This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above-mentioned proposal, submitted on 11 May 2022 and referred to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE).

The EU has made the fight against child sexual abuse (CSA) a priority. In 2011, the EU adopted Directive 2011/93/EU (the Child Sexual Abuse Directive) to harmonise minimum criminal law rules at EU level concerning the definitions of CSA, exploitation offences and corresponding sanctions, and to introduce rules on prevention and protection of victims in this area. In 2020, the Commission adopted an EU strategy for a more effective fight against CSA. The European Parliament has been an important driver in stepping up EU efforts to combat child abuse. In 2015, it adopted a resolution specifically targeting online CSA.

The present proposal is included in the 2021 Commission work programme under ‘new initiatives’, and in the 2021 Joint Declaration of Legislative Priorities. The proposal aims to establish a long-term framework building on and eventually replacing Regulation (EU) 2021/1232 (the Interim Regulation). The latter provides for a temporary derogation from certain obligations of Directive 2002/58/EC (the e-privacy Directive), which protects the confidentiality of communications and traffic data. The temporary derogation enables providers of certain number-independent interpersonal communications services to continue voluntary practices for the detection, reporting and removal of child sexual abuse material (CSAM) online after the transposition deadline of Directive (EU) 2018/1972 (the European Electronic Communications Code), which elapsed at the end of 2020.

Problem definition

The Commission identifies as the main problem the fact 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 CSA on their services. At the same time, the existing responses at national level to some CSA 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’. According to the IA, the divergent national responses to this problem create a legal fragmentation, which negatively affects the internal market (IA, p. 17).

The IA cites research according to which at least one in five children falls victim to sexual violence during childhood. The IA specifies that the majority of victims are girls, and that vulnerable children are more likely to become victims of CSA online. The Commission points out that there has been a significant increase in reports of CSA online in recent years, which have been submitted by online service providers globally through the US National Centre for Missing and
Exploited Children (NCMEC).

The IA quotes reports that some companies active and with servers in the EU have now become the largest hosts of CSAM globally (IA, pp. 22-23; Annex 6).

The IA explains that the sexual abuse of children can take place both offline and online, and that most of the cases today have an online component. The IA points out that the internet has become the main medium for sharing CSAM. The IA makes clear that the present initiative concentrates on the online aspects of the crime in relation to efforts to detect, report and remove CSAM. The Commission underscores that this also includes grooming and circulating CSAM, which are criminal acts. The continued circulation of such material is a form of re-victimisation, and thus a continuous source of distress for the victims (IA, pp. 18-19).

The IA states that the proportion of cases in which CSA is discovered in a timely manner is very limited. It appears that the COVID-19 crisis has exacerbated the problem. Evidence shows that online service providers play a crucial role in detecting CSAM on their services (mostly through private messaging services). The IA lists the following three problem drivers (IA, pp. 19, 25-37):

1) Voluntary action by online service providers to detect online CSA has proven insufficient;
2) Inefficiencies in public-private cooperation between online service providers, civil society organisations and public authorities hamper an effective fight against CSA;
3) Member States’ efforts to prevent CSA and to assist victims are limited, divergent, lack coordination and are of unclear effectiveness.

Referring to pertinent data and reports, the Commission demonstrates that CSA online is a serious problem that needs to be tackled. It frames the problem for the purpose of this IA in a narrow way, focusing on the legal fragmentation of the internal market for service providers. The IA recognises that the distribution of CSAM is closely linked to its production, and that prevention is key to tackling the problem (IA, p. 19, Box 1; p. 23). However, the root causes of the serious societal problem of offenders sexually abusing children – which leads to the production of CSAM – are not further examined.

The IA rather briefly examines the third problem driver relating to the Member States' efforts to prevent CSA and assist victims. In line with the ‘evaluate first’ principle of the Commission's Better Regulation Guidelines, a Commission ex-post evaluation of the Child Sexual Abuse Directive (which is overdue and currently under preparation) should have provided input and concrete evidence for the need for regulatory intervention feeding into this IA. The Commission points out that one of the main challenges for the Member States is linked precisely to the transposition of the articles on prevention and assistance to victims in the Child Sexual Abuse Directive (IA, p. 37).

