intelligence inputs.
- Specialist investigative capability: victim identification, Covert Online Engagement Team (in this aspect fulfils role similar to Europol's Cybercrime Centre).
- Prevention and online child safety:
  - Research – can commission studies.
  - Prevention – online safety education resources.
  - Victim protection – resources on counselling and support for victims.
- Cooperates with government agencies (including law enforcement, relevant departments of the government), state authorities, victims associations, foreign law enforcement.

- Location: Brisbane, Australia.

3.3. Description of implementation choices

Following the mapping of all possible choices, these were analysed in detail to select the final choices to be retained for comparison.

The analysis considered in particular factors such as legal and operational capacity, governance, financial sustainability, independence, accountability and transparency, and operational synergies, structured along two groups of considerations:

- **Functions** that the centre could take, closely linked to its **specific objectives**:
  - Support prevention efforts.
  - Support victims.
  - Contribute to the detection, reporting and removal of CSA online.
- **Forms** that the centre could take to best fulfil the above functions, and which are determined by:
  - Legal status: both the legal basis to set up the centre (if any) and the legislation to allow it to perform its functions (e.g. processing of personal data).
  - Funding: the sources that would allow the centre to ensure **long-term sustainability and independence** of the centre, while avoiding conflict of interest.
  - Governance: it should ensure 1) proper **oversight** by the Commission, and other relevant EU institutions and Member States; 2) **participation** of relevant stakeholders from civil society organisations, industry, academia, other public bodies, for example through advisory groups; 3) ensuring **neutrality** of the centre from overriding private and political interests.

These two considerations are closely interlinked: the level of ambition for the functions, whether the centre should take on all three of them and to what degree, determines the choice of the optimal form to enable those functions. In turn, the choice of the form, excludes or enables the centre to take on certain functions. The analysed implementation choices reflect different levels of ambition.

A: set up an EU Centre focused on prevention and assistance to victims through practical measures

This choice proposes a centre that is set up through **non-legislative (practical) measures**. It would take on **functions** mostly of **prevention and assistance to victims,** and the **form** of an EU-funded **coordination hub**, managed by the Commission with possible support from a contractor (similar to the **Radicalisation and Awareness Network, RAN**[579]). This choice constitutes policy measure 2 in the impact assessment.

Functions:

- Prevention.
    - Facilitate the implementation of the practical measures on **prevention** of measure 1, including supporting Member States on the implementation of the relevant provisions of the Child Sexual Abuse Directive (e.g. through expert workshops), and serving as a hub of expertise to support evidence-based policy in prevention. For example, it could develop and manage an **online platform** where professionals working on prevention could find information relevant to their work.
    - Support the further development of the **prevention network** introduced in the EU strategy for a more effective fight against child sexual abuse. The centre would ensure the coordination and support for the network by e.g. facilitating the planning of its work, preparing future publications, creating and maintaining a database of good practices, gathering statistics. This would allow the network to grow to its full potential.
    - Help **develop research** on prevention, including on the effectiveness of prevention programmes
    - **Facilitate dialogue** among all relevant stakeholders, within and beyond the EU, on prevention efforts.
- Victims' assistance.
    - Similarly to its role in prevention, the centre could facilitate the implementation of the practical measures on **assistance to victims** of measure 1, including supporting Member States on the implementation of the relevant provisions of the Child Sexual Abuse Directive, serving as a hub of expertise to support evidence-based policy development in assistance to victims, for example, through an **online platform** where **professionals** working on assistance to victims could find information relevant to their work.
    - Set up an **online platform** where **victims can find information** on support resources that are available to them in their area or online.
    - Help **develop research** on assistance to victims, including on the effectiveness of short-term and long-term assistance programmes, as well as on victims' needs in the short- and long-term.

[579] See here for more information about RAN.

- **Facilitate dialogue** among all relevant stakeholders, within and beyond the EU, on victims' assistance efforts.
- The lack of legislation underpinning the set-up of the centre would prevent it from conducting proactive searches of CSAM based on victims' requests for help to have their images and videos taken down.

- Detection, reporting and removal.
  - In addition to the main functions on prevention and assistance to victims, the centre could also facilitate the implementation of the practical measures on **detection and reporting** of measure 1.
  - These practical measures could include developing codes of conduct and standardised reporting forms for service providers, improving feedback mechanisms and communication channels between public authorities and service providers, and facilitating through funding and coordination the sharing between service providers of databases of hashes and detection technologies. It could also include support to service providers to implement **safety by design**, e.g. by validating design features aimed at protecting children from sexual abuse, such as more sophisticated age verification or parental controls.
  - The centre would not be able to take a more active role in the detection, reporting and removal process in the absence of a **legal basis for the processing of personal data** involved in the process.

Form:

- Legal status.
  - As a coordination hub managed by the Commission, the centre would **not have its own legal personality**.
- Funding.
  - The centre in this form would be funded under the **Internal Security Fund**. The support to running the centre would require a framework contact, which could be supplemented by project grants to relevant stakeholders on a case by case basis.
- Governance.
  - The centre would be **under the direct responsibility of the Commission**. The Commission would steer the activities of the centre, while possibly delegating the implementation of specific activities and the day-to-day management to a contracted entity. In this scenario the contractor would take on the administrative activities such as drafting work-plans, organising meetings, maintaining an online platform and carrying out other support activities as needed.
  - This form would guarantee alignment between centre's work and Commission's policies and actions. At the same time, while there could be a

possibility of input from stakeholders e.g. through an advisory group, there would be no formal governance structure in which they could participate.

B: set up an EU Centre to prevent and counter child sexual abuse as an independent EU body (decentralised agency)

This choice proposes a centre as a **new, independent EU body** in the form of a decentralised agency.

Functions:

- Prevention.
    - Facilitate the implementation of the practical measures on prevention of measure 1, including supporting Member States on the implementation of the relevant provisions of the Child Sexual Abuse Directive (e.g. through expert workshops), and serving as a hub of expertise to support evidence-based policy in prevention. For example, it could develop and manage an online platform where professionals working on prevention could find information relevant to their work.
    - Support the further development of the prevention network introduced in the EU strategy for a more effective fight against child sexual abuse. The centre would ensure the coordination and support for the network by e.g. facilitating the planning of its work, preparing future publications, creating and maintaining a database of good practices, gathering statistics. This would allow the network to grow to its full potential.
    - Help develop research on prevention, including on the effectiveness of prevention programmes
    - Facilitate dialogue among all relevant stakeholders, within and beyond the EU, on prevention efforts.
    - Fund or help facilitate funding (e.g. improve the update of EU existing EU funding) of prevention initiatives.
- Victims' assistance.
    - Similarly to its role in prevention, the Centre could facilitate the implementation of the practical measures on assistance to victims of measure 1, including supporting Member States on the implementation of the relevant provisions of the Child Sexual Abuse Directive, serving as a hub of expertise to support evidence-based policy development in assistance to victims, for example, through an online platform where professionals working on assistance to victims could find information relevant to their work.
    - Set up an online platform where victims can find information on support resources that are available to them in their area or online.
    - Help develop research on assistance to victims, including on the effectiveness of short-term and long-term assistance programmes, as well as on victims' needs in the short- and long-term.

- Facilitate dialogue among all relevant stakeholders, within and beyond the EU, on victims' assistance efforts.
- Most agencies are limited to coordination and exchange of information; however, it is possible to make specific provisions to allow them to process personal data.
- The legal basis of new agency could enable it to receive requests of support from victims to have their images and videos taken down and conduct proactive searches of CSAM following these requests, in cooperation with hotlines where needed.
- The Centre would carry out the non-legislative actions on assistance to victims.

- Detection, reporting and removal of CSA online.
  - An agency ensures **independence** from private influence and is well-placed to take on the role of ensuring transparency and accountability of the detection, reporting and removal process.
  - The legislation establishing the Centre as a new, independent entity, would provide the legal basis to carry out **all the functions** described concerning the detection, reporting and removal of CSA online, in particular with regard to **processing of personal data and child sexual abuse material**.
  - In particular, the legal basis should contain provisions to allow the agency to process personal data and host databases of indicators of CSA online. This would allow it to notably prepare and maintain these databases, process the reports from service providers, and contribute to the removal process by searching CSAM proactively.
  - The new entity would seek to build on existing efforts and **avoid unnecessary disruption and duplication.** It would focus on supporting what is working well and contributing to address the existing gaps in the process. This means that the centre would **cooperate closely** with **a wide range of stakeholders** active in the detection, reporting and removal process, including service providers, public authorities and civil society organisations, in the EU and third countries.
  - The Centre would work with a wide range of stakeholders including law enforcement (Europol, and national law enforcement agencies), NGOs (e.g. hotlines), service providers, and academia. In particular, the centre would **work very closely with Europol,** facilitating its current activities of analysis and channelling of reports to Member States for action, and with the network of hotlines, to facilitate removal and build on their expertise and experience, especially when it comes to the specificities of the national context, e.g. concerning what is considered illegal in their jurisdiction above and beyond the core definitions in the CSA Directive, or concerning efforts by service providers established in their jurisdiction.

- The new entity would also be able to effectively ensure **accountability and transparency**, thanks to its fully independent status and its expertise in the detection, reporting and removal process.

Form:

- Legal status.
  - The Centre would have its own legal personality as a decentralised EU agency, with a legal basis set up under this initiative.
- Funding.
  - The Centre would be funded mostly by the Commission. As an EU agency it would have its own budget line. The funding would come from the budget managed by the Directorate-General for Migration and Home Affairs.
  - To minimise the strain on the EU budget, the Centre may be able to receive additional funding from other sources such as Member States, not-for-profit donor organisations, and the private sector under strict conditions to prevent any conflict of interests or loss of independence, overseen by the governance body.
- Governance.
  - The Centre would be supervised by the Commission as part of its management board. To ensure that the centre maintains its **quality**, and in particular its **neutrality** and a balanced consideration of all the relevant rights at stake, it will be subject to periodic reporting to the Commission and to the public. The governance structure would also ensure participation of all the relevant stakeholders representing the different interests and rights at stake (including both children's rights and internet users' privacy rights), while strictly avoiding conflicts of interests, for example through their participation in management and advisory bodies.
  - The Centre would be subject to the highest standards with regard to cybersercurity and data protection, and will be under the supervision, inter alia, of the data protection authorities of the Member State hosting it.

C: set up an EU centre to prevent and counter child sexual abuse with some functions in Europol and others in an independent organisation under Member State law

This choice proposes a "hybrid" centre with a structure split in two: **some functions in Europol** and **other functions** in a **new, independent entity** with its own legal personality. Given its current expertise, **Europol** would retain the functions concerning **detection, reporting and removal** of CSA online, and the **new entity** would focus on **prevention and assistance to victims**.

Functions:

- Prevention.
  - The part of the centre located in a new independent body would carry out the non-legislative actions on prevention described in **choice A**.

    - The centre would be able to build on Europol's experience on prevention activities focused on decreasing the likelihood that a child falls victim of sexual abuse through **awareness raising campaigns**.
    - For the other main type of prevention activities, focused on decreasing the likelihood that a person offends, the Centre, as an entity separate from Europol, would have **more autonomy** to develop **new expertise**, currently not existing in Europol. It would also be able to **fund or help facilitate funding** of prevention initiatives.
- Victims' assistance.
    - The part of the centre located in a new independent entity would carry out the non-legislative actions on assistance to victims described in **choice A**.
- Detection, reporting and removal of CSA online.
    - The part of the centre under Europol would carry out this function.
    - **Europol's legal basis** would be **expanded** to enable it to support the detection, reporting and removal process as described above (specific objectives), with all the necessary conditions and safeguards.
    - This could include enabling Europol to receive requests of support from victims to **have their images and videos taken down** and conduct proactive searches of CSAM following these requests, in cooperation with hotlines where needed.

