Impact Assessment Quality Checklist for Regulatory Scrutiny Board Opinion[1]			
Title:	**Regulation on detection, removal and reporting of child sexual abuse online, and establishing the EU centre to prevent and counter child sexual abuse**		
AP Reference:	PLAN/2020/8915	IA submitted to the RSB on:	25/05/2021
RSB meeting	16/06/2021	Date of IAQC (initials A2 Desk):	11/06/2021 (IGL/FL)

Policy context
Child sexual abuse (CSA) is a particularly serious crime that has serious life-long consequences for victims. The exponential development of the digital world makes this crime a truly global one. The aim of this initiative is to establish an obligation for relevant online service providers to detect child sexual abuse online, to report this to the public authorities and to remove the relevant content. It also explores the option of creating a European centre to prevent and counter child sexual abuse. This initiative follows up on the child sexual abuse strategy adopted in July 2020.

MAIN ISSUES FOR DISCUSSION

1.1. How does the present initiative relate to the Digital Services Act (DSA) and to the Child Sexual Abuse Directive? Why can an evaluation and revision of the latter not tackle the problems identified in this report? What are the deficiencies of the current interim derogation in combination with the DSA? Which are the prevention, detection and victim support issues that cannot be sufficiently tackled at Member State level? (boxes 1, 2 and 3)

- Relation with the Digital Services Act. The present initiative builds on both of the other instruments. The **Digital Services Act (DSA)** proposal covers all types of illegal content and sets out a horizontal framework. Its main aim is to create a system for referral of publicly available materials, noticed by users or authorities, to companies, with obligations to respond to orders issued by national public authorities. It also obliges very large platforms to institute due diligence measures. Although this might encourage some service providers to implement voluntary detection and removal measures, it does not suffice to address the specific problem posed by child sexual abuse. In particular, the DSA does not provide a legal basis for companies to implement voluntary detection and removal measures with regard to addressing illegal content such as child sexual abuse material or grooming, nor a comprehensive reporting obligation. This is purposely left to sector-specific legislation. Child sexual

[1] The Board's assessment is based on the application of the Commission's guidelines, the evidence base, the scope and depth of the analysis and whether it is proportionate in relation to the type of initiative and likely impacts, as well as the quality of the analysis, the appropriateness of the applied tools/methodology and the reliability of the data used.

abuse material, which is often not publicly available, and is manifestly illegal regardless of context, in contrast to much of the content covered by the horizontal instrument, requires a different, targeted and stronger approach. This was agreed in spring 2020 in two dedicated Cabinets-Services meetings on whether to include this stronger approach in the DSA proposals. There was agreement that there needed to be special rules to remove CSA materials, including an obligation, and that these should be provided separately from the DSA. The College confirmed this approach in the July CSA strategy. The present initiative will join other sector-specific initiatives like the terrorist content online regulation and the Copyright and Audiovisual Media Services directives in providing more specific and stricter rules to address certain types of illegal content and activities.

- Relation with the Child Sexual Abuse Directive. The present initiative stands beside the provisions and obligations of Directive 2011/93/EU, which focus on the role of Member States and their public authorities in relation to offenders, i.e. the public law enforcement perspective. The Directive defines what is criminal behaviour, and also requires Member States to ensure adequate assistance and support to victims, as well as to put in place prevention measures. Article 25 of the Directive requires Member States to take necessary measures to ensure the prompt removal of or blocking of access to web pages containing or disseminating child pornography hosted in their territory and to "endeavour to obtain" such removal outside their territory. However, this is a reactive approach; it does not provide any legal basis or positive obligation for online service providers to take action and does not provide sufficient specification of the role of 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. Given the Directive's specific legal basis (Art. 82(2) and 83(1) of the TFEU), any revision would be constrained to establishing minimum rules concerning the definition of criminal offences and sanctions in the area of sexual exploitation of children. It would not offer a possibility to regulate online service providers, nor to set up a centre to steer and support efforts in this regard.

- Relation with the interim derogation. The interim regulation cannot provide a long-term solution since it will expire three years after its entry into force and was always intended as a temporary measure. It only addresses one specific part of the problem, for a limited subset of service providers (number independent interpersonal communication services), and relies fully on voluntary approaches. This is not in line with the Commission's commitment for its long-term approach and does not meet the established objectives.

- Subsidiarity considerations on prevention and assistance to victims. By the nature of online child sexual abuse, these crimes constantly cross borders as they take place on the Internet. A single Member State cannot ensure prevention of the circulation of a child sexual abuse image or video outside its territory without the ability to cooperate and coordinate with the private entities who provide services in several (if not all) Member States. Prevention and victim support in this context can only be truly effective if there is a centralised approach to the material circulating and to requests from victims to remove material depicting them. Without a coordinated effort, there cannot be an efficient response to this issue, as has been recognised for several other legislative initiatives dealing with illegal content, including the DSA.

  At the same time, a Member State-based approach is also more challenging for providers, which often provide their services in several Member States. If the Member

States were left to come up with their own separate approaches, this would result in a fragmentation of the legislative framework, with different rules applying in different Member States. Compared to one horizontal framework, such a Member State-based approach increases the costs of doing business in the EU as providers have to adapt to various different sets of rules, which creates challenges in particular for smaller providers seeking to expand to new markets in the EU, and can stifle innovation and competition.

Regarding the offline aspects of prevention and victim support in general, 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. The 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.

1.2. Why have all main implementation options for the EU centre not been assessed in the main report? Why is it not possible to ensure independence, accountability and transparency of detection and reporting via an existing EU body? Who would supervise the quality and independence of the EU centre under the preferred implementation option? (boxes 1, 2 and 5)

- Assessment of implementation options. To keep the report concise in view of the significant number of aspects to consider, the intended purpose of annex 10 was to screen and assess in detail all possible centre options, and determine the preferred one to be incorporated in the options of the report. This approach allowed to focus in the report on the role that the centre plays in addressing the problem and achieving the objectives (the "why"), while annex 10 focuses on setting out the corresponding requirements for the centre, analysing the possible implementation forms, and determining the most suitable one (the "how").
- Independence, accountability and transparency. Among the existing EU bodies, Europol is the one that could be considered as a candidate to host the centre with all its envisaged functions.

  The centre will be a fundamental component of the legislation by serving as a key facilitator of the work of service providers in detecting and reporting 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 this facilitator role, it is essential that the centre be **independent** from service providers and from law enforcement (including Europol), so that 1) it can remain neutral 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 (including offenders); 2) US based service providers (which are by far the most relevant service providers for this initiative), have indicated in the consultations that they are prohibited by law to work closely with law enforcement in a way that could make them "agents of the state" (Fourth Amendment to the US Constitution). 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; 3) an independent centre could verify the illegality of materials reported and serve as a further safeguard against reporting innocent persons to law enforcement; and 4) users that feel that have been unfairly treated by service providers (e.g. if their content has been mistakenly removed and

they feel that the service provider has not ensured a fair complaint procedure) can turn to a neutral entity, not directly linked to law enforcement, without fear of possible repercussions.