While the Interim Regulation only entered into force on 2 August 2021, it would have been useful for the IA to report on users' initial feedback regarding its implementation. The IA states that the Commission is preparing an implementation report of the Interim Regulation, due to be completed in August 2023 (IA, p. 10).

According to the IA, the main stakeholders affected are: children who may fall victim to sexual abuse and suffer its severe negative immediate and long-term effects; online service providers who have to comply with sector-specific, divergent rules under national laws at least in some jurisdictions where such rules exist; users of online services, whose rights can be negatively affected because the detection, reporting and removal of CSAM online currently lacks clarity, legal certainty and transparency; governments and public authorities, which need to dedicate significant resources to fight CSA; society as a whole, which has to bear the costs of the criminal acts related to CSA.

Subsidiarity / proportionality

The initiative is based on Article 114 TFEU. The initiative aims to ensure the proper functioning of the internal market. According to the Commission, the initiative should increase legal certainty, trust, innovation and growth in the single market for digital services. The IA finds that EU action is
necessary, because '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.' Without EU action, Member States would have to keep adopting national laws, which likely lead to fragmentation and diverging laws (IA, p. 41).

The EU added value of the initiative lies in reducing fragmentation, and in providing legal certainty and a coherent approach. Given the cross-border aspects of the problem, the number of policy areas concerned and the wide range of stakeholders, the Commission considers EU-level action to be the most appropriate one. EU action would also reduce dependence on NCMEC, which is currently the main source of reports of CSA online in the EU (IA, p. 42). No reasoned opinions from the EU-27 national parliaments on compliance with the principle of subsidiarity were submitted. According to the IA, all policy options are proportionate (IA, p. 111); however, considering what is at stake, a more thorough proportionality assessment would have been expected from the Commission.

Objectives of the initiative

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

The three specific objectives of the initiative (addressing the problem drivers) are:

1. ensure the effective detection, reporting and removal of online CSA 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 CSA through harmonisation of rules and increased coordination of efforts.

The second part of the general objective envisages detection, reporting and removal obligations for certain service providers, and therefore appears to predetermine the exclusion of voluntary measures from the start (which are part of options A and B below).

The Commission also identifies seven operational objectives in Section 9 on monitoring and evaluation. However, not all objectives seem to comply with all of the S.M.A.R.T criteria as set out in the Commission's Better Regulation Guidelines. The IA points out that the three specific objectives directly contribute to achieving the most relevant UN Sustainable Development Goals (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.

Range of options considered

The IA considered five policy options A to E (including one non-legislative option), next to the baseline of no EU action (see Figure 3, p. 53). The IA explains that the options take a gradual approach with an 'increasing level of obligations and intrusiveness', and that they follow a 'cumulative logic' (IA, pp. 51-52). The Commission's preferred option is option E.

The IA contains a summary (sort of a 'mini-IA') on the implementation choices for an EU centre to prevent and counter CSA when describing option B. These are: 1) establishing a self-standing, independent EU agency to support detection, reporting and removal of CSA online, and to facilitate Member States' efforts on prevention and assistance to victims; 2) tasking Europol with supporting detection, reporting and removal of CSA online and establishing an independent private-law entity for prevention and assistance to victims; 3) tasking the EU's Fundamental Rights Agency with all functions. Based on a qualitative and quantitative analysis of these three options, as well as a comparison thereof, the Commission concluded that its preferred option is option 1 (establishing an EU Centre as a dedicated EU decentralised agency) (IA, pp. 58-64; see also Annex 10).
Some options were discarded at an early stage: an indefinite continuation of the Interim Regulation would only perpetuate the insufficient voluntary action by online service providers; obligations to detect CSA online, which are limited to technologies currently used for detection (e.g. unencrypted services), would not be effective in achieving the objective of the initiative, and would possibly worsen the problem 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 through their services or stop the dissemination of CSAM (IA, p. 83).

The IA lays out the most likely scenario, excluding the initiative (baseline scenario), as one containing the following elements: after the end of the application period of the Interim Regulation (3 August 2024) and in the absence of other legislation, providers of number-independent interpersonal communications services would no longer be permitted to detect and report CSA; victims’ images and videos would continue to circulate; and law enforcement authorities (LEAs) would be unaware of the undetected crimes and unable to identify and rescue victims and investigate and prosecute these cases.