Form:

- Legal status.
    - The part of the centre under Europol would operate under the **Europol Regulation**. The Regulation would need to be modified so that Europol's mandate can cover the additional functions concerning detection, reporting and removal of CSA online.
    - The part of the centre under a new entity would have its own legal personality as an **independent organisation** established under **a Member State's law**.
- Funding.
    - The part of the centre under Europol would be funded through **Europol's budget**, which would need to increase to provide for extra staff and equipment.
    - The part of the centre under a **new entity** would operate under a Member State law, entailing that its employees, they are assumed to be employed under the provisions of the national law in the host country (i.e. not EU staff).
    - This new entity should be funded mostly by the Commission, to ensure the centre's independence, in particular from potentially overriding private and political interests. This would entail an additional supervision by the European Court of Auditors.
    - The centre could be funded through the Internal Security Fund. Initially, the centre could be launched as a specific action, and later though a national ISF

programme of the Member State where it is established[580], or under a direct grant if appropriate. This part of the centre would be able to receive additional funding from other sources such as Member States, not-for-profit donor organisations, and the private sector under strict conditions to prevent any conflict of interests. This would ensure financial sustainability without compromising the functions of the centre, while minimising the strain on the EU budget.

- Governance.
  - The centre under Europol would be integrated in the **current governance structure in Europol**.
  - The part of the centre under a **new entity** would have the governance structure determined by its legal personality under a Member State's law. In any case, it should allow the participation of the Commission in its governing body and ideally include also key stakeholders such as public authorities, civil society organisation and companies, to facilitate coordination and cooperation, while strictly avoiding conflicts of interests.

D: set up an EU Centre to prevent and counter child sexual abuse within the Fundamental Rights Agency (FRA)

This choice would require legislation to set it up, notably expanding FRA's legal basis to cover the relevant aspects of the detection, removal and reporting process, and the victims' support to have their images and videos removed.

Functions:

- Prevention.
  - FRA could facilitate the implementation of the practical measures on prevention of measure 1. It could collect and analyse data and provide advice in the area of prevention; it could produce materials such as handbooks and guidelines and possibly run awareness raising campaigns.
  - FRA would also be well-equipped to perform the **research-related** roles of the EU centre.
- Victims' assistance.
  - FRA could facilitate the implementation of the practical measures on assistance to victims of measure 1.
  - FRA has considerable expertise in the area of child rights and has contributed to the EU Strategy on the rights of the child.[581] Its work also covers victim's rights.
  - Currently FRA addressed the areas of victims' and child rights on a project basis. If the centre were to become a part of FRA, it would need to be a permanent element of its structure.

[580] In a similar way as the initial funding was provided for the Specific Action 'European Return and Reintegration Network (ERRIN)' under the Asylum, Migration and Integration Fund (AMIF).

[581] EU Strategy on the rights of the child, COM(2021)142 final.

- Detection, reporting and removal of CSA online.
    - Facilitate the implementation of the practical measures on detection and reporting of measure 1.
    - **The legal status of FRA would need to be modified to allow it to support the processing of reports** of child sexual abuse, to host a database of CSAM, and the support to victims who wish to have their images and videos removed from the internet.
    - With regard to ensuring **transparency and accountability** of efforts around combating child sexual abuse, FRA would be able to build on its expertise in ensuring the fundamental rights of citizens in policy making.

Form:

- Legal status.
    - The centre would operate under the FRA Regulation[582]. The Regulation would need to be modified so that FRA's mandate can also cover all the centre functions.
- Funding.
    - The centre would be funded through FRA's budget, which would need to increase to provide for extra staff and equipment.
- Governance.
    - The centre would be integrated in the current governance structure in FRA which includes Member States and the Commission. The involvement of the Commission in the governance would obviously be less direct than in choice A. FRA has a Scientific Committee which guarantees the scientific quality of the FRA's work. Additional mechanism to involve relevant stakeholder groups would need to be created, e.g. though new advisory groups.

3.4. Choices discarded following initial analysis

Entities that do not require specific legislation to be set up, e.g. a designated Unit in the Commission (DG HOME)

The advantage of creating a dedicated unit for the fight against child sexual abuse in DG HOME would be that no specific legal basis would be required. Considering the pressing issue of child sexual abuse, creating a unit that can be implemented relatively quickly and operate in the near future.

The main drawback of this type of implementation choices is that extent to which they could undertake the intended functions is limited due to the lack of legal basis. It would focus on implementation of practical measures through facilitating coordination and exchange of best practices. It could not support operational cooperation between

[582] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights.

providers and law enforcement nor the analysis of materials. The effectiveness of this solution and its expected impact would therefore be low.

Creating a designated unit could also result in the **increased logistical, financial and policy coordination** within the Directorate-General.

Another limitation would be that it could become quite difficult for **external stakeholders** and interests groups to **participate** in the processes of such unit, raising transparency and participatory issues. This would likely result in a **limited buy-in from key actors** in the field, and limit the impact this choice for the centre could make.

Centre fully embedded in Europol

The centre would operate under the **Europol Regulation** governing its mandate. It would require expanding Europol's legal basis so that Europol's mandate can also cover all the centre functions.

Functions:

- Prevention.
    - The centre under Europol would carry out the non-legislative actions on prevention described in **choice A**.
    - The centre would be able to build on Europol's experience on prevention activities focused on decreasing the likelihood that a child falls victim of sexual abuse through **awareness raising campaigns**[583].
    - For the other main type of prevention activities, focused on decreasing the likelihood that a person offends, **new expertise** would need to be developed as Europol does not carry out such prevention activities.
- Victims' assistance.
    - The centre under Europol would carry out the non-legislative actions on prevention described in **choice A**. These are activities not directly related to Europol's core mandate of supporting law enforcement in Member States.
    - Europol's legal basis (currently under revision[584]) would need to be expanded to enable it to receive requests of support from victims to **have their images and videos taken down** and conduct proactive searches of CSAM following these requests, in cooperation with hotlines where needed.
- Detection, reporting and removal of CSA online.
    - **Europol's legal basis** would be **expanded** to enable it to support the detection, reporting and removal process as described above (specific objectives), with all the necessary conditions and safeguards.
    - This would notably mean that Europol's legal basis would need to be changed to enable it to receive reports directly from service providers, and to make

[583] See for example: Say NO! campaign covering all EU Member States as well as UK Norway and Switzerland.

[584] See annex 5, the Commission proposal was adopted in December 2020 and is currently under negotiation between the European Parliament and the Council.

available to them databases of indicators on the basis of which they should conduct the detection of child sexual abuse material (known and new).

- The centre would be able to build on the existing capacities and processes in Europol's European Cybercrime Centre (EC3) to receive the reports of child sexual abuse from online service providers[585]. EC3 also reviews the reports, and eventually enriches them with intelligence before forwarding them to the 18 Member States that have chosen to not receive the reports directly from NCMEC.
- The centre under Europol would not be able to take on the function of ensuring accountability and transparency on efforts by companies to tackle child sexual abuse online. This function, which is not directly linked to supporting law enforcing operations, requires a high degree of **independence**. Being part of a law enforcement agency, which would keep its **current key role** of processing the reports from service providers before forwarding them to Member States for action, the centre may not be seen as a neutral party in the process by online service providers and the public.

- Funding.
  - The centre would be funded through **Europol's budget**, which would need to increase to provide for extra staff and equipment.
- Governance.
  - The centre would be integrated in the **current governance structure in Europol**, which includes Member States and the Commission. The involvement of the Commission in the governance would obviously be less direct than in choice A. Currently, there is no mechanism to involve other, non-law enforcement stakeholders in the governance and management structure (although advisory groups with various stakeholders exist at working level).

Europol (provided that the Europol Regulation is modified so that its mandate can also cover all the centre functions), would have the potential to take on the role linked to detection, reporting and removal of CSA online, as it already takes part in the process of handling the reports. The centre could facilitate the work of national law enforcement agencies, alleviating their workload linked to handling of the reports.

On the other hand, the creation of the centre as part of a law enforcement authority can limit the impact of the actions taken on prevention and victim support. Some tasks would be too far from Europol's core mandate: some of the envisaged functions within prevention and assistance to victims are significantly different from the core law enforcement mandate of Europol. This would require significant capacity building efforts in Europol and the creation of teams that would work on very different tasks from those

[585] As explained in the problem definition (see also annex 6), online service providers currently send their reports to NCMEC, which determines whether they concern the EU, and if so, forwards them to US law enforcement (Homeland Security Investigations) for further transmission to Europol or Member States directly. Europol's current legal basis does not allow it to receive the reports directly from NCMEC.

of the rest of the organisation. This notably includes research on prevention (e.g. on the process by which a person with a sexual interest in children may end up offending) and assistance to victims (e.g. on the long-term effects of child sexual abuse).

Whereas the Centre would be able to build on the established procedures of Europol, being part of a larger entity which covers multiple crime areas may limit the visibility of EU efforts in the fight against CSA. Moreover, the imbalance created by inserting such an entity in a law enforcement agency could create an obstacle to its smooth operation. It would be difficult to justify that Europol expands its mandate to cover prevention and assistance to victims only in the area of child sexual abuse. This could lead to Europol gradually deviating from its core law-enforcement mandate and covering prevention and assistance to victims in multiple crime areas, becoming a "mega centre" of excessive complexity to be able to attend to the specificities of the different crime areas adequately.

A further disadvantage lies in the inherent conflict between Europol's mandate as an organisation to support criminal law enforcement and the role it would need to play in ensuring transparency and accountability of the whole process, including where service providers and other actors are concerned. Service providers have expressed legal concerns about a reporting obligation and exchanging data with law enforcement directly. An example of such potentially problematic cooperation would be receiving the database of indicators (e.g. hashes) from law enforcement on which to conduct the mandatory detection of CSA online. Apart from legal concerns, there is a risk of a perception of partiality, which can hinder open cooperation with the service providers, but also with key stakeholders in the area of prevention and assistance to victims. Such concerns are likely to limit the positive impact of this choice.

In addition, the risk of not appearing as a neutral facilitator could also be seen on the prevention function when it comes to prevention programmes for offenders and people who fear that they might offend. Europol's capacity to reach out to persons who fear that they might offend could be limited by the distrust that its core law enforcement task could generate among those people.

Centre partly in Europol and partly in another entity
Some of the choices analysed considered a hybrid option of establishing part of the Centre in Europol and part in another (new or existing) organisation. This set-up would allow using the advantage of Europol's expertise and current role in the fight against child sexual abuse, and have another entity perform the functions for which Europol is less or no experienced or are not part of Europol's mandate (i.e. assistance to victims and prevention initiatives for offenders and people who fear that they might offend).

- **Europol and Fundamental Rights Agency**

Functions:

- Prevention.
    - Actions relating to prevention would be mostly performed by FRA in this scenario (see section 3.3.4.), while coordinating actions already conducted by Europol (e.g. some awareness-raising campaigns).
- Victims' assistance.

    - Actions relating to assistance to victims would be performed by FRA in this scenario (see section 3.3.4.), except for the support to victims in removing images, which would be carried out by Europol.
- Detection, reporting and removal of CSA online.
    - In this scenario, Europol's legal basis would be expanded to enable it to support the detection, reporting and removal process. The Centre would be able to build on the existing capacities and processes in Europol's European Cybercrime Centre (EC3) to receive the reports of child sexual abuse from online service providers.