- Supervision of quality and independence. The governance of the Centre will be set up in line with existing agencies, to ensure accountability to EU institutions and the Member States. 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 Commission will further supervise the centre as part of its management board. The governance mechanism would also ensure participation of all the relevant stakeholders representing the different interests and rights at issue (including both children's rights and internet users' privacy rights). The centre will 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.

  To ensure the centre's **independence**, in particular from potentially overriding private and political interests, the centre would be financially independent and receive a majority of its funding from the EU. This would entail an additional supervision by the European Court of Auditors.

1.3. How is the general obligation to detect child sexual abuse material (CSAM) or grooming compatible with the prohibition of general monitoring?

The case law of the Court of Justice of the EU (CJEU) has not yet provided a clear delineation between general and targeted/specific monitoring obligations. Furthermore, its case law so far has only dealt with this issue concerning copyright infringement and defamation in specific cases in a given Member State. It has not yet had to assess a similar obligation with regard to illegal content such as child sexual abuse material and it has not yet had to consider the implications of such obligations on EU level.

That said, certain criteria have been indicated by the Court when deciding whether a monitoring obligation is to be considered general and thus prohibited. As long as the preventive monitoring obligation ensures a fair balance between the affected fundamental rights, does not impose an excessive burden on providers, and does not require them to conduct an independent assessment on the illegality of a piece of content, it can be reconciled with the general monitoring obligation prohibition.

For all three options requiring detection and reporting of child sexual abuse online, the EU centre on prevention and assistance to victims would become a fundamental component of the legislation, as it would serve both as the source of reliable information about what is illegal and as a control mechanism to help ensure the effective implementation of the legislation (for ex.: sharing hashes of material that is illegal in the EU or specific and reliable indicators of new material, such as AI patterns/classifiers).

All three options in the report requiring mandatory detection (options C, D and E) aim to ensure a fair balance between the rights of victims (right to security, protection of personal data, respect for private life), users (freedom of expression, right to protection of personal data and right to privacy) and providers (right to conduct a business). The proposed options achieve this through a number of detailed conditions and safeguards, which will include:

- Making available clear information on what is considered illegal;
- Making available for free reliable tools to be used for detection;
- Ensuring that those tools offer automated solutions and are the least intrusive and fully compliant with the data protection rules;
- Ensuring reporting of suspected child sexual abuse and independent verification including feedback to the providers;
- Ensuring the reliable quality of data used by the tools;
- Requiring independent auditing of the database used by the tools;
- Ensuring accuracy of the tools through independent expert certification;
- Ensuring regular supervision and verification of the procedures of the EU Centre;
- Requiring regular and detailed reporting on the monitoring measures to ensure transparency and accountability;
- Providing redress/remedies to challenge providers' decisions to report suspected content or behaviour;
- In the case of new material and grooming, requiring human review of suspected content or behaviour before reporting it (for SMEs this can be provided by the EU centre, see below);
- In the case of grooming, targeting specific inter-personal communications services where children are at high risk and providing requirements for the objective determination of risk factors indicating possible grooming.

1.4. Are the risks of future CSA detection technologies for encrypted communications sufficiently known and assessed to already decide on their mandatory use in this initiative? How will coherence with the horizontal process on encryption be ensured? How could effective political oversight on the use of proper detection technology look like? (box 5)

- Risks of technologies to detect CSA in encrypted communications. The legislation would determine in a clear and comprehensive way the minimum conditions and safeguards that the technology should meet before the mandatory detection of child sexual abuse online would apply also to encrypted content. The legislation would not impose a priori the use of any given technology, and only those technologies that meet the conditions set out in the legislation (and therefore minimise the risks) would be lawful.
- Coherence with the horizontal process. As stated in the report 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 CSA therefore cannot leave aside the question of encryption without putting at risk the *effet utile* of the legislation. This includes the legislative proposal under consideration.

  The coherence with the Commission's horizontal work stream on encryption would be ensured as all the DGs participating in such process are also part of the inter-service group that will be assisting in the preparation of the legislative proposal. In addition, the legislative proposal would not prescribe any given technology, also to allow for new and improved solutions, but rather set out the safeguards that must apply across the

board. This approach, which is necessary to maintain technological neutrality, also minimises any risk of lack of coherence. In any case, it is important to note that the horizontal process focuses on lawful access (i.e. **ex-post** access) to any kind of illegal content by public authorities (not in the scope of this initiative), rather than on **proactive** detection by companies of **specific** content, which may not be necessarily encrypted.

- Oversight on the use of the technology. The ultimate responsibility to comply with the requirements set out in the legislation would lie on the service provider. This includes not only the technological solution chosen but also the particularities of its deployment in the service provider's systems.
  That said, to support the service provider in this process, the legislation would require it to be subject to oversight by national competent authorities, including data protection authorities with regard to data protection issues, as well as other nationally designated authoritieswith regard to the technical requirements other than data protection (e.g. security of the technology, i.e. vulnerability to be misused for other purposes than the fight against CSA). Where prior consultations are obligatory, these are to be completed prior to deploying the technology. Beyond prior consultations, national authorities would continue to supervise the respective data protection and other technical aspects during the deployment of the technology and during its continuous application.

1.5. How robust is the evidence used to estimate the costs and benefits for the various options? Which part of the benefits is due to the mandatory obligations and which is due to the centre? What are the impacts on SMEs? (boxes 3, 6 and 7)

- Robustness of the evidence. Given the limited availability of data, the estimates for the costs and benefits for the various options are based on a number of assumptions combined with the data that is available. As noted in section 6.2, rather than providing exact forecasts, the estimates of costs and benefits can only provide with a certain degree of reliability the order of magnitude of the expected costs and benefits, which would also enable the comparison of options.

- Origin of benefits. The estimated benefits under each option presented on are calculated based solely on the estimated reduction in crimes, which is assumed to be directly correlated with the increased number of reports received. Two factors contribute to these benefits, namely the obligations placed upon service providers, and the role played by the centre in facilitating processes relating to detection, reporting and investigation. These factors are intrinsically linked, and the benefits arising from each one cannot readily be separated. As described in annex 10, the centre will also lead to other benefits. For example, the centre's role in facilitating prevention efforts will also lead to a reduction in crime, while its role in victim assistance will lead to possible savings due to a reduced duplication of efforts, thanks to the enhanced cooperation and exchange of best practices that the centre would enable. The above clarifications will be added to the report.