The Commission considers that under the baseline scenario, the existing policy instruments in the fight against CSA are not sufficient. Moreover, the inefficiencies under the baseline are expected to have a significant negative economic impact on society (likely resulting in a diminished life quality of the victims, productivity loss and costs to provide public services to assist victims). According to the IA, the estimated annual CSA costs in the EU amount to €13.8 billion (IA, pp. 44-51). As highlighted above, an ex-post evaluation of the Child Sexual Abuse Directive (currently under preparation) could have provided further insights into the current situation.

---

### Proposed policy options to address the identified problems

<table>
<thead>
<tr>
<th>Option A</th>
<th>practical measures to enhance prevention, detection, reporting and removal, and assistance to victims + EU Centre on prevention and assistance to victims (non-legislative option) (IA, pp. 53-55)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• practical measures to stimulate cooperation among stakeholders in prevention and assistance to victims, and enhance voluntary detection, reporting and removal of CSA online by relevant online service providers offering their services in the EU.</td>
</tr>
<tr>
<td></td>
<td>• the establishment of an EU Centre as an 'EU funded expertise hub', managed by the Commission with the help of a contractor, to support and facilitate information sharing on prevention and assistance to victims with Member States.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option B</th>
<th>option A + legislation 1) providing for a regulatory framework for voluntary detection, 2) requiring mandatory reporting and removal of online CSA, and 3) expanding the EU Centre to also support detection, reporting and removal (IA, pp. 55-58; Annex 10)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Option B combines option A with legislation to improve the detection, reporting and removal of CSA online (known and new CSAM, and grooming), applicable to service providers offering their services in the EU. It would provide for:</td>
</tr>
<tr>
<td></td>
<td>• a long-term regulatory framework for voluntary detection of CSA online (replacing the Interim Regulation) establishing an explicit legal basis permitting service providers to take action to detect CSA online in their services, and providing for mandatory limits and safeguards for voluntary detection;</td>
</tr>
<tr>
<td></td>
<td>• mandatory reporting to the EU Centre and removal of CSA online by service providers, including by SMEs, if CSA online is found (rules would contain conditions and safeguards);</td>
</tr>
<tr>
<td></td>
<td>• the establishment of an EU Centre to facilitate the detection, reporting, and removal of CSA online, as well as prevention and assistance to victims. The EU Centre would be independent and it would ensure transparency and accountability for the detection,</td>
</tr>
</tbody>
</table>
reporting and removal of CSA online. It would take the form of an EU decentralised agency.

**Option C: option B + mandatory detection of known CSAM (IA, pp. 69-76)**

Option C builds on option B and imposes on the relevant providers an **obligation to perform a risk assessment** on whether their services are likely to be used for the sharing of known CSAM. It also imposes on these providers the obligation to propose **mitigating measures** to reduce that risk. The service providers would be required to report to the competent national authority on the risk assessment they have made, including any mitigating measures they have taken.

Where the risk assessment reveals a level of risk that is not minor (not defined), national competent authorities would issue orders to detect material that has previously been confirmed by courts or other independent public authorities as constituting CSAM. The **detection orders for known CSAM** would be issued by a court or an independent administrative authority to a specific service provider. Such orders would be limited in time and would apply **regardless of the technology used** in the online exchanges. The detection of new CSAM and grooming would remain voluntary, whereas reporting and removal would be mandatory.

The **EU Centre** would support service providers by: providing relevant practical or technical information; developing a database of **indicators of known CSAM** (e.g. hashes and URLs) and facilitating access to free-of-charge detection tools; and reviewing the reports submitted to ensure accurate reporting to LEAs (see Annex 10, pp. 337-339).

The obligation to detect known CSAM would apply regardless of the technology deployed in the online exchanges; this would be done with the aim of ensuring that legislation remains **proportionate, technology-neutral and future-proof**. The legislation would provide for **three types of safeguards**: 1) what standards the detection technologies used must meet (e.g. to be sufficiently reliable and the least privacy-intrusive; 2) safeguards on how the technologies are deployed; such safeguards can be put in place by conducting a prior data protection impact assessment or by ensuring human oversight, where necessary; and 3) EU Centre-related safeguards, as listed above under how the EU Centre would provide support.