This set up would have a number of drawbacks. First, **splitting the centre** between two entities poses coordination risks, and a possible limitation of the synergies that would otherwise occur if all the functions were under the same entity. Additionally, splitting the roles of the centre is **contrary to the concept of holistic response** set out in the EU Strategy for a more effective fight against child sexual abuse. In addition, both agencies have specific mandates and missions, which are only partially compatible with the new tasks they would be given, creating a risk of competition between different and at times mutually exclusive objectives the agencies have to accomplish, such as the tension between providing independent expert advice (e.g. on fundamental rights) and taking on an operational role.

The resources of both agencies would have to be increased, and **additional expertise would need to be brought in**. As explained above in the case of FRA, a shift in the focus of the agency would be needed. In both organisations, embedding parts of the centre in their structure could cause a certain disruption to adapt to the new tasks.

- **Europol and a unit in the Commission**

Functions:

- Prevention.
    - Actions relating to prevention would be mostly performed by the Commission, including coordination of actions already conducted by Europol.
- Victims' assistance.
    - Actions relating to assistance to victims would be mostly performed by the Commission.
    - Europol would receive and process requests from victims to remove images and videos pertaining to their sexual abuse from the internet, provided its legal basis is expanded.
- Detection, reporting and removal of CSA online.
    - This option would build on Europol's experience and capacity to support the detection, reporting and removal process, requiring a significant expansion of resources. In this scenario, the Commission would take on the role of **ensuring transparency and accountability** in the efforts against child sexual abuse.

This choice would suffer from potential coordination issues stemming from dividing the work of the centre between two entities, which exist at different levels in the institutional setup. It would also require a significant investment within the Commission to make available the necessary resources.

- **Europol and an NGO (e.g. hotline)**

Functions:

- Prevention.
    - While both organisations would bring in value with regard to support to the detection, reporting and removal process, neither of them is well-suited to take on the role of a facilitation and knowledge-sharing hub on prevention. None of the existing hotlines currently serves as a hub, and the overall network structure of INHOPE has been kept light-weight. The expertise and resources would need to be significantly expanded. As such activities are out of the normal scope of organisations considered, adding the necessary new functions could disturb the existing structures of the organisation.
- Victim's assistance.
    - Hotlines, if granted the possibility to conduct a proactive search, could also receive requests from victims who want their images removed from the internet, or cooperate on such requests with Europol.
    - The role of a knowledge hub on victim's assistance would suffer from similar drawbacks as in the case of prevention.
- Detection, reporting and removal of CSA online.
    - This option would build on Europol's experience and capacity to support the detection, reporting and removal process. If the NGO involved is a hotline able to perform analysis of reports, it could also contribute to this process. Legislation would be needed to allow proactive search by hotlines in this case.

In terms of structure and governance, in case of an NGO, and particularly a hotline, the EU and other relevant stakeholders may have a limited role in governance, limiting the possibility for steer from the EU. Additionally, this scenario would suffer from potential coordination issues stemming from dividing the work of the centre between two entities.

EU executive agency

This choice would imply creating the centre as an executive agency established under Regulation (EC) No 58/2003[586]. Executive agencies are established for a specific period of time by the European Commission to manage specific activities related to EU programmes.

[586] Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes, *OJ L 11, 16.1.2003.*

This choice was discarded because an executive agency cannot address the array of functions that the potential Centre will require. In particular, an agency created for a finite time period cannot create of sustainable, long-lasting mechanisms needed to achieve the policy objectives of this initiative.

Establishing an EU centre as part of a Member State authority

Functions:

- Prevention
    - Such an entity could be tasked with becoming an effective hub for connecting and disseminating expertise. It could have the potential to cooperate with all relevant stakeholders and take on the role of the prevention functions of the centre.
- Victims' assistance
    - It would be able to conduct proactive search of images and videos on behalf of the victim. However, as a national authority of an EU Member State, there could be limitations on its capacity to carry out its work at EU level.
- Detection, reporting and removal of CSA online
    - An independent public law administrative body would be able to work closely with hotlines and law enforcement. It would be well-suited to collect data on efficiency and times required to take down content, and work with service providers.
    - The possibilities of such entity to **process personal data** may be limited. Also, depending on the condition in the Member State where it is established, the function of receiving reports and maintain a database of indicators could fall under national law enforcement. This could limit its capacity to work across the EU with service providers and other stakeholders, given possibly jurisdiction issues.

This choice was therefore discarded mainly due to possible limitations to work at EU level while being a national entity.

Joint Undertaking

EU public/private partnerships are based on Articles 187 TFEU thereof and take the form of joint undertakings. For the partnerships before the Lisbon Treaty, the legal basis was Article 157 TEC (now Article 173 TFEU) on Industry. The objective of such legal structures is to facilitate investment in knowledge and innovation in Europe. As a result, this legal form could only cover some aspects of the centre's role in relation to research and innovation (if the centre was tasked to conduct research).

The operational role of Join Undertakings is limited to publishing open calls for proposals and managing grants.

This choice was discarded because it would not allow the Centre to take on some of its envisaged core functions, in particular facilitating detection, reporting and removal of CSA online.

Centre as part of the INHOPE network/a national reporting hotline in a Member State.

Functions:

- Prevention
  - The INHOPE network/national hotlines could to some degree facilitate the implementation of the practical measures on prevention.
  - However, hotlines specialise on processing of reports of CSAM, and the research role of INHOPE is focused on statistics about the reports it receives and its work. Currently it **does not have the resources and expertise** to become a hub of expertise and coordination on **prevention**.
- Victims' assistance
  - There is some potential in facilitating the implementation of the practical measures on prevention of measure 1, although the capacity of INHOPE/national hotlines to become a hub of expertise and coordination on **assistance to victims is limited** given the lack of experience and existing resources.
  - Hotlines, if granted the possibility to conduct a **proactive search**, would be able to receive requests from victims who want their images removed from the internet. It would require the establishment of legal basis and a significant increase in resources. On the other hand, national hotlines could be a natural point of contact for survivors.
- Detection, reporting and removal of CSA online
  - The number of reports received from the public is not nearly as high as the number of reports from service providers.[587] If the EU-based service providers were obliged to report to INHOPE hotlines, the **volume of report would be higher** than what the network could effectively handle under the current resources.

In terms of structure, INHOPE is an international association of hotlines. Its **governance is in the hands of members of the association**. This greatly limits the possible steer from the EU or other relevant stakeholders (e.g child's rights and victims' associations NGOs). While INHOPE is supported by the EU, it does **not focus its activities on Europe** only, and needs to accommodate the needs of members globally. This could limit the effectiveness of the centre as a European organisation.

[587] According to the INHOPE 2020 report, there were 1,038,268 content URLs exchanged via ICCAM globally. While this number does not specify how many reports were received by hotlines in relation to those URLs, it has to be noted that this number encompasses the whole world. The only hotline to perform proactive monitoring in Europe, the Internet Watch Foundation, indicated that, in 2020, only 13% of CSAM it detected resulted from user reports. NCMEC received around 300,000 reports received from users, out of a total of 21.7 million reports, equalling 1.4%.

Therefore, while INHOPE would be a **key partner** for the centre, it does not appear to be best placed to take its role.

4. IMPACTS OF IMPLEMENTATION CHOICES

3.5. Qualitative assessment

The qualitative assessment of the implementation choices considers their social, economic, and fundamental rights impacts.

Social impact

All proposed measures except the baseline scenario would improve, to differing degrees, the capacity of all relevant actors in the EU to respond to this crime and mitigate its social consequences. Any improvement of this capacity could also lead to improved deterrence for criminals, better protection of victims and improved security for children.

The impact level differs based on the whether the Centre would coordinate and support existing stands of work, or whether it would take on a leading role in the fight against child sexual abuse, opening up new areas of work that could have a positive impact on society in general.

Under all options except the baseline, support for the implementation of safety and privacy by design features by online service providers provided by the centre could considerably improve the protection of children online. The Centre could also provide feedback to policymakers, both on prevention-related issues and as an advocate for victims. This would increase the social impact of the Centre in the long-term, ensuring that future policy can be based on a more solid body of evidence and hence may offer improved solutions that better address actual problems.

Choice A: EU Centre on prevention and assistance to victims

Establishing an EU centre on prevention and assistance to victims would help to improve coordination and facilitate the implementation of practical measures in these areas. The centre is expected to bring a limited impact in terms of enhanced cooperation and exchange of knowledge and best practices in the field of prevention and assistance to victims. It could also lead to some improvements in the feedback given to policy makers.

The support for practical measures on victim support and prevention would be expected to have a positive impact on the ability of society and authorities to prevent these crimes and on the experience of survivors of child sexual abuse, as they might have easier access to information about available resources, and these resources might be strengthened through exchange of best practice among Member States, facilitated by the Centre. Similar positive impacts could be expected from the support for development of codes of conduct and safety by design. However, the positive impact would be expected to be limited due to the limited degree of standardisation that would likely result from purely voluntary practical measures, especially in view of the sensitivity both of the content to be identified and of the impact on the rights of all users.

This measure is therefore expected to have a **positive** social impact overall, albeit only to a limited extent.

Choice B: Set up an EU Centre to prevent and counter child sexual abuse as an independent EU body

This choice would improve the ability of relevant public authorities to respond to cases of online child sexual abuse, leading to more victims being rescued and more cases of crime prevented. The centre could facilitate the work of national law enforcement agencies, alleviating their workload linked to handling of the reports.

Maintaining a single, reliable database in the EU of known CSAM would also improve the ability of service providers to detect it in their systems. Europol has a good capacity to host such a database, also in view of the necessary security and data protection procedures and the channels it has already set up for cooperation with national law enforcement and with NCMEC.

Assisting victims in removing images and videos depicting their abuse from the internet would address a gap in the current efforts. It could significantly improve their psychological well-being by reducing the stress of knowing that images and videos depicting their abuse are circulating online. The positive social impact of this choice would be that victims can focus on recovery rather than pursuing service providers to demand the removal, potentially causing retraumatisation and legal jeopardy given the illegal nature of possession of CSAM. Victims may also be more inclined to turn to an independent organisation, without links to law enforcement, for help. The centre would have also a greater impact in realising the potential of the network of hotlines for victim support. In addition, it would add credibility to the transparency and accountability tasks if these can be performed by a separate organisation whose mission is dedicated to ensuring such transparency and accountability.

This option would also likely improve the rate and speed of take-down of CSAM, and help to fully realise the potential of the currently underutilised network of hotlines, thereby improving the cooperation between civil society organisations, service providers and public authorities.

An advantage of this option is that it encompasses all of the centre's roles, allowing processes to be streamlined in one entity only. One designated entity taking up different tasks in the fight child sexual abuse facilitates processes and can potentially increase their efficiency. It can reduce the burden on law enforcement and allow them to focus on those tasks only they can perform, and it can provide a reliable and independent point of contact for service providers as well. In addition, one entity taking up several tasks related to the fight against child sexual abuse increases the visibility of such entity and could encourage victims to take all steps necessary for their recovery and fighting offenders. Creating a dedicated agency would also improve the centre's visibility and send an important message about the dedication of the EU as a whole to combating child sexual abuse more effectively and to ensuring that rules apply online as they do offline. It would place the EU at one level with those leading the fight against child sexual abuse worldwide, such as the United States with NCMEC.

One disadvantage of this option may be that a completely new entity would lack an established network of expertise, organisations and communication channels at first, potentially reducing the efficiency of its operations in the beginning. However, this

disadvantage most likely only concerns the first months after the creation of a centre and expertise and networks can be quickly built up, also based on cooperation with Europol.

In summary, this implementation choice would contribute to increased security of EU citizens, children in particular; it would also serve to diminish criminals' feeling of impunity. In reducing revictimisation caused by the recirculation of CSAM, maintaining a database would facilitate the task for service providers and have a significant positive impact on victims. If the centre is to be a new independent entity, this option can also fully address the need for an improved framework for prevention efforts to decrease the prevalence of child sexual abuse, especially where measures targeting would-be or repeat offenders are concerned, and would provide the important transparency and accountability functions a centre would need to perform.