- Impacts on SMEs. 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.
To alleviate the economic impact on SMEs, several mitigating measures are envisaged. SMEs would be exempted from obligations to perform human review, which would instead be carried out by the centre. In addition, the centre would make available to SMEs technologies and reliable indicators for the detection of child sexual abuse available at no cost.
Annex 11 (SME test) will be reviewed to state upfront the exemptions foreseen for SMEs under the various options, and to include cost estimates for SMEs.

1.6. How does the initiative strike a balance between the need to prevent and counter child sexual abuse online and the preservation of other fundamental rights (e.g. data protection, privacy)? (boxes 5 and 6)

To ensure that a balance with be struck between all the fundamental rights as stake (see in particular section 6.1.3. on fundamental rights impact) the legislation will include the necessary safeguards, which will also ensure accuracy, transparency, and accountability, including supervision by designated authorities , of the process to detect, report and remove child sexual abuse online.

In the case of the preferred option, these safeguards 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. Other safeguards could include requirements to ensure the quality of data used to train algorithms, and mechanisms such as mandatory human review to further increase the accuracy of the detection process

The centre will be a fundamental component of the part of the legislative initiative and will serve as **a key safeguard** on its role of facilitator of the work of service providers in detecting and reporting the abuse, and of the work of law enforcement in receiving and investigating the reports from service providers. The centre would serve both as the source of reliable information about what constitutes CSAM, providing companies with the sets of indicators on the basis of which they should conduct the mandatory detection of CSAM, and as a control mechanism to help ensure transparency and accountability of service providers, including possibly helping to resolve complaints from users. Moreover, to be able to play its role as a facilitator, the centre must be independent and neutral and maintain 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.

1.7. How robust is the scoring methodology used for the assessment and comparison of options? Why are the options not compared in terms of effectiveness, efficiency and coherence? (box 7)

- Scoring methodology. The scoring methodology used for the comparison of the policy options is based upon the qualitative analysis of the options.. Based upon the comments in box 7 below, the scoring will be revised in particular by ensuring that the baseline always has a score of 0 (no change).

- Comparison criteria. The options are compared in terms of effectiveness, efficiency, coherence and proportionality in section 7.1 ,

1. CONTEXT AND SCOPE

1. Context and scope
The report should better describe the political context of the initiative, in particular commitments made and the link to parallel initiatives. It should clarify how the current initiative contributes to the **EU strategy for a more effective fight against child sexual abuse**.
OK. This information, currently in annex 5 (p. 112), will be summarised and included in the report.
The report should clarify the role of the proposed **Digital Services Act** in the fight against online child sexual abuse on which the present initiative is supposed to build (p.2 and reference to sectoral legislation on p.14). Coherence aspects should be considered, in particular regarding the prohibition of general monitoring (pp.12, 13, 18 of the report, p.28 of annex 2, Verizon Media's view on IIA).
OK, the role of the DSA in the fight against CSA and the coherence with the present initiative, in particular in relation to the prohibition of general monitoring, will be made explicit in this section of the report.
The report should briefly explain the role of the **Child Sexual Abuse Directive 2011/93** (CSA Directive) that covers both offline and online abuses. What is the relationship between the Directive and the present initiative? Why is the present initiative launched before an evaluation of the Directive? In view of the fact that the **offline** and **online** aspects of the CSA related crimes have become increasingly intertwined (p.124 annex 6), why has the present initiative not been integrated into a revision of the Directive (after evaluation of the latter)? How will the present initiative address implementation issues with the Directive (p.8)?
The provisions and obligations of Directive 2011/93/EU are addressed to Member States (and their public authorities) and define what is illegal (both online and offline crimes) and aim to harmonise substantive and procedural criminal law, while also requiring Member States to ensure - predominantly in the offline sphere - adequate assistance and support to victims as well as to put in place prevention measures.
The Directive is constrained to establishing minimum rules concerning the definition of criminal offences and sanctions and predominantly offline prevention measures in the area of sexual exploitation of children and does not regulate online service providers nor provide for efficient online prevention and detection measures.
Given the different objectives to be achieved by the revised Directive and the long-term proposal, the decision was taken to prepare the two work streams in parallel. The two instruments are meant to complement and mutually reinforce each other without creating unnecessary overlaps. A study is being prepared to explore the necessity to revise the Directive. Even if based on the outcome of the study, there will be a need to revise the Directive, due to the constraints of its legal basis it will not provide enough flexibility for regulating private companies and for imposing effective online detection and prevention measures. The long-term proposal is meant for this very specific purpose of creating more efficient detection and prevention obligations for online service providers, while also fostering the improvement of assistance and support to victims in practical terms through the EU Centre, as well as supporting prevention efforts. In sum, a possible revision of the

Directive will aim to address issues that can be tackled by public authorities while the long-term proposal aims to do so with regard to relevant private sector stakeholders offering their services on the Single Market.

The present initiative is not meant to directly address implementation issues with the Directive. As highlighted above, a study has been launched to prepare the evaluation of the Directive and there are ongoing infringement and EU Pilot procedures against 21 Member States. The majority of 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), substantive criminal law and offline assistance, support and protection measures for child victims. Despite the long term proposal's particular objective, it will have a positive effect on the implementation of the Directive in an indirect way, in particular through the EU Centre, which will foster the exchange of best practices and expertise from which, Member States' public authorities will be able to benefit when applying the Directive.

The context section should describe more clearly which obligations and (operational) tasks the CSA Directive imposes on Member States. It should explain how existing EU level coordination relates to operational prevention, enforcement and victim support measures taken at Member State or local level. The report should also briefly explain whether there are differences in the implementation of the CSA Directive across Member States and whether infringement action is on-going (and, if so, on which issues).

OK, an overview of the implementation of the CSA Directive will be added to the report.

The report should better frame the present initiative, clarify what is already decided and what is the scope of this initiative. It should clearly explain why this initiative focuses on the creation of a centre and hardly considers the role that existing EU bodies such as Europol could play.

OK, additional clarifications on the scope of the initiative will be added. Also, elements of the analysis of the various implementation options for the centre in annex 10 (which analyses the creation of the centre entirely or partly embedded within Europol as two of the four possible choices) will be incorporated in the report.