**Option D: option C + mandatory detection of new CSAM (IA, pp. 77-79)**

Option D is the same as option C, but it **adds the mandatory detection of material that has not been previously verified as CSAM** (i.e. ‘new’, as opposed to ‘known’ CSAM). The detection of new CSAM often reveals ongoing or recent abuse and thus implies a heightened need to act to rescue the victim.

As in option C, to ensure that the legislation is technology-neutral and ‘as future-proof as possible’, 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.

The **mandatory risk assessment**, as envisaged in option C, is expanded in so far as online service providers would be required to also assess **the risk that their services are misused to distribute new CSAM**. As in option C, the service providers would be required to report to the competent national authority on the risk assessment they have made, including any mitigating measures they may have taken. On the basis of the risk assessment, the competent national authority would decide whether to issue a **detection order** for new CSAM to a service provider.

The **EU Centre** would support service providers by: developing a database of **indicators of new CSAM** (e.g. AI classifiers) that providers would be required to use; facilitating access to free-of-charge detection tools; and reviewing the reports submitted to ensure accurate reporting to LEAs. According to the IA, the **safeguards** could include all those described in option C, extended to **new CSAM**.

**Option E (the Commission’s preferred option): option D + mandatory detection of grooming (IA, pp. 79-82)**
Option E is the same as option D, but it adds the mandatory detection of grooming for certain providers of interpersonal communications services as the key vectors for online grooming.

Option E would therefore comprise the mandatory detection of known and new CSAM, and ‘grooming’ (solicitation of children), limited to the service providers relevant for each of the types of content. Such providers are different for grooming: while CSAM can be shared in various ways, grooming requires a direct communication channel between the offender and the child. Whereas known and new CSAM depict crime scenes of abuses already committed (even though the IA also states that for new CSAM under option D the crime could also be ongoing), grooming can indicate abuse that is ongoing and/or about to happen, and which therefore could be prevented or stopped.

As in options C and D, the obligation to detect grooming would apply regardless of the technology deployed in the online exchanges. Reporting and removal by service providers would be mandatory for all types of CSA online.

The mandatory risk assessment is expanded in so far as online service providers would also be required to assess the risk that their services are misused for grooming. According to the IA, the risk factors specific to grooming could include, inter alia: whether the services are likely to be accessed by children; whether the services enable sharing images and videos via private communications for all users; whether robust age verification measures are in place. As in options C and D, the service providers would be required to report to the competent national authority the risk assessment, including any mitigating measures. 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 its service.

The EU Centre would support service providers by: developing a database of indicators for grooming (e.g. AI classifiers) that providers would be required to use; facilitating access to free-of-charge detection tools; and reviewing the reports submitted to ensure accurate reporting to LEAs. According to the IA, the safeguards could include all those described in option C, extended to grooming.

The design and description of the options raise some questions. First, since the five options are largely cumulative, it is questionable whether such options qualify indeed as ‘alternative options’, as stipulated in the Commission’s own Better Regulation Guidelines. Second, the general objective of the initiative includes detection, reporting and removal obligations for certain service providers, and therefore appears to predetermine the exclusion of voluntary measures from the start (which are part of options A and B). Third, the IA does not discuss the time needed to build up the EU centre (as an EU agency) and have it fully operational, and how this may affect the measures proposed.

Moreover, service providers appear to have a broad discretion when preparing the envisaged risk assessments, and the IA does not seem to explain what appropriate mitigating measures are. As regards the issuance of detection orders, the IA does not make it clear which necessary standard of proof/risk courts and competent authorities would apply when deliberating whether to issue a detection order, nor is the interplay with national criminal law discussed in greater detail.

Assessment of impacts

The IA contains a qualitative and a quantitative assessment of the impacts of the five policy options. The IA examined the impact on social, economic and fundamental rights, as well as the impacts on the UN Sustainable Development Goals (SDGs). It is surprising that the IA did not assess the impacts either on the internet environment or on the technologies currently used for online exchanges.

As regards social impacts, the Commission considers that options A and B would have a limited impact and therefore would not fully address the problem drivers. Option C is expected to have a positive impact on the protection of children and on the users’ confidence in the services they are
Using. According to the IA, the tools to detect known CSAM have a high accuracy rate (Annex 8). However, the IA admits that reporting could have a negative impact in the case of (occasional) false positives (that is, images and videos erroneously identified as CSAM): ‘additional strict safeguards would apply’, such as independent expert auditing of the database of indicators (IA, p. 87).