This choice is considered to have a **highly positive** impact on society by improving the security of EU citizens and contributing to the well-being of victims of child sexual abuse.

Choice C: Set up an EU Centre to prevent and counter child sexual abuse with some functions in Europol and others in a separate organisation under Member State law

In this choice, the impact on the ability of relevant public authorities and service providers to respond to cases of online child sexual abuse would be improved when compared to the baseline.

The choice would result in animprovement in terms of decreasing the prevalence of child sexual abuse through prevention, and enhanced support for victims of child sexual abuse through a holistic multi-stakeholder approach. It would also relieve Europol from the burden of having to assume all the tasks, allowing it to focus on the strictly operational elements of facilitating the detection, verification and investigation of child sexual abuse. This would reduce the pressure on Europol as an organisation and also reduce – but not eliminate – the associated risk of the task's getting deprioritised among Europol's many competing important objectives.

Dividing the tasks of the centre between two entities could limit its overall impact by creating and additional burden of coordination and a potential for inefficiencies. For example, charging one entity with the operational aspects of the centre's tasks and another one with ensuring transparency and accountability of the process would be highly complex an ineffective. Therefore, the part of centre under another organisation would solely focus on prevention and assistance to victims, without playing any role in the detection, reporting and removal process. This would severely limit this choice's impact in terms of ensuring accountability and transparency.

If given additional specialised resources, Europol would be well-suited to cover law enforcement support aspects of the Centre's work, and to perform the coordination roles; at the same time, a significant effort would be needed to ensure cohesion between the activities in all strands of work, which may run counter to the objective of establishing a centre which acts as a hub/one-stop-shop. A centre split between two entities would risk not having the same public impact as an dedicated and unified body, where the leadership of the organisation would be solely dedicated to this topic and could focus on the precise tasks of the centre, as well as on positioning the centre in the maze of relevant stakeholders within the EU and beyond. Other concerns relate to the ability to coordinate between the two separate bodies; the risk of the task's being deprioritised in a large

organisation with many important tasks; and the fact that transparency reporting and accountability measures based in an agency with a law enforcement mandate may not be perceived as being sufficiently independent.

The impact of the centre's work in assisting victims in removing images and videos related to their abuse from the internet would be positive, similarly to option A.

The overall societal impact of this choice is deemed to be moderately positive, as it would improve the security of EU citizens, contribute to the prevention, investigation and prosecution of child sexual abuse crimes, and to the well-being of victims of child sexual abuse.

Choice D: Set up an EU centre to prevent and counter child sexual abuse within the Fundamental Rights Agency (FRA)

In this choice, provided that FRA is given a legal basis that can cover all of the centre's function, the centre would contribute to improved processing of reports, likely leading to an increase in removals, in investigations and eventually also in identifying and rescuing victims. This would have a positive impact on society.

The focus of FRA on fundamental rights could reinforce the recognition of independence, which is key to ensure transparency and accountability of companies' efforts to detect CSA online and of the outcome of the follow up of the reports by law enforcement. This would help gain trust and buy-in from key stakeholders, which is necessary for the success of the centre's actions.

Similarly to choice A, this choice would offer the possibility to carry out all relevant functions in the same place (contribute to the detection of CSA online, support victims and facilitate prevention) and liaise with all relevant stakeholder groups.

However, to effectively work with all relevant stakeholders, new structures and networks would have to be established. While the main task of FRA include also strengthening cooperation between fundamental rights actors, its main focus is helping policy makers by collecting and analysing data and providing independent advice. The main focus of the EU centre to prevent and counter child sexual abuse is to become a practical knowledge and coordination hub; input for policy purposes would be an important but secondary role. The EU centre is expected to support practitioners from all relevant backgrounds in an operational manner, from education to law enforcement. This includes e.g. collecting information on effectiveness of programmes for offenders. While there is a link to protecting fundamental rights, the main focus would need to be on practical and scientific expertise about the subject in an operational perspective. Addressing the needs of this stakeholder group on a regular basis would require a significant shift in the set-up of the agency. The expertise currently available in FRA would have to be expanded to cover other issues linked specifically to child sexual abuse, for example in the area of prevention of offences. Similarly, the cooperation with Europol and national law enforcement would have to be created anew.

Being part of larger entity could also limit the ability of the centre to dispose of its own resources and dedicate them exclusively to the fight against child sexual abuse, as it could be constrained by other needs and priorities of the larger entity. It may also limit the visibility of the centre, as child sexual abuse is only one of the many tasks FRA deals with. The risk of locating the centre in FRA is therefore that it will be overshadowed by

activities to tackle other types of crime, both internally and externally, limiting the overall impact the centre would have.

If the operational functions were assigned to another entity, namely Europol, once more, the disadvantages of close cooperation with law enforcement that would be required to fulfil its tasks might call into question its overall status as an independent provider of impartial advice and expertise on all fundamental rights. (See section 3.4 for a more detailed discussion on the possibility to embed the EU centre in Europol and another organisation).

In summary, this implementation choice would improve the ability of relevant public authorities to respond to cases of online child sexual abuse, leading to more victims being rescued and more cases of crime prevented. A possible limitation of the positive impact of this option would be the necessity to shift the role of the existing agency and build up new networks among relevant stakehodlers, including law enforcement.

Economic impact

The assessment of the economic impact focuses mostly on the costs which would be incurred if there is a decision to establish a Centre, both for its creation and for carrying out its duties on an ongoing basis. However, it is important to note that the costs incurred by establishing the Centre would be accompanied by benefits in terms of limiting the societal cost of child sexual abuse. Economic costs include those of police and judicial services (e.g. criminal prosecution, correctional system), social services, victim support services (e.g. community organisations), victim compensation programmes, education, health, and employment costs.

Choice A: Set up an EU Centre on prevention and assistance to victims

Compared to the baseline scenario, the practical measures to set up a Centre as a hub of knowledge and information would enhance coordination in the areas of prevention and assistance to victims. This would have a positive impact on the Member States, which could reduce duplication and improve effectiveness by making use of existing research and best practices established in other countries. This, in turn, would allow for more efficient use of financial resources to build further on existing research and experience and implement initiatives on a more widespread and evidence-based basis.

The cost of supporting the centre in this form, including its activities with networks of experts and practitioners, actions to increase capacity and exchange good practices, could be covered under the Internal Security Fund. The economic impact of these actions is deemed to be limited.

Such practical measures could be accompanied by increased funding through relevant programmes (e.g. ISF, Horizon Europe), adding additional costs to the EU budget. Improved coordination between relevant authorities of Member States and other stakeholders would help to ensure that EU funds are used to the benefit of a broad range of actors and therefore bring real value.

The centre could also stimulate efficient uptake of EU funds through coordination and better information sharing, which would have a positive impact on the Member States (which would be able to streamline EU funding to priority areas) and the EU budget

(better use of EU funding, e.g. avoiding supplication of parallel projects in the same area).

Choice B: Set up an EU Centre to prevent and counter child sexual abuse as an independent EU body

Establishing the EU centre as a new independent EU body would require higher initial expenses. However, compared to choice B, as all the activities of the centre would be a part of one organisation, this choice would allow minimising administrative costs by avoiding duplicate structures. When setting up a new EU body, there is also room for some degree of budget diversification, allowing funding from Member States, and potentially private entities (NGOs, such as foundations and charities, industry) under strict conditions to preserve the independence of the centre. This could alleviate the strain on the EU budget.

On the other hand, a more efficient and coordinated system of handling the reports would likely lead to a net reduction of costs and necessary resources for each report for both service providers and law enforcement authorities. In addition, the existence of a reliable set of indicators of what is illegal in the EU and its Member States, as well as the access to reliable technologies free-of-charge should create efficiencies, as service providers can rely on independently verified information for the whole of the Single Market. Furthermore, the reduction of reporting channels in the EU would reduce costs of potentially needing to comply with several different national framework.

The centre could also stimulate efficient uptake of EU funds through coordination and better information sharing, which would have a positive impact on the Member States (which would be able to streamline EU funding to priority areas) and the EU budget (better use of EU funding, e.g. avoiding supplication of parallel projects in the same area).

The centre's activities could reduce duplication of efforts to combat CSA, leading to cost saving in the long-term, and serve to reduce the long-term societal and economic impact of these crimes. The positive impact for Choice A is expected to be somewhat greater than that of the other analysed choices, as this option would relieve law enforcement of all tasks that can be accomplished elsewhere and at the same time would provide an independent counterpart to service providers.

Overall, setting up a completely new entity would incur significant costs in the beginning. However, these initially high costs have to be viewed against the cost savings the centre would trigger, namely limiting the risk of duplicating efforts and streamlining of activities in an economic manner. Moreover, the centre's contribution to the fight against child sexual abuse would lead to **decreasing the economic costs of this crime in the long run**.

Choice C: Set up an EU Centre to prevent and counter child sexual abuse with some functions in Europol and others in a separate organisation under Member State law

As in implementation choice B, this choice would require increased funding for Europol, at somewhat lesser levels than choice B. Additionally, under this implementation choice a new organisation would be created with responsibility for parts of the functions of an

EU centre. While it would to a large extent be funded by the EU, the new entity could also receive funding from additional sources. This additional funding could include:

- contributions from the Member States and third countries,
- contributions from industry,
- contributions from not-for-profit organisations and charities.

Initially, the Centre would likely be funded entirely, or almost entirely, by the EU. With time, this proportion could change. In a comparable example, approximately 60% of the budget of NCMEC is provided by the US government.

The drawback of this choice is that splitting the centre among two organisations could lead to duplication of services providing administrative and logistic support (with each organisation having its own financial, human resources and communication units, for example), ultimately leading to higher costs.

In terms of the economic impact on service providers and on society as a whole, the same considerations as for Choice A apply to a large extent. There may be a positive economic impact on society as a whole of the prevention measures targeting potential offenders, which may be more effectively supported by a centre that is independent of law enforcement.

In short, despite the costs associated with creating and running the centre, the effect it would have on the fight against child sexual abuse would lead to a **positive** economic impact on society though decreasing the economic costs of this crime in the long run.

Choice D: Set up an EU Centre to prevent and counter child sexual abuse within the Fundamental Rights Agency (FRA)

Embedding the centre within FRA would require an increase in its funding to provide for the cost of additional activities, including increasing staff numbers to handle the workload related to all functions of the centre.

With regard to detection, setting up and maintaining the infrastructure for the database (both hardware and software) would incur significant one-time costs, as well as more limited running costs. While, the **annual and initial costs** may be lower than creating a new body, they would still be substantial. e.g. to find, hire and train a number of dedicated non-law enforcement experts, and to carry out the centre functions (including manually reviewing the reports from companies to filter false positives, determining the jurisdiction best placed to act).

With regard to the actions on prevention and support to victims, the costs incurred would be higher compared to the baseline, and comparable to choice A and B (e.g. supporting Member States on prevention and assistance to victims would require expertise that is not currently present in FRA).

In all areas, the centre's work could reduce duplication of efforts to fight CSA, leading to cost savings in the long-term. The actions proposed in this choice would also contribute to reducing the economic impact of child sexual abuse on society in general through reductions in crime as a result of the centre's functions in support of law enforcement and service providers.

In short, similarly to previous options, the potential for **decreasing the economic costs of this crime** in the long run is high and counterbalances the costs associated with creating and running the centre.