2. PROBLEM DEFINITION AND USE OF EVALUATION

2. Problem definition and use of evaluation
The problem analysis should better explain why **existing and new parallel initiatives** fail to address the problem of online child sexual abuse. This concerns the Digital Services Act, the interim derogation, the Child Sexual Abuse Directive and the ongoing revision of the Europol mandate to improve cooperation between authorities and service providers. The report should fully incorporate expected future progress resulting from new initiatives. For example, it should not claim that 'EU law does not provide for an obligation for providers to act upon notified content, not even where it manifestly constitutes CSAM' (p. 10). This is covered (at least partly) by the DSA. OK, explanation of the parallel new initiatives and why they fail to address the problem will be added. In addition, there are also the efforts by the Member States (the report refers to "significant resources" invested by Member States (p.7)). Are there lessons to be learnt from national experiences? Are the results different between Member States? Moreover, the report should clarify figures that refer to an uneven distribution of CSA across the EU, with apparently a hosting concentration in some Member States (on p.5, it refers to "77%" in the Netherlands). The report should explain the meaning and source of the figures and possibly explain such concentration, including why no action has been taken neither at Member States nor at EU level. The problem drivers section incorporates information from national experiences gathered in particular during the analysis of the implementation of the child Sexual Abuse Directive and other exchanges with Member States. The assessment shows that the situation with regard to e.g. existence and efficiency of efforts in the areas of prevention of victim support differs among the Member States. A general overview of the state of the implementation and infringement proceedings will be added. However, as there are open infringement proceedings against 21 Member States, revealing details of the situation on the ground in individual member States could harm the process of resolving the cases without having to refer it to the Court of Justice, so the information in the report will not "name and shame" any individual Member State unless the information is already public. The origin and significance of the figures in the Netherlands will be clarified in the report. shows the ineffectiveness of the current system. It will also describe the actions planned in the Netherlands to address this issue, partly as a result of the bilateral exchanges with the Commission (EU Pilot) during the monitoring of the implementation of the Child Sexual Abuse Directive. The problem analysis should further develop the **international and cross-border nature of the problem**. It should clarify why measures taken at the national level may be ineffective. There are several international and cross-border aspects to the problem. In many cases, these are due to the inherent 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 minimal standards relating to child sexual abuse crimes have been widely adopted in criminal law in many countries, precise definitions and offences differ from one country to another. In addition, long-standing difficulties with regard to

access to electronic evidence across borders pose a particular problem for the investigation of child sexual abuse with a cross-border dimension. Furthermore, due to the existing legal framework and the dominant market position of US service providers, Member States are heavily dependent on reports received from a third country (through NCMEC) in the fight against child sexual abuse.

The international and cross-border nature of the problem will be further developed in the report.

The problem analysis should explain why the present initiative **separates online abuse from offline abuse** and why this separation is desirable even though online and offline abuses can be closely linked and other legal acts (such as the CSA Directive) cover both. The introduction states that illegal content should be tackled as effectively online as it is offline (p. 2). To what extent is this content tackled less effectively online? It seems that many of the arguments regarding the unique capacity of online service providers to detect CSA material are valid for offline services, such as mail services, where no similar measures exist.

The commitment in the CSA strategy was "to propose in 2021 the necessary legislation to tackle child sexual abuse effectively, online and offline". The present initiative aims to address both spheres where the crime is committed by measures improving prevention and support to victims. In fact, the proposed title in the report of the possible legislative proposal is "Proposal for a Regulation of the European Parliament and of the Council on preventing and combatting the sexual abuse and sexual exploitation of children", without making any distinction between the online and offline aspects. These two aspects are indeed so closely linked that an explicit general separation is not desirable.

That said, the initiative focuses on the online aspects of the crime with relation to detection efforts. 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 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 much lower level and was not signalled as a common issue encountered by law enforcement in CSA investigations during stakeholder consultations.

It also needs to be noted that the internet allows for creation of communities in which offenders share materials and experiences. Therefore, this initiative addresses the online sphere, which enables and fuels abuse, with the aim of tackling the abuse both offline and online.

These clarifications will be added to the report.

This initiative targets both CSA material and grooming. The problem description should clarify which problems and problem drivers apply to each of these areas.

All problem drivers apply, to different degrees, to CSAM (both known and new) and grooming. This will be elaborated further in the report.

The report is not sufficiently clear whether the problems, particularly those related to the EU centre, involve predominantly coordination issues or also more operational prevention and victim support measures. It is also not clear enough on the kind of tasks currently performed by the Member States and on the issues, they cannot adequately deal with

alone.

The report highlights that, to the extent that tasks relating to the centre's functions are currently carried out by Member States, they are limited, lack coordination and are of unclear effectiveness. While Member States are obliged under the Child Sexual Abuse Directive to put in place programmes for prevention and assistance to victims, these provisions of the Directive have been among the most difficult for Member States to implement. The report also identifies the need for the development of a rigorous, evidence-based approach in these areas and mechanisms for the sharing of best practices. As such, the problems in the areas of prevention and victim assistance are not solely related to coordination, but also operational issues and issues regarding effectiveness. This will be further clarified in the report.

Four Member States (i.e. AT, DE, FR and NL) have already issued **national provisions**, which aim to regulate online service providers with regard to illegal content and acts online (annex 5). The report should provide evidence on how the existing measures have worked so far and which problematic cross-border issues have been observed. In particular, it should show that this national legislation would not be harmonised by the Digital Services Act, thus removing risks of legal fragmentation. It should point to the gaps and shortcomings of current measures that would warrant a policy change and better assess its impact.

OK, the report will include evidence on how the existing national measures have worked so far, to the extent that this evidence is available.

As regards the problem driver of **limited Member States efforts to prevent child sexual abuse and to assist victims** the report should explain and substantiate with evidence why Member States apparently have problems in "putting effective prevention programmes" in place and do not provide tailored and comprehensive assistance to victims. What is the evidence for "the duplication of efforts and the existence of gaps across Member States" (p.199). Why would structuring prevention at the EU level necessarily generate more effective national prevention programmes? Similarly, the report should demonstrate why the necessary coordination between 'health, legal, child protection, education and employment' for the assistance to victims is not best done at Member States level.

The monitoring of the implementation issues of the Child Sexual Abuse Directive indicates that Member States struggle in particular with the correct transposition of the articles of the Directive that relate to prevention programmes and assistance to victims (see p.8, "problem drivers" section). These transposition shortcomings contributed to launching infringement cases against 23 Member States. The six workshops supporting the implementation of the Directive organised by the Commission, and bilateral dialogue clarifying the remaining implementation issues with the Member States indicate the problems are linked to the lack of expertise in relevant areas, difficulties in communication and coordination between key actors, e.g. different ministries.

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 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.

Similarly, the Member States are in the best position to coordinate the practical efforts on assistance to victims, but some of them lack specific expertise on how to build sustainable victim support mechanisms. Research and evidence base to inform policy making is also

insufficient.

These clarifications will be added to the report.

If the situation on the ground differs across Member States, the report should provide a corresponding analysis. Stakeholder views (including those of public authorities) on these aspects should be an element of the evidence base.

OK, the report will be updated accordingly, and in coherence with the above comments.

More generally, **stakeholder views** reflected in the problem analysis should refer to the problems. At present, the paragraph on stakeholders on p.14 refers to their views on the policy measures.

OK, the report will be updated accordingly.