The social impacts of option D would be the same as those for option C, plus the impacts linked with establishing a legal obligation for the mandatory detection of new CSAM. Such a detection of new CSAM requires a different technology that relies on pattern recognition. While such technologies are quite advanced in terms of their reliability and efficacy, a systematic human verification of suspected new CSAM would be required. Option D would entail a positive social impact on children’s welfare resulting from the detection of new CSAM (IA, pp. 88-89). The social impacts of option E would be the same as in option D, plus those related to 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 ... grooming requires systematic human verification’. The IA explains that at present the tools for the detection of grooming have a slightly lower accuracy than those for the automatic detection of known or new CSAM, and would therefore require additional safeguards (IA, p. 89).

In terms of economic impacts, option A would overall entail a limited positive impact, generating moderate costs for service providers and public authorities, but also leading to cost reductions, e.g. reducing transaction costs. Option B would have the same economic impacts as option A, plus the impacts linked with: clarifying the legal basis for the voluntary detection of CSA by relevant online service providers; introducing a reporting and removal obligation; and the cost of establishing and maintaining an EU Centre. A reporting and removal obligation could result in additional costs for LEAs and service providers. For the public and the private sectors, the implementation of new legislation might involve new administrative and compliance costs. The economic impact of (voluntary) 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. Establishing an EU Centre would entail a significant cost for the EU budget (€25.7 million). In the long run, however, the Centre’s activities would lead to a decrease in the economic costs of CSA (IA, pp. 90-91, see also Annex 10).

Option C would have the same impacts as those under option B, plus those derived from the obligation to detect known CSAM. 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. However, they would benefit from the fact that this option would limit a further fragmentation of the Internal Market. Moreover, service providers would benefit from technologies provided by the EU Centre free of charge. The expected increase in reports from service providers would result in significant additional costs for public authorities. 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. Option D would have the same economic impacts as option C, plus those stemming from the obligation to detect new CSAM. The expansion to new CSAM could further increase the workload of LEAs. While the overall number of newly detected CSAM is expected to be lower than that of known CSAM, it will likely remain significant, considering that the cases require urgent attention. Thus, this increased workload would be accompanied by additional costs. 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 (IA, pp. 91-92, 195).

Option E would have the same economic impacts as option D, plus those stemming from the obligation to detect grooming. This latter aspect would require service providers to invest in integrating additional tools to detect this type of abuse. These costs could be mitigated by technologies that are made available for free by the EU Centre. By contrast, staffing costs for the Centre would increase. Compared to option D, LEAs would incur higher costs related to their obligation to process reports. The number of additional reports is expected to be lower compared
to known CSAM, but as regards new CSAM, swift action would be required. According to the IA, the positive economic impact would increase (as a result of improved victim support and quality of life), due to the higher number of children that would be protected against falling victim to CSA because of the timely detection of grooming (IA, p. 93).

As regards impacts on fundamental rights, the IA highlights the need to strike a fair balance between all of the fundamental rights affected. These include: the children's fundamental rights to human dignity, the rights to integrity of the person, the rights to the prohibition of inhuman or degrading treatment, as well as the rights of the child (Articles 1, 3, 4, 24 of the EU Charter) on the one hand, and the fundamental rights to respect for privacy, to protection of personal data and to freedom of expression and information, and the freedom to conduct a business, on the other (Articles 7, 8, 11, 16 of the EU Charter).

The non-legislative option A would be expected to have a limited positive impact on fundamental rights. Under option B, the IA considers that 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, to the confidentiality of their communication. A strong justification and strong safeguards (which are specified) would be needed to ensure an appropriate balance between the different fundamental rights. According to the IA, the justification consists in the particularly serious crimes that the envisaged measures aim to prevent and combat and the protection of children that they aim to ensure. Only service providers who do take action to detect CSAM proactively would be subject to new requirements, in addition to those arising from the proposed Digital Services Act (such as requirements on the reliability and accuracy of technologies). The EU Centre would have a significant positive impact on the rights of (potential) victims (IA, pp. 93-95).