Fundamental Rights impact

This section examines the impact of establishing a European Centre to prevent and counter child sexual abuse on fundamental rights as laid down in the Charter of Fundamental Rights of the European Union. Children, users of the services at issue and providers of such services were identified as relevant right holders for the centre:

1. **Rights of the children:** fundamental rights to human dignity and to the integrity of the person, the prohibition of inhuman or degrading treatment, rights to respect for private and family life and to protection of personal data, as well as the rights of the child.[588]
2. **Rights of the users whose data is accessed:** the rights to respect for privacy (including of communications, as part of the broader right to respect for private and family life), to protection of personal data and to freedom of expression and information.[589]
3. **Rights of the service providers**: the freedom to conduct a business.[590]

Overall, none of the options considered for the centre would have any significant negative impact on any fundamental right. Rather, one can observe a strengthening of protection of specific fundamental rights – such as the rights of the child and the rights of all users to data protection – in line with the importance of the role of the centre in providing legal certainty about what is illegal content, in facilitating swift analysis and processing of reports, in improving prevention and victim assistance, and in ensuring accountability and transparency. The analysis shows that the Centre's own impact is limited from a fundamental rights perspective, but that it serves as an important safeguard to ensure that the measures strike a fair balance between the different rights at stake.

Choice A: Set up an EU Centre on prevention and assistance to victims

A limited positive impact on fundamental rights may be expected from better coordination of efforts on prevention and assistance to victims of child sexual abuse. Under this choice, there would be no improvement with regard to the rights of victims of ongoing abuse in need of rescue, and those who wish to have their images removed from the internet. The rights of the persons affected by CSAM detection measures implemented by service providers would remain as in the baseline.

Overall, the analysis suggest that this choice would serve to minimally improve the protection of fundamental rights.

---

588 Art. 1, 3, 4, 7, 8 and 24 of the Charter, respectively.
589 Art. 7, 8 and 11 of the Charter, respectively.
590 Art. 16 of the Charter.

Choice B: Set up an EU Centre to prevent and counter child sexual abuse as an independent EU body

This option would contribute to improved processing of reports, likely leading to an increase in removals, in investigations and eventually also in identifying and rescuing victims. This could have a significant positive impact on the fundamental rights of victims of ongoing abuse. The establishment of an EU database would also facilitate prevention by stopping crimes from happening in cases where imminent abuse (grooming) is detected, positively impacting the rights of people who may become victims of child sexual abuse.

The benefit of this options would be improved coordination of efforts in relation to overall prevention and assistance to victims of child sexual abuse, leading to positive impact on the fundamental rights of persons who are or may become victims of crime.

The centre would serve as a safeguard in the process of detection and reporting of CSA online. In case of potential false positives, companies would not be reporting innocent persons to law enforcement directly. The creation of transparency and accountability processes, which depend on the centre, serves as a safeguard to mitigate the impact on fundamental rights of users resulting from a detection obligation. Similarly, the creation of a single database of reliable indicators and facilitation of access to reliable technology via a centre can mitigate the impact on the freedom of the provider to conduct a business and contribute to balancing the impact on the fundamental rights of users by supporting service providers in improving the accuracy of their technologies. Overall, a positive impact on fundamental rights may be expected with respect to the relevant fundamental rights of all three categories set out above.

Choice C: Set up an EU Centre to prevent and counter child sexual abuse with some functions in Europol and others in a separate organisation under Member State law

The impacts of this option with regard to improving investigations and rescuing victims are as in option A.

In this choice, the part of centre under an independent organisation would solely focus on prevention and assistance to victims, without playing any role in the detection, reporting and removal process. This could potentially limit the positive impact on fundamental rights, and the centre's effectiveness as a safeguard ensuring transparency.

Overall, a moderate positive impact on fundamental rights of all groups affected is to be expected.

Choice D: Set up an EU Centre to prevent and counter child sexual abuse within the Fundamental Rights Agency (FRA)

The impact of this choice is expected to be positive, as in choice A. The expertise of FRA in the field of fundamental rights would be an additional benefit.

With regard to ensuring **transparency and accountability** of efforts around combating child sexual abuse, while FRA focuses on ensuring the fundamental rights of citizens in policy making, it **does not intervene in individual cases**. It has not previously engaged

in overseeing the efforts of industry, including overseeing the development and implementation of technologies. Including these functions into FRA would **contribute to the shift of the agency's structure** and change its role from an independent and neutral observer into an actor in the field.

3.6. Quantitative assessment

Costs

The quantification of the costs and benefits of the policy measures/policy options is limited by the **lack of data**, and requires the use of a number of **assumptions**:

1. The estimate of recurrent and one off costs related to the functioning of the Centre are based on the budget of EU agencies and other organisation similar in size to what is predicted for the Centre:

Name	Staff (approx.)	Budget (approximately)	Funding sources
Fundamental Rights Agency (FRA)	105	24,3 MEUR/year	EU budget
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	100	19 M EUR/year	EU budget
The European Union Agency for Law Enforcement Training (CEPOL)	40	30 M EUR/year	10 M EUR EU subsidy, other sources of funding include EU project funding
European Institute for Gender Equality (EIGE),	40	8 M EUR/year	EU budget
US National Center for Missing and Exploited Children (NCMEC)	300	15 M EUR/year[591]	US government funding and voluntary donations
Canadian Centre for Child Protection	45	4 M EUR/year.	Supported by the Canadian government and private donors

2. The cost estimates make the following assumptions:
   Staff costs
   - Detection, reporting and removal:
     - The **same number of staff** would be required to analyse the estimated surge in reports (x8 compared to 2020) **in all options**.
     - Europol currently has dedicated staff from law enforcement to cross-match and enrich the reports. This staff will **not be able to be repurposed** to contribute to the tasks of reviewing the reports to ensure that they are actionable that the EU centre would carry out.

[591] NCMEC, 2019 Annual Report, when costs relating to missing child case management/information and case analysis are excluded.

- The staff costs for admin staff in charge of **overheads** (HR, accounting, management) would be lower in the Europol+ and FRA options, given the **existing set ups**.

o Prevention and assistance to victims:
  - **Non-EU staff** (28 posts) could be envisaged for these functions **across all options.** They could be funded by a grant to a separate organisation (NGO, Foundation) selected via a call for proposals instead, so that there is no impact on the future EU budget (e.g. pensions, etc).
  - The operational staff would be the **same in all options**, as these would be **new functions** in all cases.
  - The staff costs for admin staff in charge of overheads (HR, accounting, management) would be **lowest for FRA**, as it could benefit from economies of scale in the existing setup and with the detection, reporting and removal function.
  - The staff corresponding to the prevention and assistance to victims functions in all options could be non-EU staff and be covered by a **call for proposals/grant**, and would not have impact on the future EU budget (e.g. pensions, etc).

Infrastructure
- Initial costs are estimated at 3 MEUR to set up the databases of indicators, and 1 – 2 MEUR relating to the selection and fitting out of its premises where necessary.
- Annual costs: include notably the costs of running and maintaining the databases of indicators.

Operational expenditure:
- It includes the costs from carrying out the facilitation of detection, reporting and removal (support to companies and law enforcement), as well as the support to Member States on prevention and assistance to victims (e.g. studies, etc).
- The centre would not have its own research budget for prevention and assistance to victims. This would be provided through calls for proposals through funds like Horizon Europe.

3. The estimate assumes that the centre would take about two years to become operational and up to four years to reach its full size and operational capacity. Therefore the costs related to personnel and logistics are projected to increase gradually in the first years, reaching a stable level after year 4. Some other costs, such as expenditure related to staff recruitment and training may be higher in the early stages of setting up the centre. The continuous costs estimates refer to the situation in which the Centre is fully operational.

4. The one off and recurring costs related to the creation of an EU database of hashes of known CSAM are based on a Commission study[592].

The estimates in this section provide an idea of the order of magnitude of costs and benefits and therefore should not be taken as exact forecasts.

The following sections discuss the cost estimates for each of the implementation choices.

Choice A: Set up an EU Centre on prevention and assistance to victims

This choice assumes the creation of a centre through non-legislative measures.

The cost of non-legislative measures, namely creating a centre as a hub without a legal personality is estimated based on assumption that it would take 4 full-time equivalent units in the Commission to coordinate the hub. The cost of 1 FTE is based on the following assumptions:

- the average of the salaries in the EU of whose activities are classified under Section O (public administration) in the NACE Rev. 2 statistical classification of economic activities in the European Community[593].
- This cost includes compensation of employees, plus taxes, minus subsidies;
- An additional 25% is added to account for overheads (i.e. expenses not related to direct labour, such as the cost of office equipment.)
- The value is 38.50 EUR/hour

FTEs	Salary	Annual cost
4	38.50 EUR/hour	320 286 EUR

The operational activities of the hub could be supported by a framework contract of estimated value 10 M EUR/ year. This estimate is based on existing framework contacts, such as the one supporting the Radicalisation Awareness Network[594]. The specific tasks to be carried out by the hub would be specified in the framework contract.

These tasks could include the development of activities and good practices by networks of practitioners, policy makers and researchers. The cost of this task is estimated at 3M EUR/year, or 30% of the contract value. Administrative, logistical and technical support for the work of the hub is also expected to represent a significant cost due to the

[592] Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues, 2021, p.67

[593] Eurostat, NACE Rev. 2 - Statistical classification of economic activities, accessed 27 April 2021.

[594] The annual costs of RAN are 7,5 MEUR for the practitioners network and 7,5MEUR/year for the policy support network. They are implemented through two framework contracts of 30MEUR each for 4 years. See for example European Commission, Technical Support to Prevent and Counter Radicalisation, accessed 21 May 2021.

hub's highly decentralised nature. These costs, which would cover the organisation and reporting on events such as study visits and working groups, are also estimated at 3M EUR/year.

Facilitation of coordination and research activities could be another significant task for the hub, however due to the maximum duration of framework contracts of 4 years, the hubs abilities in this regard would be limited to focus on short-term research. The cost for this task is estimated at 1.5M EUR/year, or 15% of the value of the contract.

The hub could also organise cross-cutting thematic events bringing together stakeholders of different types, going beyond the topics of individual working groups. These could include a Steering Committee to provide strategic guidance and evaluation of the hub's overall work. The cost of this task is estimated at 2M EUR/year, 20% of the value of the contract.

Finally, due to the decentralised nature of the hubs operations, the maintenance of an EU website dedicated to the hub's activities is estimated at 5% of the contract value, or 0.5M EUR/year.

Each of the above costs are assumed to be divided evenly between the hubs functions in relation to assistance to victims and prevention. The estimated costs of this choice are summarised in Table2.

The total (continuous) cost of this choice is therefore estimated to be **10.32M EUR/year.** There would not be any **one-off costs**.

Table 2: Estimated costs of Implementation Choice A (EUR millions/year)

	Annual Cost
Support to service providers and public authorities for detection, removal and reporting of child sexual abuse online	
Total	**€0**
Prevention	
Development of activities and good practices	€1.50
Administrative, logistical and technical support	€1.50
Research activities	€0.75
Thematic events	€1.00
Website	€0.25
Total	**€5**
Assistance to Victims	
Development of activities and good practices	€1.50
Administrative, logistical and technical support	€1.50
Research activities	€0.75
Thematic events	€1.00
Website	€0.25
Total	**€5**
Supporting services	
Commission staff costs	€0.32
Total	**€0**
Grand total	**€10.32**

Choice B: Set up an EU Centre to prevent and counter child sexual abuse as an independent EU body

This choice assumes the creation of a Centre as a new EU body (i.e. decentralised agency) which would perform all of the roles considered in this Annex.

The Centre as an EU agency would incur on **initial costs of a total of EUR 5 million**: EUR 3 million to set up the databases of indicators + EUR 2 million for the building.

The costs of establishing databases of indicators of child sexual abuse online are based upon a Commission study and bilateral consultations with operators of similar databases[595].

This choice estimates an **annual cost** of **EUR 25.7 million per year** after the initial ramp-up.