The report should also explain how the problem differs or not for CSA content on websites hosted outside the EU. The close relationship with the US NCMEC and its current importance for the EU combat against CSA deserves a more elaborate explanation (the future relations between the new EU centre and the NCMEC may continue to play a significant role).

OK, the report will be updated accordingly. Please see also comments on US and NCMEC in box 6.

The estimated costs resulting from CSA are based on a single US study. The robustness of the study result and its extrapolation to an EU context should be thoroughly assessed (please see comments on box 6).

OK, please see comments in box 6.

3. SUBSIDIARITY AND EU VALUE ADDED

3. Subsidiarity and EU value added
The report should justify the choice of the **legal basis**. In particular, it should explain why the legal basis (article 114 of the Treaty) would be different from the legal basis of the Child Sexual Abuse Directive (articles 82.2 and 83.1). If the approach of this report is mainly from the point of view of the internal market, then it should clarify and justify this. However, many of the envisaged measures (in particular, those envisaged for the EU centre) concern the coordination of CSA prevention, prosecution and victim support. While there seems overall a clear "fighting CSA crimes" narrative (as expressed in the general objective), a strong internal market dimension is less obvious for these tasks. Moreover, section 2.1.2 is confusing in this regard, as it refers to child sexual abuse as a "public health problem". The report's choice of the legal basis must be based upon the nature of the main or predominant objective and content. The report refers to **fragmentation and conflicts of law** but it fails to demonstrate how the current legal differences between Member States stand in the way of action that is more effective. The report should describe the practical consequences of the legal fragmentation in the combat against child sexual abuse. It should use as much as possible evidence from the four Member States that have already legislated CSA, taking into account the legal harmonisation resulting from the Digital Services Act. It needs to **demonstrate the cross-border aspects of the problems** to justify the need for EU action (develop this mainly in the problems analysis, see also box 2). It should explain (and possibly quantify) the compliance and operational costs from fragmentation (p.15). OK, an explanation for the legal basis and an overview of the fragmentation issues will be added to the report. While for some of the measures concerning service providers and transnational coordination the necessity for EU action seems more plausible, it is less clear when it comes to more operational prevention and victim support measures. The report states that "the centre would provide support on all types of prevention efforts" (p.195) without providing clear evidence on the need for all measures. Given the local dimension of prevention and victim support, the report needs to be much clearer on which tasks EU level support is necessary and cannot be provided by national authorities in a sufficiently effective and efficient manner. Information obtained in the process of monitoring the Child Sexual Abuse Directive and the stakeholder consultations, indicate that there is a need for a more structured approach to prevention. In particular, the difficulties in implementing Articles of the Directive relating to putting in place programmes for offenders and people who fear they may offends point to significant gaps in this area. Also, the feedback from stakeholders, in particular NGOs focused on child's rights, shows the need for improving awareness and education of children, parents, and caregivers. A more structured support from the EU could enable Member States to take more effective action at their level. EU level action can provide a forum for exchange of necessary expertise and best practices, to avoid duplication of efforts and blind spots. It can help the Member States with less advanced approach to prevention and victim support learn from experiences of the ones with successful initiatives. While some exchange in this area exists, the feedback from the network of expert on prevention, coordinated by the Commission, indicates there is a need for a structured framework for such exchanges, as

opposed to relying on professional contacts of individual researchers or officials. EU level action promoting and disseminating research would help to enrich the evidence base in both areas.

EU intervention could also include coordinated EU-wide campaigns, and practical support to local interventions, e.g. translations of existing materials, possibly leading to cost savings at Member State level.

4. OBJECTIVES AND INTERVENTION LOGIC

4. Objectives and intervention logic
The report should clarify the **intervention logic**. The link between the specific objectives and the problem drivers is not always obvious. This concerns objectives 2 and 3: how are inefficient public-private cooperation and insufficient voluntary action addressed by these two objectives? (e.g. the third objective refers to legal certainty, but the problem analysis has not clearly established legal uncertainty as a problem driver, it is rather mentioned as the consequence of certain problem drivers; similarly, lack of transparency is linked to missing means to measure the effectiveness of measures taken, but is not presented as a problem driver). The inefficient public-private cooperation and the insufficient voluntary action prevent addressing adequately some child sexual abuse crimes in the EU in two main ways: 1) By not being effective at combatting the crimes, i.e. by not detecting some crimes or by not being effective in dealing with those detected ("the what"). Specific objective 1 focuses on this issue. 2) By not tackling the crimes in a sufficiently transparent way that does not leave room for concerns on accountability, legality of the actions, and protection of fundamental rights of all users ("the how"). Specific objective 2 focuses on this issue. Concretely, in relation to legal certainty and transparency: • Lack of legal certainty has discouraged some service providers from taking voluntary action. This will be better explained in the report in problem driver 2 Also, the lack of legal certainty also limit the impact of hotlines' action. In particular, the memorandums of understanding with public authorities cannot provide the same legal certainty that legislative acts would. This will be better described in the report in problem driver 2, in the section on cooperation between public authorities and civil society organisations, (p. 10). • The lack of transparency is already presented as part of problem driver 1, in the section "Voluntary action lacks harmonised safeguards" (p. 13), given the importance of transparency as some of the voluntary measures may interfere with users' rights, including those to privacy and data protection.

5. BASELINE AND OPTIONS

5. Baseline and options

Baseline: the report should regroup the information on the baseline into one section; the information is now divided between sections 2.3, 5.1, 6.1.1, 6.1.2 and 6.1.3. The impacts of the policy options should be measured against the baseline (therefore the impact of the baseline should always be 0). Here again, the impact of the DSA should be fully integrated in the baseline. Moreover, the baseline should reflect the most likely scenario in the absence of the initiative, taking into account the likelihood that the interim derogation will be prolonged after three years if the present initiative would not go ahead.
 	
OK, the report will be updated accordingly.
 	
The methodological criteria to estimate CSA costs in the EU (p.18) based on an extrapolation of the US figures (p.7) deserve clarification (see comments in boxes 2 and 6).
 	
OK, please see comments in box 6.
 	
The report should explain the exact meaning of the **prohibition to impose 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 (article 15.1 of the e-commerce Directive). In how far does systematic looking for CSA via dedicated IT tools in online messages and online postings not constitute monitoring information which they transmit or store? How do we draw the line between general monitoring and targeted monitoring (section 5.1)?
 	
The exact meaning of the prohibition to impose a general monitoring obligation cannot be found in the eCommerce Directive or the DSA. The only indication of the extent of this prohibition can be found in the case law of the Court of Justice of the EU (CJEU). The CJEU has not yet provided a clear delineation between general and targeted/specific monitoring obligations either, but certain criteria have been indicated by the Court when deciding whether an obligation to monitor the information, which intermediary service providers transmit or store, or to actively seek facts or circumstances indicating illegal activity is to be considered general and thus prohibited. It has to be highlighted that so far the CJEU has only dealt with this issue concerning copyright infringement and defamation in specific cases in a given Member State. It has not yet had to assess a similar obligation with regard to illegal content such as child sexual abuse material and it has not yet had to consider the implications of such obligations on EU level.
 	