Option C would have a significant positive impact on fundamental rights of victims whose images are circulating on the internet (especially as regards the right to privacy and rights of the child). At the same time, the mandatory nature of detection of known CSAM would have a notable impact on service providers’ freedom to conduct business. This, according to the IA, can only be justified by tackling the particularly serious crimes at hand. In addition, user rights (in particular freedom of expression, privacy and data protection) would be affected to a greater extent than in option B. The availability of free and verified tools could ensure that the impact on their rights does not go beyond what is strictly necessary according to the IA (IA, p. 97).

Option D would have a greater impact on service providers’ freedom to conduct business and interfere more deeply with the users’ rights to privacy, personal data protection and freedom of expression, because of the service providers’ obligation to detect new CSAM. ‘However, there is corresponding increase in the types of CSA that are tackled and, thus, in the achievement of the objective of combating the particularly serious crimes at hand and protecting children. Moreover, stricter safeguards, remedies and transparency and accountability measures would be provided for to safeguard users’ rights’. Safeguards include, for example, human confirmation and free-of-charge detection tools (IA, p. 98).

The impacts of option E are the same as in option D, with 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. At the same time, the detection process would be the most intrusive one for users (as it would involve searching text as the most important vector for grooming). This obligation would be restricted to only certain specific service providers, which are at high risk of being misused for grooming. According to the Commission, this approach would contribute to ensuring the required level of proportionality (IA, p. 100).

Considering the significant impacts of some of the envisaged measures on fundamental rights (as the Commission admits itself), one would have expected a more in-depth analysis of the balance
between the different fundamental rights of children and users, and of the proportionality of the measures envisaged.\textsuperscript{15}

The IA discusses the risk of errors in the detection process and the possible negative consequences for users’ rights. However, the IA could have also examined the risk of misusing the envisaged detection technologies for purposes other than for detecting CSAM, the risk of such technologies being hacked, and possible other unintended consequences that the measures could entail (for example, a decreased level of security, possible chilling effects). It is also not clear how service providers would, or in fact, could be supervised with regard to using the detection technologies and data obtained through their use.

As regards the impacts on the UN SDGs (which is a new requirement of the Better Regulation Guidelines), the IA points out that options C to E would have a positive impact on all SDGs, while options A and B would have a more limited impact on them.

The IA compares the five options against the baseline in terms of their effectiveness, efficiency, coherence and proportionality in a qualitative and quantitative way. The Commission concludes that option E is the most effective option to address the problem, despite its greatest impacts on fundamental rights compared to the other options.

**SMEs/ Competitiveness**

The IA takes into account the impact on SMEs (an SME test was conducted, see IA, Annex 11). The Commission quotes estimates suggesting that at least 10,000 service providers concerned by the proposal could be SMEs. It details how SMEs would be particularly affected under options C to E, since they have limited capacity to deploy state-of-the-art technological solutions to detect CSAM or employ specialised staff (IA, p. 92). Several of the SME 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 (Annex 11).

The IA considered different mitigating measures, including exempting SMEs from the obligations to detect, report and remove CSAM online and to detect and report grooming. However, this exemption was discarded because it would risk ‘creating a gap that could easily be exploited by offenders moving to services offered by SMEs’. Retained mitigating measures include: the EU Centre’s support to SMEs by supplying them with free-of-charge detection technologies and a database of indicators. In addition, the Commission would provide guidance to SMEs (IA, p. 81).

**Simplification and other regulatory implications**

According to the Commission, the initiative aims to build on and complement the existing policy instruments in the fight against CSA. The existing legal framework consists of horizontal instruments in the area of data protection and online privacy (e.g. the General Data Protection Regulation (GDPR) and the e-Privacy Directive and its proposed revision), and of the single market for digital services (e.g. the e-Commerce Directive and the proposed Digital Services Act), as well as sector-specific legislation, such as the Child Sexual Abuse Directive, the Europol Regulation and its proposed revision (which has now been adopted, see revised Europol Regulation), the Interim Regulation derogating from the application of certain rights and obligations under the e-Privacy Directive, and the Victims’ Rights Directive.