The cost estimates for this choice (as well as choices C and D) are based on cost structures of similar organisations in the EU (FRA, EMCDDA, etc) and similar Centres around the world (e.g. NCMEC[596],)[597]. The costs estimates include the costs of reviewing manually all the reports submitted. Cost estimates relating to the Centre's functions in the areas of prevention and victim support are also informed by the costs of NCMEC's activities in the areas of community outreach and training, which respectively develop and disseminate prevention materials and provide training to relevant professionals.

The following table gives an overview of all the costs to cover all the functions of the Centre: prevention, assistance to victims and facilitation of the process to detect, report and remove CSA online:

[595] Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues, 2021, p.67

[596] See in particular National Center for Missing and Exploited Children, 2019 Audit Report, 31 December 2018 and 2019.

[597] Staff costs include staff wellbeing programmes, in line with best practices in other serious crime areas such as terrorism (see for example here and here). For reference, these programmes represent 15% of staff costs in the Internet Watch Foundation.

Table 3: Estimated costs of Implementation Choice B

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	€3.000.000	€5.000.000	€10.000.000	€13.000.000	€15.000.000	€15.000.000	€15.000.000	€15.000.000	€15.000.000	€15.000.000
Expenditure relating to Staff recruitment	€600.000	€600.000	€600.000	€200.000	€50.000	€50.000	€50.000	€50.000	€50.000	€50.000
Mission expenses	€300.000	€300.000	€300.000	€500.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000
Socio-medical infrastructure & training	€150.000	€200.000	€200.000	€200.000	€250.000	€250.000	€250.000	€250.000	€250.000	€250.000
Total staff costs	**€4.050.000**	**€6.100.000**	**€11.100.000**	**€13.900.000**	**€15.900.000**	**€15.900.000**	**€15.900.000**	**€15.900.000**	**€15.900.000**	**€15.900.000**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000
ICT (not related to database)	€800.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000
Databases of indicators										
• Technical maintenance	€0	€200.000	€300.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
• Allowance for annual hardware licensing	€50.000	€50.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
• Annual hosting for databases	€50.000	€100.000	€150.000	€200.000	€300.000	€300.000	€300.000	€300.000	€300.000	€300.000
Movable property and associated costs	€30.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Current administrative expenditure	€50.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Audits	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Total infrastructure costs	**€2.380.000**	**€2.550.000**	**€2.790.000**	**€2.960.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	€500.000	€1.000.000	€1.500.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000
Support to expert networks (coordination activities, meetings)	€500.000	€1.000.000	€1.500.000	€2.000.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000
Translation and interpretation	€300.000	€300.000	€400.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Publishing and research dissemination	€50.000	€150.000	€200.000	€300.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Communication (incl. campaigns)	€500.000	€600.000	€700.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000
Total operational expenditure	**€1.850.000**	**€3.050.000**	**€4.300.000**	**€5.700.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**
TOTAL EXPENDITURE	**€8.280.000**	**€11.700.000**	**€18.190.000**	**€22.560.000**	**€25.700.000**	**€25.700.000**	**€25.700.000**	**€25.700.000**	**€25.700.000**	**€25.700.000**

Choice C: Set up an EU Centre to prevent and counter child sexual abuse with some functions in Europol and others in a separate organisation under Member State law

This scenario assumes the creation of a centre with some roles performed by Europol, and some by a separate organisation established under Member State law.

Europol would carry out the tasks of facilitating the detection, reporting and removal of CSA online. The independent organisation would carry out the tasks of facilitating Member States' action on prevention and assistance to victims.

Costs relating to central administration providing supporting services to the prevention and assistance to victims functions are expected to be higher under this implementation choice. These increases are due to the creation of a new, independent organisation, which will be unable to benefit from the existing structures and resources of Europol.

The costs estimates include the costs of reviewing manually all the reports submitted.

The Centre in this form would incur on **initial costs** of a total of **EUR 5 million**:

- EUR 4 million under Europol (EUR 3 million to set up the databases of indicators + EUR 1 million for the building); and
- EUR 1 million under the independent organisation (building).

This choice estimates an **annual cost** of **EUR 24.1 million per year** after the initial ramp-up.

The following table gives an overview of all the costs to cover all the functions of the Centre: prevention, assistance to victims and facilitation of the process to detect, report and remove CSA online:

Table 4: Estimated costs of Implementation Choice C (Europol component)

EUROPOL	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	€3.000.000	€5.000.000	€6.000.000	€7.000.000	€8.000.000	€9.700.000	€9.700.000	€9.700.000	€9.700.000	€9.700.000
Expenditure relating to Staff recruitment	€400.000	€400.000	€400.000	€200.000	€50.000	€50.000	€50.000	€50.000	€50.000	€50.000
Mission expenses	€300.000	€300.000	€300.000	€500.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000
Socio-medical infrastructure & training	€150.000	€200.000	€200.000	€200.000	€250.000	€250.000	€250.000	€250.000	€250.000	€250.000
Total staff costs	**€3.850.000**	**€5.900.000**	**€6.900.000**	**€7.900.000**	**€8.900.000**	**€10.600.000**	**€10.600.000**	**€10.600.000**	**€10.600.000**	**€10.600.000**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
ICT (not related to database)	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000
Databases of indicators										
• Technical maintenance	€0	€200.000	€300.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
• Allowance for annual hardware licensing	€50.000	€50.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
• Annual hosting for databases	€50.000	€100.000	€150.000	€200.000	€300.000	€300.000	€300.000	€300.000	€300.000	€300.000
Movable property and associated costs	€30.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Current administrative expenditure	€50.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Audits	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000
Total infrastructure costs	**€1.480.000**	**€1.750.000**	**€1.990.000**	**€2.160.000**	**€2.400.000**	**€2.400.000**	**€2.400.000**	**€2.400.000**	**€2.400.000**	**€2.400.000**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	€50.000	€100.000	€100.000	€200.000	€200.000	€500.000	€500.000	€500.000	€500.000	€500.000
Support to expert networks (coordination activities, meetings)	€50.000	€50.000	€50.000	€70.000	€70.000	€100.000	€100.000	€100.000	€100.000	€100.000
Translation and interpretation	€50.000	€80.000	€100.000	€200.000	€300.000	€400.000	€400.000	€400.000	€400.000	€400.000
Publishing and research dissemination	€50.000	€150.000	€200.000	€300.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Communication (incl. campaigns)	€500.000	€600.000	€700.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000
Total operational expenditure	**€700.000**	**€980.000**	**€1.150.000**	**€1.770.000**	**€2.070.000**	**€2.500.000**	**€2.500.000**	**€2.500.000**	**€2.500.000**	**€2.500.000**
TOTAL EXPENDITURE	**€6.030.000**	**€8.630.000**	**€10.040.000**	**€11.830.000**	**€13.370.000**	**€15.500.000**	**€15.500.000**	**€15.500.000**	**€15.500.000**	**€15.500.000**

Table 5: Estimated costs of Implementation Choice C (separate entity component)

Separate entity	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	€1.000.000	€2.000.000	€3.000.000	€3.500.000	€3.500.000	€3.500.000	€3.500.000	€3.500.000	€3.500.000	€3.500.000
Expenditure relating to Staff recruitment	€200.000	€200.000	€150.000	€100.000	€50.000	€50.000	€50.000	€50.000	€50.000	€50.000
Mission expenses	€50.000	€50.000	€100.000	€150.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000
Socio-medical infrastructure & training	€50.000	€100.000	€100.000	€100.000	€150.000	€150.000	€150.000	€150.000	€150.000	€150.000
Total staff costs	**€1.300.000**	**€2.350.000**	**€3.350.000**	**€3.850.000**	**€3.900.000**	**€3.900.000**	**€3.900.000**	**€3.900.000**	**€3.900.000**	**€3.900.000**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	€400.000	€400.000	€400.000	€400.000	€400.000	€400.000	€400.000	€400.000	€400.000	€400.000
ICT (not related to database)	€50.000	€50.000	€50.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Databases of indicators										
• Technical maintenance	€0	€0	€0	€0	€0	€0	€0	€0	€0	€0
• Allowance for annual hardware licensing	€0	€0	€0	€0	€0	€0	€0	€0	€0	€0
• Annual hosting for databases	€0	€0	€0	€0	€0	€0	€0	€0	€0	€0
Movable property and associated costs	€30.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Current administrative expenditure	€50.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Audits	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Total infrastructure costs	**€1.030.000**	**€1.050.000**	**€1.090.000**	**€1.160.000**	**€1.200.000**	**€1.200.000**	**€1.200.000**	**€1.200.000**	**€1.200.000**	**€1.200.000**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	€150.000	€150.000	€200.000	€200.000	€300.000	€300.000	€300.000	€300.000	€300.000	€300.000
Support to expert networks (coordination activities, meetings)	€500.000	€1.000.000	€1.500.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000
Translation and interpretation	€300.000	€300.000	€400.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Publishing and research dissemination	€50.000	€150.000	€200.000	€300.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Communication (incl. campaigns)	€50.000	€100.000	€100.000	€150.000	€200.000	€200.000	€200.000	€200.000	€200.000	€200.000
Total operational expenditure	**€1.050.000**	**€1.700.000**	**€2.400.000**	**€3.050.000**	**€3.500.000**	**€3.500.000**	**€3.500.000**	**€3.500.000**	**€3.500.000**	**€3.500.000**
TOTAL EXPENDITURE	**€3.380.000**	**€5.100.000**	**€6.840.000**	**€8.060.000**	**€8.600.000**	**€8.600.000**	**€8.600.000**	**€8.600.000**	**€8.600.000**	**€8.600.000**

Choice D: Set up an EU Centre to prevent and counter child sexual abuse within the Fundamental Rights Agency (FRA)

This scenario assumes the creation of a Centre fully integrated in the Fundamental Rights Agency. The Centre would carry out all the functions envisaged on prevention, assistance to victims, and facilitation of detection, reporting and removal of CSA online.

The costs estimates include the costs of reviewing manually all the reports submitted.

The Centre in this form would incur on **initial costs** of a total of **EUR 4 million**: EUR 3 million to set up the databases of indicators + EUR 1 million for the building.

This choice estimates an **annual cost** of **EUR 23.7 million per year** after the initial ramp-up.

Table 6: Estimated costs of Implementation Choice D (Centre under FRA)

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	€3.000.000	€5.000.000	€10.000.000	€11.000.000	€13.000.000	€13.000.000	€13.000.000	€13.000.000	€13.000.000	€13.000.000
Expenditure relating to Staff recruitment	€600.000	€600.000	€600.000	€200.000	€50.000	€50.000	€50.000	€50.000	€50.000	€50.000
Mission expenses	€300.000	€300.000	€300.000	€500.000	€600.000	€600.000	€600.000	€600.000	€600.000	€600.000
Socio-medical infrastructure & training	€150.000	€200.000	€200.000	€200.000	€250.000	€250.000	€250.000	€250.000	€250.000	€250.000
Total staff costs	**€4.050.000**	**€6.100.000**	**€11.100.000**	**€11.900.000**	**€13.900.000**	**€13.900.000**	**€13.900.000**	**€13.900.000**	**€13.900.000**	**€13.900.000**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000	€900.000
ICT (not related to database)	€800.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000	€700.000
Databases of indicators										
• Technical maintenance	€0	€200.000	€300.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
• Allowance for annual hardware licensing	€50.000	€50.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
• Annual hosting for databases	€50.000	€100.000	€150.000	€200.000	€300.000	€300.000	€300.000	€300.000	€300.000	€300.000
Movable property and associated costs	€30.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Current administrative expenditure	€50.000	€50.000	€70.000	€80.000	€100.000	€100.000	€100.000	€100.000	€100.000	€100.000
Audits	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Total infrastructure costs	**€2.380.000**	**€2.550.000**	**€2.790.000**	**€2.960.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**	**€3.200.000**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	€500.000	€1.000.000	€1.500.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000	€2.000.000
Support to expert networks (coordination activities, meetings)	€500.000	€1.000.000	€1.500.000	€2.000.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000	€2.600.000
Translation and interpretation	€300.000	€300.000	€400.000	€400.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Publishing and research dissemination	€50.000	€150.000	€200.000	€300.000	€500.000	€500.000	€500.000	€500.000	€500.000	€500.000
Communication (incl. campaigns)	€500.000	€600.000	€700.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000	€1.000.000
Total operational expenditure	**€1.850.000**	**€3.050.000**	**€4.300.000**	**€5.700.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**	**€6.600.000**
TOTAL EXPENDITURE	**€8.280.000**	**€11.700.000**	**€18.190.000**	**€20.560.000**	**€23.700.000**	**€23.700.000**	**€23.700.000**	**€23.700.000**	**€23.700.000**	**€23.700.000**

Benefits

The quantification of benefits is based on the estimated reduction of CSA crimes that could be attributed to the functions carried out by the Centre.