Based on the indication of the CJEU, the following elements can be identified:
 	
• It is not allowed to impose an obligation, which would cumulatively introduce (*see case C-360/10*):
  ○ 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;
  ○ a system for filtering most of the information to identify electronic files (stored on a provider's servers),
  ○ and subsequently block the exchanges of such files.

- Any monitoring obligation should ensure a fair balance between the affected fundamental rights (see cases C-360/10 and C-401/19).
- General monitoring for equivalent content is allowed under the following conditions (see case C-18/18 and joined cases C-682/18 and C-683/18):
  - *protection is not provided by means of an excessive obligation being imposed on the host provider;*
  - *the monitoring does not require the host provider to carry out an independent assessment of the illegality of the equivalent content (which should be essentially unchanged for the most part compared to the original illegal content).*
  - *A duty to prevent the removed content from being re-uploaded (notice and stay down), may also be permissible as long as the above conditions are met.*

As a matter of legal principle, secondary law (such as the eCommerce Directive or the DSA) can be derogated from if necessary and in a proportionate manner. However, a derogation is not allowed from primary law, being the Charter of Fundamental Rights. The principle is also reflected in the CJEU's case law, which seems to allow preventive monitoring obligations as long as those ensure a fair balance between the affected fundamental rights.

In light of the above, as long as the systematic detection of online child sexual abuse fulfils this condition of ensuring a fair balance between the affected fundamental rights, such detection should be in conformity with the general monitoring prohibition obligation.

The above clarifications will be added to the report.

Options on the EU centre

All the policy options include the **creation of an EU centre** (although in option A it would just be a kind of network). While for a number of envisaged tasks (e.g. coordination, operation of the data base) there seem some potential efficiency arguments, this is less clear when it comes to certain operational tasks in the area of prevention (see comments in box 3). The report should be more specific on the envisaged tasks for the centre.

OK, please see comments in box 3.

The report should elaborate the concept of **independence** of the European centre. It should better justify the need for independence, from whom and why the centre should be independent and how the quality and neutrality of the centre would be democratically controlled (assess the risk that the centre could shift in time its view on the trade-off between children's protection and internet users' privacy in one way or the other).

The centre will be a fundamental component of the part of the legislative initiative that deals with the detection and reporting of CSA online (p. 21, p. 50). It would serve as a key facilitator of the work of service providers in detecting and reporting the abuse, and of the work of law enforcement in receiving and investigating the reports from service providers. To be able to play this facilitator role, it is essential that the centre be independent:

- from service providers, as the centre would serve both as the source of reliable information about what constitutes CSAM, providing companies with the sets of indicators on the basis of which they should conduct the mandatory detection of CSAM, and as a control mechanism to help ensure transparency and accountability of service providers, including possibly helping to resolve

complaints from users; and

- from 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.

To ensure that the centre maintains this neutrality and this balanced consideration of all the relevant rights at stake, it will be subject to periodic reporting to the Commission and to the public. The Commission will further supervise the centre as part of its management board. This board would also ensure participation of all the relevant stakeholders representing the different interests and rights at issue (including both children's rights and internet users' privacy rights).

To ensure the centre's independence, in particular from potentially overriding private and political interests, the centre would be financially independent and receive a majority of its funding from the EU. This would entail an additional supervision by the European Court of Auditors.

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 above clarifications will be added to the report.

The options description should also clarify the distribution of tasks between the European centre and the Member States' authorities.

OK, the report will further clarify this.

The report needs to explain why the creation of such a centre has been retained as the sole solution to improve the coordination between Member States and why no other viable coordination solutions should be considered. Moreover, the presentation of a single legislative EU centre option in the main text is surprising given that the comprehensive screening and assessment of possible centre options in annex 10 has led to the identification of a number of *per se* feasible implementation choices with different costs and benefits. This analysis does not support (safely) excluding implementation forms B and C from the political decision-making (also in view of the political commitment taken in the CSA strategy to consider existing EU bodies such as Europol). In addition, the applied scoring methodology contains serious deficiencies, the correction of which may lead to a different ranking of the implementation options (see comments in box 7).

To make the report concise and readable, the intended purpose of annex 10 was indeed to comprehensibly screen and assess in detail all possible centre options, and determine the preferred one to be incorporated in the options of the report. This approach allowed to focus the report on the role that the centre plays addressing the problem and achieving the objectives (the "why of the centre") while annex 10 focuses on explaining the need for the centre, analysing the possible implementation forms, and determining the most suitable one ("the how").

That said the report does discuss implementation choices B and C as part of the discarded options (p. 26), as this is the result of the analysis in annex 10.

The commitment in the CSA strategy was "to explore the various implementation options,

including making use of existing structures for the centre's functions where appropriate" (p. 14). The strategy also states that "building on Europol's role and experience, the centre could work with law enforcement agencies in the EU and in third countries to ensure that victims are identified and assisted as soon as possible and that offenders are brought to justice."

Annex 10 fulfils the commitment in the strategy by carefully considering the various implementation options. Also, the report makes clear in p. 21 that, while being and independent entity, "the centre would work closely with the European Police Agency (Europol), the Fundamental Rights Agency (FRA) and the national hotlines to benefit to the extent possible from their expertise and resources".

Please see comments in box 7 regarding the scoring methodology.

The option of establishing the centre at Europol (which already plays an important role in fighting CSA), has been discarded on the basis of "impartiality" arguments, not being able to ensuring transparency and accountability given its current legal enforcement mission (p.258). However, it is not clear why this should not be possible. It is also not clear why expertise in prevention and assistance to victims cannot be added to Europol task portfolio (potentially based on an amended Europol mandate).

As indicated above, the centre will be a fundamental component of the part of the legislative initiative that deals with the detection and reporting of CSA online. It would serve as a key facilitator of the work of service providers in detecting and reporting 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 this facilitator role, it is essential that the centre be independent from service providers and from law enforcement (including Europol), so that:

- it can remain neutral 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 (including offenders);
- US based service providers (which are by far the most relevant service providers for this initiative), have indicated in the consultations that they are prohibited by law to work closely with law enforcement in a way that could make them "agents of the state" (Fourth Amendment to the US Constitution). 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; and
- users that feel that have been unfairly treated by service providers (e.g. if their content has been mistakenly removed and they feel that the service provider has not ensured a fair complaint procedure) can turn to a neutral entity, not directly linked to law enforcement, without fear of possible repercussions.