The IA outlines how EU-level cooperation in investigations, prevention and assistance to victims, as well as multi-stakeholder cooperation complement the existing legal framework. The IA details how the initiative would interact with existing instruments, policies, and funding mechanisms (IA, pp. 5-14; Annex 5). The initiative would replace the Interim Regulation currently in force. However, it seems that the IA did not consider the risk of a legal gap between the end of the application of the Interim Regulation (3 August 2024) and a possible delayed entry into force of the new legislation.
Monitoring and evaluation

The IA points out that progress in the fight against CSA will be monitored and evaluated against the three specific objectives, which have corresponding operational objectives (see IA, Table 11, p. 117). The achievement of the operational objectives would be monitored through indicators. Different players would be responsible for collecting and sharing the various data sources for the indicators. The indicators would build on those of the Interim Regulation (IA, p. 115). It appears that many but not all indicators were taken over in the proposal (for example, it seems that those regarding prevention and victim assistance programmes are missing). Every 5 years, the Commission plans to prepare an implementation report and an ex-post evaluation.

Stakeholder consultation

The Commission carried out several stakeholder consultation activities (Annex 2), including an open, public stakeholder consultation from 11 February to 15 April 2021. However, instead of the mandatory 12 weeks, as envisaged by the Better Regulation Guidelines, the public stakeholder consultation only lasted 9 weeks. The Commission argued that the consultation period had to be shortened so that its outcome could be used for the IA. A total of 587 valid responses were received: 3/4 of them came from EU citizens (78 %) and almost half of them came from Germany (45 %). Of note is the fact that service providers expressed little support for the imposition on them of a legal obligation 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 given the current state of technology, be in line with other EU legislation (e.g. e-Commerce Directive and the DSA), and not impose an excessive burden on SMEs (IA, p. 82).

The Commission had previously also consulted stakeholders on the Inception Impact Assessment from 2 to 30 December 2020 (41 contributions were submitted). Moreover, the IA is based on two sets of targeted surveys for LEAs in Member States. The Commission also organised several expert group meetings and bilateral meetings with stakeholders, including member states' authorities at the national level, several private sector service providers and civil society organisations. The Commission also received letters and public statements from stakeholders expressing their views on the commitments in the EU Strategy for a more effective fight against CSA, and more particularly in the Interim Regulation.

The IA reports on the different stakeholder views, including regarding the options. Stakeholder views diverged, for example, on the mandatory detection of grooming, which forms part of the preferred option. In the public stakeholder consultation, it received little or no support from privacy rights organisations, service providers and individuals, while the level of support by public authorities and child rights NGOs was at 48 %, and 51 %, respectively (see IA, p. 82). The European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) in their joint opinion on the proposal raised serious concerns about the necessity and proportionality of the measures for the detection of unknown CSAM and grooming.

Supporting data and analytical methods used

The IA is based on several studies, reports, case law, data, academic articles and related IAs, in addition to the stakeholder consultations. According to the Commission, 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’ (Annex 1, p. 122). The three external supporting studies, prepared by ICF et al. for the IA, are the following:

1) a study on options for the creation of a European Centre to prevent and counter CSA, including the use of ICT for creation of a database of hashes for CSAM and connected data protection issues, 2021;
Preventing and combating child sexual abuse

2) a study on a framework of best practices to tackle CSAM online, 2020 (only the executive summary is publicly available);

(3) an overview of the legal framework of notice-and-action procedures in Member States, 2018.

The first two studies are not publicly available. While it is comprehensible that the part of the first study on the use of ICT for creation of a database of hashes of CSAM, as well as the second study on best practices are kept confidential, it is less understandable why the options for the creation of a centre were not made public. Annex 4 of the IA on analytical methods contains qualitative and quantitative assessments of the measures proposed. The assumptions and limitations are set out in a transparent manner. Annex 8 provides information on technologies to detect CSA online, including hashing technology, classifiers and artificial intelligence, and technologies to detect grooming in text-based communications. Annex 9 outlines the role of encryption in the dissemination of CSAM and the grooming of children.