The **EU Centre** will **facilitate** action of Member States and service providers in preventing and combating CSA, and support victims. This will generate **cost savings**, by, e.g. helping **avoid duplication of efforts** and facilitating a more effective and efficient use of resources. In addition, the Centre's tasks would contribute to a reduction of the prevalence of CSA, and therefore cost savings caused by those crimes.

It is not possible to quantify **exactly** what those benefits would be. In particular, it is not possible to isolate precisely the effects of the Centre from the effects of the other policy measures, in particular the obligations on service providers to detect, report and remove CSA online. This section focuses therefore on **estimating** those benefits as a reduction of the annual costs of CSA in the EU that could be attributed to the Centre **only**.

To estimate how each implementation choice could reduce crime, the **qualitative scores** on the social impact (enhanced security through more effective fight against crime, prevention leading to decreased prevalence of CSA) obtained in the assessment of each implementation choice were **translated into percentages of decrease of child sexual abuse crimes**.

The social impacts of the various implementation options for the centre are determined based on how effectively they would enhance security by helping increase the capacity to detect, report and remove child sexual abuse online, prevent these crimes, and increase the assistance to victims.
This assumption was used for the **sole purpose of comparing the options**. Therefore, the total value of benefits derived from a reduction of crime for a given implementation must be interpreted in relation to the other options, **rather than as an accurate estimate** of the actual reduction of crime that a given policy option would cause.

See the quantitative comparison of benefits below for an estimates of the benefits based on the effectiveness ratings.

5. COMPARISON OF IMPLEMENTATION CHOICES

Qualitative comparison

The following criteria are used in assessing how the implementation choices would potentially perform, compared to the baseline:

- **Effectiveness** in achieving the specific objectives:
  a) **Help** ensure that victims are rescued and assisted as soon as possible and offenders are brought to justice by **facilitating detection, reporting and removal** of CSA online.
  b) **Support Member States** in putting in place usable, rigorously evaluated and effective **prevention** measures to decrease the prevalence of child sexual abuse in the EU.
  c) **Support Member States** to ensure that **victims** have access to **appropriate and holistic support**, by **facilitating** efforts at EU level.

- **Efficiency**: cost-benefits assessment of each policy option in achieving the specific objectives, including financial and administrative costs.
- **Coherence** with relevant initiatives at national, EU and international level, using all the relevant policy instruments (legislation, coordination and funding):

The tables below summarise the qualitative scores for each main assessment criteria and each option. The options are compared below through listing positive (+), negative (-) and 'no-change' (~) impacts compared to the baseline (with > indicating more costs in relation to baseline).

Table 7: qualitative comparison of implementation choices for the Centre

Criteria		A	B	C	D
Effectiveness		+	+++	++	++
Efficiency	Costs	>	>>>	>>>	>>>
	Benefits	+	+++	++	++
Coherence		+	++	+	++

Effectiveness

This criterion, closely linked to the social impact, concerns how effectively the various implementation choices would achieve the specific objectives, including helping increase the capacity to detect, report and remove child sexual abuse online, prevent these crimes, and increase the assistance to victims.

a) **Help** ensure that victims are rescued and assisted as soon as possible and offenders are brought to justice by **facilitating detection, reporting and removal** of CSA online.

Choice A would be the least effective in reaching this objective, as the Centre in this choice would not address the functions of facilitating detection, reporting and removal of CSA online, for which legislation is required.
Choices B, C and D would cover these functions. Under choice C, the Centre could benefit from Europol's expertise in the fight against CSA online, including the existing processes and relationships with stakeholders. On the other hand, its ability to appear as a neutral facilitator of the detection, reporting and removal process may be limited, given that it would be part of law enforcement.
Choices C and D, as EU agencies independent from both service providers and law enforcement, could effectively play that facilitator role.

b) **Support Member States** in putting in place usable, rigorously evaluated and effective **prevention** measures to decrease the prevalence of child sexual abuse in the EU.
The four choices would be able to achieve this objective effectively.

c) **Support Member States** to ensure that **victims** have access to **appropriate and holistic support**, by **facilitating** efforts at EU level.
The four choices would be able to achieve this objective, including by offering the possibility for the centre to support victims who want their images proactively removed from the internet. They would also harness the potential of the network of hotlines to improve support to victims. However, in choice C, this process could be more complicated as the centre would be split between two separate entities. The part of the centre which would be a suitable partner for work with victims, victims' association and hotlines would be an independent entity, which would not be involved in proactive search for CSAM. This separation of the centre roles between two entities increases the risk of silos and therefore the risk of inefficiencies.

Efficiency

Costs

Choice A is the most cost effective, as it covers only part of the envisaged functions for the Centre.

Choices B, C, and D have very similar costs, both one-off and continuous. For one-off cost, the difference between the most expensive and the cheapest option is EUR 1 million. For continuous costs, the difference between the most expensive and the cheapest option is EUR 2 million. Whereas there are some savings by using an existing entity (e.g. Europol, FRA), these are offset by the need to build new functions, notably on prevention and assistance to victims, or expand on similar ones, like Europol's capacity to support detection, reporting and removal of CSA online.

Benefits

As discussed earlier, the main benefits are those linked to a reduction of CSA crimes, and therefore costs caused by its negative consequences on victims and society. This is directly correlated with the efficiency of each choice. Therefore, the ratings for benefits are the same as those for efficiency.

Coherence

Legislation

All choices would be coherent with existing and planned legislation at EU level relevant for the fight against CSA. In particular, the Centre in all the implementation choices would support Member States on the implementation of the prevention and assistance provisions of the CSA Directive, as well as the relevant ones from the Victims' Rights Directive. The Centre under all the implementation choices would also facilitate compliance with the future Digital Services Act, in relation to the provisions relevant to CSA online, notably the notice and takedown requirements.

Coordination

The main role of the Centre is to facilitate the efforts of both Member States and service providers in preventing CSA, assisting victims, and detecting, reporting and removing CSA online. All the choices allow the Centre to fulfil that role in a way that would ensure coherence with existing coordination mechanisms at national and EU level. In choice C, the ability of the Centre to ensure coherence with existing initiatives could be somewhat limited by its separation into two different entities, which could cause inefficiencies in coordination within the Centre itself.

Funding

The Centre in all the implementation choices would ensure coherence with existing funding mechanisms, as part of its facilitation efforts.

Quantitative comparison

Overall costs

The tables below summarise the one-off and continuous costs estimates for the retained implementation choices (table 8), and a detailed overview of the choices that require legislation (table 9):

Table 8: one-off and continuous costs for the implementation choices of the Centre (EUR million)

IMPLEMENTATION CHOICE	ONE-OFF COSTS	CONTINUOUS (ANNUAL) COSTS
A	€0	€10.3
B	€5	€25.7
C	€5	€24.1
D	€4	€23.7

Table 9: summary of estimated costs for the choices that require legislation to set up the EU centre

			1. EU body (e.g. agency)	2. Europol + separate entity		3. FRA
				Europol	Separate entity	
Staff (number of people)	Detection, reporting, removal	Operational staff	70	70	N/A	70
		Overheads staff	15	5		5
	Prevention	Operational staff	10	N/A	10	10
		Overheads staff	4		4	2
	Assistance to victims	Operational staff	10		10	10
		Overheads staff	4		4	2
	Total staff (number of people) [598]		**113**	**75**	**28**	**99**
				103		
Staff (MEUR/year)			**15,9**	10,6	3,9	**13,9**
				14,5		
Infrastructure (MEUR/year)		**Initial costs**	5	4	1	4
		Annual costs	3,2	2,4	1,2	3,2
				3,6		
Operational expenditure (MEUR/year)			6,6	2,5	3,5	6,6
				6		
Total annual costs (MEUR)			**25,7**	**15,5**	**8,6**	**23,7**
				24,1		
Total initial costs (MEUR)			**5**	**5**		**4**

[598] 28 posts corresponding to the prevention and assistance to victims functions in all options could be non-EU staff and be covered by a call for proposals/grant. They would therefore not be part of the EU establishment plan and would not have impact on the future EU budget (e.g. pensions, etc).

Overall benefits

Following the rationale described in section 3.2, and taking into account the qualitative scores on effectiveness, a quantitative estimate of the benefits could be the following:

- The qualitative scores range from 0 (baseline) to +3 (choices C and D) (see **Error! Reference source not found.**11 below).
- The qualitative scores range from + to +++. The model assumes that the decrease of crime could be proportional to this rating, as + (3%), ++ (6%) and +++ (9%).
- The total annual cost of CSA in the EU is EUR 13.8 billion.

Table 10: annual estimated benefits for the policy options (EUR billion)

Implementation choices	Qualitative score for social impact	Estimated decrease of crime and its societal costs	Benefits from reduction of child sexual abuse crimes
A	+	3%	€0.41
B	+++	9%	€1.23
C	++	6%	€0.89
D	++	6%	€0.89

Table 11: annual estimated net benefits for the policy options (EUR billion)

	A	B	C	D
Overall costs	€0.103	€0.257	€0.241	€0.237
Overall benefits	€0.41	€1.23	€0.89	€0.89
Total (savings)	(€.307)	(€0.973)	(€0.649)	(€0.653)

Given the limitations caused by the lack of data, the calculation of benefits as a reduction of crime was carried out for the main purpose of comparing the options. In consequence, the total value of benefits must be interpreted in relation to the other options, rather than as an accurate estimate of the actual reduction of crime that the preferred policy option would actually cause. That said, based upon this analysis, implementation choice B would offer the greatest benefits in the form of reduction of crime.

6. PREFERRED IMPLEMENTATION CHOICE

On the basis of the assessment, the identified preferred choice is choice B, which includes:

- the creation of the EU centre in the form of a decentralised EU agency:
  - providing support to the development and dissemination of research and expertise and facilitating coordination on prevention;
  - providing support to the development and dissemination of research and expertise and facilitating coordination on victims' assistance;
  - supporting victims in removing their images and videos from circulation;

- supporting the detection, reporting and removal of CSAM by receiving reports in relation to child sexual abuse from companies, maintaining a database of indicators to detect child sexual abuse online;
- providing a structured oversight role to ensure accountability and transparency on efforts to tackle child sexual abuse online.

Main advantages

Effectively **achieves** the **general and specific objectives**

Choice B would effectively achieve the strategic objectives of the EU intervention. The form of the centre proposed in this choice would bring the best improvements in all envisaged areas of the centre's activity. Effectively, it proposes the **most efficient approach for a coherent and holistic approach** to the problem of CSA in the present and the future.