With regard to **prevention and assistance to victims**, these could in theory be added to Europol task portfolio through an amended Europol mandate where needed. In practice, however, this presents a number of drawbacks which reduce the interest and feasibility of this option compared to placing these functions in a separate entity, including:

- lack of (perceived) neutrality given its core law enforcement task: the centre would serve as a facilitator of exchanges of best practices and lessons learned in prevention and assistance to victims among all relevant parties. The core Europol activity would remain law enforcement, and this would create tensions with some relevant parties. For example, as indicated in the report (p. 26),

Europol's capacity to reach out to persons who fear that they might offend would be limited by the likely distrust that its core law enforcement task could generate among those people;

- 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 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). Being so different from Europol's core tasks, and given the significant capacity building efforts, there is a real risk that the functions of prevention and assistance to victims would be deprioritised from the core tasks, in particular given Europol's constant requests for additional budget for its core tasks. Being part of 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 (p. 27);
- risk of mission creep: it would be difficult to justify that Europol expands its mandate to cover prevention and assistance to victims only in the area of CSA. 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.

The above considerations will be added to the report.

As regards the currently preferred implementation option D it is not clear how the institutional setting of a foundation (or similar) would actually work, how transparency and accountability would be effectively achieved and how potential conflict of interests (by donors) would be eliminated from the beginning and on a lasting basis (for example, as a result of threats to reduce contributions).

Compared to the initial report provided to the Board, the preferred implementation choice for the Centre has been modified to a decentralised agency, to implement guidance from the Legal Service on the necessity of this legal form given the important role of the Centre in implementing EU legislation. The governance structure and legal framework of a decentralised agency would therefore apply, including all mechanisms for the elimination of conflict of interests.

- To ensure that the centre maintains this neutrality and this balanced consideration of all the relevant rights at stake, it will be subject to periodic reporting to the Commission and to the public.
- The Commission will further supervise the centre as part of its management board. The Centre would also ensure participation of and input from all the relevant stakeholders representing the different interests and rights at issue (including both children's rights and internet users' privacy rights).
- To ensure the centre's independence, it will be subject, like any decentralised agency, to scrutiny by the European Court of Auditors.
-

In view of the above the report should broaden the scope of implementation options presented and assessed in the main report. It should also look at scope alternatives to

reflect different degrees of ambition in terms of tasks covered by the centre. Stakeholder views may provide some orientation in this regard.

OK, elements of the analysis of the various implementation options for the centre in annex 10 will be incorporated in the report.

The report should explain how the European centre would exchange information with similar institutions worldwide (e.g. NCMEC) given the international character of the problems.

OK, the report will explain that the legal basis of the centre should allow it to cooperate closely with entities in the EU and beyond, in particular with regard to data exchanges (currently mentioned in annex 10, p. 199).

The report should clarify why an indefinite continuation of the interim derogation cannot be part of the options (if it is not part of the baseline), in particular in combination with option A (non-legislative measures).

An indefinite continuation of the interim derogation is one of the early discarded options The current reasoning to discard it will be expanded with an explicit reference to option A (non-legislative measures).

Annex 10 provides a detailed - IA alike - analysis of the options for a centre. It takes choice D "Set up an EU Centre to prevent and counter child sexual abuse as a separate organization" (p.293 annex 10) as preferred option; letters do however not correspond to the numbering used in the *overview of options for the EU Centre* (table 2, p.202 annex 10). More details of annex 10 (around the information summarised in tables 1 and 3) should feed the report.

The numbering used table 2 on p. 202 of the annex is used to list all possible options, including the ones discarded at an early stage, which could be considered to set up the centre. This numbering is not meant to correspond to the letters used to designate implementation choices retained for detailed analysis.

More details from annex 10 (around the information summarised in tables 1 and 3) will be included in the report.

This option also seems to contain legal provisions on the status of hotlines (p. 21). As the link with the centre is not evident, it seems that this should be part of a separate measure.

The report and annex 10 will further clarify the link between the centre and the hotlines. To coordinate and support the detection, reporting and removal of CSA online, the centre should be able to cooperate effectively not only with service providers but also with hotlines.

Options for service providers (B, C, D, E)

The mandatory detection options C, D and E make their application to **encrypted content** conditional upon the availability of the necessary technology. The report should clarify who would take the decision that the technology is sufficiently developed and that the screening would apply to encrypted content. It should also explain which "designated authority" would supervise these technologies (p.24). Would implementing regulation or certification have any role to play in this?

The legislation would determine in a clear and comprehensive way the minimum conditions and safeguards that the technology should meet before the mandatory detection of child sexual abuse online would apply also to encrypted content.

As the report indicates, whereas a proof of concept for technical solutions to detect CSA in encrypted systems has been delivered (see annex 9), the solutions are still under development to be deployed at scale.

The ultimate responsibility to comply with the requirements set out in the legislation would lie on the service provider. This includes not only the technological solution chosen but also the particularities of its deployment in the service provider's systems.

That said, to support the service provider in this process, the legislation could require it to consult both the data protection authorities, with regard to data protection issues, as well as the EU centre to prevent and combat CSA, with regard to the technical requirements other than data protection (e.g. security of the technology, i.e. vulnerability to be misused for other purposes than the fight against CSA). The consultations should take place prior to deploying the technology.

Beyond the prior consultations, both the data protection authorities and the EU centre could continue to supervise the respective data protection and other technical aspects during the deployment of the technology and during its continuous application.

The above clarifications will be added to the report.

How will safeguards be determined if technical solutions are still in the development phase (and likely to continuously evolve)?

This is a challenge faced by all legislation that seeks to be technology neutral, and it can be addressed in a number of ways. For the purposes of the present initiative, the legislation would determine in a clear and comprehensive way the minimum conditions and safeguards that should be met, regardless of the technical solution chosen. A similar approach was followed in, e.g., the data protection rules, which specify standards but take a technology-neutral approach, or in the interim regulation. Safeguards can be specific without pre-determining the choice of technology, e.g. in requiring human review where certain accuracy benchmarks are not met. They can also be adaptive, e.g. by requiring the use of state-of-the-art tools, meaning that providers may have to adapt their choice of tool to ensure that they make use of the tool that is most accurate, targeted, privacy-protective and secure. Independent certification and oversight are additional examples of safeguards that are not specific to any given technology.

In that way, the legislation would be not only technology neutral but also future-proof.

How will coherence with the Commission's horizontal work stream on encryption be ensured?

As stated in the report (p23), 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 CSA therefore cannot leave aside the question of encryption. This includes the legislative proposal under consideration.