Follow-up to the opinion of the Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) issued two opinions: first a negative opinion (date of RSB meeting was 16 June 2021) and subsequently an opinion marked 'positive with reservations' on 15 February 2022. The board criticised shortcomings that concern, inter alia, the problem definition; the necessity for EU action; how the options that include the detection of new CSAM or grooming would respect the prohibition of general monitoring obligations; how fundamental rights would be protected (in particular regarding technologies to detect CSA in encrypted communications); the role of and options for the EU Centre; and the proportionality of the preferred option E. The Commission services describe in Annex 1 to the IA how the RSB's recommendations were addressed. It appears that efforts were made to address these recommendations; however, some of the points would have deserved a more in-depth assessment (for example, as regards how fundamental rights will be safeguarded).

Coherence between the Commission's legislative proposal and IA

It seems that the Commission proposal corresponds to the preferred option of the IA.

The Commission demonstrates that child sexual abuse online is a serious problem that needs to be tackled. It frames the problem for the purpose of this IA in a narrow way, focusing on the legal fragmentation of the internal market for service providers. The root causes of the serious societal problem of offenders sexually abusing children – which leads to the production of CSAM – are not further examined. The IA considered five cumulative options; however, the formulation of the general objective of the initiative appears to predetermine the exclusion of voluntary measures from the start (which are part of options A and B). The IA examined the economic, social and fundamental rights impacts of all options. It is surprising that the IA did not assess the impacts either on the internet environment or on the technologies currently used for online exchanges.

While the open public stakeholder consultation period was shortened, the IA made efforts to consult widely, and reported on the different stakeholder views (which diverged, for example, regarding the detection of grooming). The IA is substantiated by pertinent data, studies and reports. However, two of the supporting studies are not publicly available. The IA seems transparent about the lack of data and limitations. Considering that the initiative involves striking a balance between the fundamental rights of children and users, more in-depth analysis might have been expected of 1) all fundamental rights of all stakeholders affected; 2) the necessity and proportionality of the proposed measures.

ENDNOTES

1 For an overview of existing legislation at EU, Member State and the international level related to online CSA, see P. Jeney, Combating child sex abuse online, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, October 2015.

3 Since the proposal for the Interim Regulation was not accompanied by a Commission impact assessment, the LIBE Committee requested a substitute impact assessment from the European Parliamentary Research Service (EPRS).

4 See the *One in Five Campaign*, Council of Europe, 2010-2015 (campaign website).

5 The IA uses the term ‘child sexual abuse online’ to denote the three main types of abuse: known and new child sexual abuse material, as well as grooming (see IA glossary, p. 2). Child sexual abuse content refers to text-based exchanges, photos, videos and other material illegal under EU law (see the CSA Directive).

6 The National Centre for Missing and Exploited Children (NCMEC) is a US private, non-profit organisation. Online service providers in the US are required to report instances of potential CSA that they find in their networks to the NCMEC.

7 See the IA glossary, p. 2).

8 The IA defines grooming as ‘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’ (see IA glossary, p. 2).


10 The Commission substantiates this point by explaining that voluntary action i) varies significantly among companies, ii) is susceptible to changes in companies’ policies, iii) leaves decisions affecting fundamental rights to service providers and lacks harmonised safeguards, and iv) has failed to remove victims’ images effectively.

11 The Commission launched a study to prepare an evaluation of this directive at the time when the IA was being written (see IA, p. 9). In 2016, the Commission published two reports assessing the extent to which the Member States had taken the necessary measures to comply with the Child Sexual Abuse Directive: COM(2016) 871 and COM(2016) 872.

12 The operational objectives are: on prevention: 1) reduce CSA prevalence; 2) reduce duplication and blind spots of Member States’ efforts; on assistance to victims: 3) provide the required assistance; 4) reduce duplication and blind spots of Member States’ efforts; on detection and reporting: 5) detect, report and remove all CSAM, known and new, distributed online; 6) increase detection and reporting of grooming; 7) make clear all relevant aspects of the detection, reporting and removal process by online service providers (IA, p. 117, Table 11).

13 The S.M.A.R.T criteria refer to objectives being specific, measurable, achievable, relevant and time-bound.

14 See also joint opinion of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) of 28 July 2022, p. 14; on the mitigating measures, see Question 2 of the letter from the German government sent to the European Commission on 17 June 2022).

15 See also the EPRS Substitute Impact Assessment of the Interim Regulation, European Parliament, February 2021.

16 The third study is publicly available, however, its quality was questioned by an Expert Advisory Group composed of five academics. In a preamble to the Annexes (p. i), the group raised grave methodological concerns about the study.