In terms of **support to law enforcement and industry,** choice B proposes solutions to improve processing of reports of CSA and maintain systematic information on child sexual abuse material at EU level. It allows for a **transparent and independent oversight** of the efforts to combat CSA, and **improvement of cooperation** between public authorities, civil society organisations and service providers, in particular by realising the full potential of hotlines.

Furthermore, it would contribute to **improving dissemination of expertise** and research on prevention and assistance to victims at EU level, ultimately leading to supporting and developing practical initiatives at Member State level. It also accommodates the possibility to **support victims who want their images removed** from the internet, offering a possibility to effectively address the issue of secondary victimisation.

Finally, the advantage of choice B over other options is that it includes **all the services the centre would provide in one organisation**, avoiding creating needs for additional coordination between different institutions which could potentially drive up costs, lead to confusion for external organisations and victims seeking help, and potentially slow down processes.

All in all, choice B offers a possibility to create an EU centre which would have a significant impact on the fight against CSA in the EU. It would become the **main point of reference** for all aspects of this crime in the EU and an accessible contact point for victims. It would also become the **main point of contact** for international cooperation, allowing the EU to join the lead the fight against child sexual abuse.

The centre as an independent organisation would be a good fit for similar organisations around the world working in the area of child protection and victim assistance(e.g. the Canadian Centre for Child Protection), and would be a natural counterpart for cooperation with them.

There are examples showing that this type of organisation is able to perform similar function as those envisaged for the Centre. Both NCMEC in the United States and the Canadian Centre for Child Protection have a similar legal personality (not-for-profit corporation and national charity respectively), and have a proven record of successful and close cooperation with law enforcement while not being a public authority

themselves. Additionally, independent organisations can have advanced technical capability, including database hosting capacity. Some of the world's most important databases of CSAM are hosted within a not-for-profit organisations (e.g. NCMEC, Internet Watch Foundation[599]).

In addition, the creation of a dedicated EU Centre as an EU Agency would send an important message about the dedication of the EU to combating child sexual abuse more effectively. It would place the EU at one level with those leading the fight against child sexual abuse worldwide, which have made the same choice of creating one independent centre. It would also ensure **independence** from all stakeholders, allowing the centre to cooperate with all on the same terms. It would promote **visibility**, and ensure that all resources of the organisation are dedicated to one single objective.

Respects **subsidiarity** and **proportionality**

Subsidiarity: Choice B offers the **highest added value of EU action**. In particular, it facilitates Member States' action, enables the exchange of best practices and reduces dependence and increases cooperation with third countries. It addresses the fragmentation and inefficiencies of cooperation between law enforcement, public authorities, private sector and civil society, varying level of resources and expertise in EU Member States.

Proportionality: Choice B complies with a **legitimate purpose**, which is tackling child sexual abuse and exploitation online and offline based on massive numbers of crimes in this area. It **corresponds to explicit calls for a more coordinated approach at EU level** and does not go beyond what is necessary to achieve the objectives identified for the EU intervention. Considering the increasing trends and threats of child sexual abuse over the past years, choice B is also proportionate with regard to anticipated future developments in this crime area.

Protects **fundamental rights**

Choice B protects fundamental rights to **human dignity**, to the **integrity of the person**, and the fundamental **rights of the child**, among others, by boosting efforts to **better prevent and protect children from sexual abuse and better support victims.** Additionally, choice B provides an important and effective safeguard that can help ensure and continuously verify that the impact on the rights of users to data protection and privacy of communications is limited to what is necessary, and support a fair balance between the different rights at stake.

Main disadvantages

Implies more extensive **preparation efforts** and **higher costs**

Choice B includes establishing a new organisation, which would incur **higher initial and running costs** than if the centre were established as part of an existing entity. It also creates **additional workload in the preparatory phase** with regard to finding the most suitable legal form and a Member State that could host it. Overall, the need to assemble resources, equipment and personnel will incur high implementation costs.

[599] Internet Watch Foundation, Victims are rescued with the help of your reports, accessed 28 April 2021.

Trade-offs

Coherent and holistic approach implies **higher costs**

Choice B would **enhance the overall response** to the threat of child sexual abuse at EU level, but the EU budget and/or the Member States would face **additional expenses** linked to the establishment of a new organisation. Whereas this choice seeks to streamline Member States efforts and ensure efficient use or resources in the big picture and in the long run, it is clear that additional human, technical, and financial efforts are required to provide a central point for improving prevention, support of victims, and the detection and reporting mechanisms. Considering the increasing number of child sexual abuse material online, the high costs to implement such a Centre which could respond to future threats more adequately than present mechanisms appears reasonable.

A newly established entity's overall efficiency might suffer from a lack of an established network and communication channels in the beginning, meaning investments by Member States will take some time to pay off until this centre becomes fully operational in practice. However, considering that this is a pioneering initiative, that no comparable entity can be found in the EU to date and that global examples exist about the success of such Centres (e.g. NCMEC), the risk of making high investments for an unknown, new initiative appears worthwhile.

ANNEX 11: SME TEST

1. Identification of affected businesses

SMEs are among the service providers affected by the measures described in this impact assessment, although it is known that almost 95% of reports of child sexual abuse online from service providers are made by a single large provider (Facebook), while just 5 providers are responsible for 99% of such reports[600]. This shows that SMEs account only for a small proportion of the current reporting.

Estimates suggest that at least 10 000 service providers concerned by the proposal could be SMEs. In this regard, 45% of these SMEs are micro-enterprises and 40% constitute medium-sized businesses[601]. Even though SMEs only accounted for a small proportion of the reports, their services are at a particular risk of being misused for child sexual abuse online, since they tend to lack the capacity to hire trained staff or deploy state-of-the-art technology to fight malicious content on their services.

2. Consultation of SME Stakeholders

1.1 SME stakeholders provided feedback to the Inception Impact Assessment and participated in the open public consultation through four industry associations:

- ETNO (European Telecommunications Network Operator's Association)
- EuroISPA (one of the largest 'umbrella' associations of Internet Services Providers in the world, which includes a significant number of SMEs)
- ACT – The App Association (representing more than 5,000 app companies and information technology firms across the mobile economy.)
- Interactive Software Federation of Europe (ISFE) - European Games Developers Federation

And directly as individual micro, small and medium enterprises:

- jurmatix Legal Intelligence UG
- Markus Hopfenspirger MaHop.Net
- AiBA (spin-off company under establishment and administration of NTNU Technology Transfer AS)
- Safer Together

[600] National Center for Missing and Exploited Children, 2020 Reports by Electronic Service Providers (ESP) (missingkids.org).

[601] Estimates based on data available in the Dealroom database, https://dealroom.co/.

- Open-Xchange AG
- Mega Limited
- Yubo
- The Computer & Communications Industry Association (CCIA)
- Bumble

Several of the above listed stakeholders raised concerns regarding the potential administrative burden and compliance costs for SMEs, and suggested a differentiated approach that takes into consideration the different circumstances of the various providers in order to avoid a one-size-fits-all approach. Although some stakeholders expressed support for obligatory detection, one stakeholder pointed out that while larger providers have the means to put in place mandatory detection systems, this is not always the case for SMEs. Some stakeholders expressed concerns regarding reporting obligations, which might also impose burdensome requirements on SMEs, in particular with regard to reporting to a central authority (since SMEs find it easier to report to national authorities). It was also pointed out that sanctions should be proportionate to the violation, especially for smaller players.

Nevertheless, several stakeholders recognised the need for legal clarity, and expressed general support for establishing obligations to detect, remove and report child sexual abuse conditional to ensuring the necessary flexibility and a differentiated approach. It was also highlighted that all providers should be allowed to make use of the available automatic technical tools to detect CSAM and preventing its distribution.

3. Measurement of the impact on SMEs

The different measures have been found to have the following impacts on SMEs:

Baseline scenario

The baseline scenario disincentives action by SMEs against child sexual abuse online. In this scenario, SMEs face legal uncertainty in relation to voluntary measures they may wish to implement against child sexual abuse online. Furthermore, certain SMEs will be impacted by the expiry of the Interim Regulation after 3 years following its entry into application, which will result in a prohibition of such voluntary measures in their services. As such, the main impacts on SMEs in the baseline scenario are conditions which tend to discourage action against child sexual abuse online, preventing SMEs who wish to do so from making their services safer.

Non-legislative measures

Given that the practical measures are largely voluntary in nature and do not require participation by all service providers, SMEs can participate where they deem the measures to be cost-effective in view of their individual business model, corporate social responsibility and other factors. Therefore, the economic impact of the practical options does not go beyond the necessary and should not disfavour SMEs. On the contrary, SMEs should benefit from standardised processes and improved feedback mechanisms

and communications channels, as well as practical support in the form of enhanced sharing of technologies and databases. The possibility to opt in to these practical measures may alleviate the cost burden for SMEs, increase legal certainty of their actions when tackling illegal content and contributing to ensure a level-playing field with larger companies.

Legislative measures

All the legislative options (B, C, D and E) would have an impact on SMEs.

Option B could provide greater legal certainty for SMEs who wish to undertake voluntary measures. While these measures would be voluntary in nature, the requirements and safeguards in the legislation could represent a burden to those SMEs considering implementing them.

Options C, D and E contain obligations to detect child sexual abuse online which would have higher impact on SMEs than options A and B.

SMEs will be subject to the same obligations as larger providers. As the report indicates, they are particularly vulnerable to exploitation of illegal activities, including CSA, not least since they tend to have limited capacity to deploy state-of-the-art technological solutions to detect CSAM or specialised staff. Even though companies may have unequal resources to integrate technologies for the detection of CSAM into their products, this negative effect is outweighed by the fact that excluding them from this obligation would create a safe space for child sexual abuse and therefore defeat the purpose of the proposal.

The implementation of technologies for the detection of such abuse may create new barriers and present a burden to SMEs. While the EU Centre would make technologies available to SMEs without charge, the continuous operation of those technologies could also lead to increased costs. SMEs would also experience an increased burden in relation to ensuring the appropriate human resources for the process of detection, reporting and removal of CSA online, including responding to follow-up requests from law enforcement authorities. The additional costs would imply that SMEs might have less funds at their disposal for research and innovation, increasing their competitive disadvantage towards large companies.

It is not possible to quantify exactly these costs since they would depend on the level of abuse that they would be exposed to. And this depends on the services they offer, and whether the degree to which they can be subject to effective and efficient mitigation measures, rather than the size of the company. For example, a SME with a small number of employees may offer a service with millions of users, which is particularly prone to be misused for CSA online, whereas a larger company may offer relatively niche services where the possibilities of misuse to commit CSA online are very limited.

4. Assessment of alternative mechanisms and mitigating measures

The following mitigating measure was considered:

- *Exempting SMEs from scope of one or more measures on obligations to detect, report and remove child sexual abuse material online and to detect and report solicitation of children online.*

This mitigating measure has not been retained, since such an exemption would risk creating a gap that could easily be exploited by offenders moving to services offered by SMEs. Smaller services becoming instrumental to the spread of child sexual abuse crimes would result in the infringement of the fundamental rights of victims, impacting the ability to pursue the specific objectives of the intervention.

The following mitigating measures were retained:

- Obligation for the competent national authorities to take into account the size and financial and technological capabilities of the provider when enforcing the Regulation, including in relation to the risk assessment, detection obligations and penalties.
- SMEs would be able to request free support from the EU Centre to conduct the risk assessment.
- Support from the Centre and the Commission in the form of:
    - **guidance**, to inform SMEs about the new legal framework and the obligations incumbent on them. This guidance could be disseminated with the help of industry associations; and
    - **specific training**, delivered in collaboration with Europol and the national authorities.

- Support from the Centre in the form of :
    - **Tools free of charge** to detect and facilitate reporting and removal of CSA online;
    - **Human review** of the reports, so that service providers (in particular SMEs), do not need to dedicate resources to it.