The coherence with the Commission's horizontal work stream on encryption would be ensured as all the DGs participating in such process are also part of the inter-service group that will be assisting in the preparation of the legislative proposal. In particular, the ISG will ensure that the minimum conditions and safeguards that the technology should meet before the mandatory detection of child sexual abuse online would apply also to encrypted content are coherent with the purpose of the horizontal process. At the same time, the challenge here is significantly different from that of the horizontal work stream, which focuses on lawful and targeted access by law enforcement authorities, and encompasses any information, including ex-post. The present initiative will only require performing a "yes or no" check as to whether a specified image or video is being shared, or a specified pattern of grooming behaviour can be identified. In a further difference, the obligation is also open to technologies that can provide a response based on other, unencrypted data, as long as those are effective in making the determination.

Imposing the use of this technology already in the current initiative is not technology neutral (as claimed on p. 24) because not all technologies will be available at the same time. This obligation would require to use the first available technology.

The legislation would not impose a priori the use of any given technology and therefore it would be technology neutral. It is not possible to tell a priori whether at any point there will be only one technical solution that meet the criteria of the legislation or several, as multiple technical solutions could be deployed in parallel. Moreover, the deployment of a given technical solution would vary from service provider to service provider, depending on the particularities of each provider's systems. While a number of technologies have already been developed, further development is ongoing and would be expected to deliver before the obligation is in place, providing a range of choices to companies.

As annex 9 shows, all technologies that could be applied relatively fast raise privacy and security issues (overview table p. 187). Balancing the detection of CSAM against privacy and security issues should be fully analysed before taking the decision on the use of certain technologies. Such a decision cannot be taken, based on current knowledge.

As indicated above, the legislation would determine in a clear and comprehensive way the minimum conditions and safeguards that the technology should meet before the mandatory detection of child sexual abuse online would apply also to encrypted content. This includes conditions to ensure privacy and security. The data protection authorities would need to be consulted before a service provider deploys such technical solutions. In addition, the ex post supervision by national authorities will monitor correct deployment.

It is not clear whether the reporting of CSA content goes hand in hand with the **removal** of such content. The options description is currently vague on this. The report states that the centre would facilitate the removal and notify providers of content to be removed (p.29), that service providers are obliged to report but not to remove (p.32), that the centre would support victims in obtaining the removal of content (p.21), and that the decision on removal could remain within the purview of the service provider (p.23). The report should clearly state (for each option) who decides upon the removal of content.

The report will further clarify the considerations related to removal.

The report mentions that the general obligation to detect CSAM would happen 'in a manner consistent with the **prohibition of general monitoring** and active fact-finding'. The report should specify how this would be achieved.

We will add further explanations on this point. As also outlined on p. 4 above, the case

law of the Court of Justice of the EU (CJEU) has not yet provided a clear delineation between general and targeted/specific monitoring obligations. That said, certain criteria has been indicated by the Court when deciding whether a monitoring obligation is to be considered general and thus prohibited. Based on this indication, it can be discerned that as long as the preventive monitoring obligation ensures a fair balance between the affected fundamental rights, it can be reconciled with the general monitoring obligation prohibition. In that context, it is of particular importance that there be no obligation to proactively seek out any indicators of illegal activity, but rather to limit any obligation to specific content that is reliably identified. Providers should also not have to bear excessive costs when it comes to their ability to detect such specific content. The present initiative complies with these requirements in the following way:

For all detection obligations, the obligation will not apply horizontally but only on the basis of a targeted and specific detection order, issued by a national authority based on a risk assessment provided by the relevant service provider in its jurisdiction (similar to the approach in the Terrorist Content Online Regulation). Service providers will also not need to determine what is illegal by themselves but will receive guidance on how to determine illegality and on possible tools to deploy. In addition, it should be considered that the EU centre on prevention and assistance to victims would become a fundamental component of the legislation related to the detection and reporting of child sexual abuse online, as it would serve both as the source of reliable information about what constitutes CSAM (thus illegal material) and as a control mechanism to help ensure the effective implementation of the legislation (for ex.: sharing hashes of known material or specific indicators of new material [e.g. AI patterns/classifiers] that providers should use to detect).

Detection of known material: In addition to clear information on what is considered illegal content in the EU and tools to identify such content, the automated and anonymized nature of the tools and the above-mentioned safeguards combined with the low rate of false positives would ensure that the essence of users' fundamental rights would not be disproportionately affected. The low costs, the automated measures and their low level of intrusiveness would also ensure that the essence of providers' fundamental rights would not be affected either. Finally, removing CSAM can significantly help to protect several of the victims' fundamental rights, both when it comes to the possibility of an ongoing offline abuse and to the victimisation and privacy violation inherent in sharing the materials. Hence, this solution would ensure conformity with the prohibition of general monitoring obligations by proportionately and fairly balancing the rights of victims, users and providers.

Detection of new material: On one hand, this option would have a positive impact on victims of ongoing abuse and would significantly enhance the possibility of safeguarding them from additional abuse. In addition, the early detection and swift addition to the database of verified CSAM can limit the spreading of content across platforms and hence serve to protect victims' fundamental rights. On the other hand, this option would have a higher impact on the fundamental rights of users (which would be mitigated by mandatory human review) and on the providers by mandating them to put in place and maintain detection systems that require additional oversight. To mitigate this, once again, clear indicators and free and reliable tools would be made available. The EU centre would support SMEs in particular in providing independent human verification. To protect users, strict requirements would apply, including on the reliability of indicators. With the highlighted safeguards, a fair balance can be achieved in this option as well.

Detection of grooming: would have a positive impact on the fundamental rights of potential victims by contributing to the prevention of abuse since service providers are the

only entities able to detect such abuse. At the same time, this obligation would have the highest impact on the fundamental rights of users and providers, since it would involve searching text, including in inter-personal communications as the most important vector for grooming. The proposal would therefore specify detailed conditions and safeguards building on those already adopted in the interim derogation, plus the additional support and safeguards resulting from the creation of the EU Centre and its tasks. It would also contain specific requirements regarding the quality of data used to train algorithms and the standards for the objective determination of risk factors indicating possible grooming.

More generally, the report often mentions the need for possible **safeguards**, without specifying which ones would be part of the options and why.

The report refers to safeguards to ensure accuracy, transparency, protection of fundamental rights and accountability, including supervision by designated authorities (p. 19, p. 22). It also lists possible safeguards for the various options, notably those imposing mandatory detection of CSA online and which therefore present a higher potential interference with fundamental rights:

- under option C (p. 23): "Safeguards 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.";
- under option D (p. 24): "In addition to the safeguards in option C, this option would include others regarding the quality of data used to train algorithms, and mechanisms such as mandatory human review to further increase the accuracy of the detection process.";
- under option E (p. 25): "In addition to the safeguards in option C, this option would include others regarding the targeting of specific services where children are at risk, the quality of data used to train algorithms, mechanisms such as mandatory human review to further increase the accuracy of the detection process, and requirements for the objective determination of risk factors indicating possible grooming.".

The report purposely uses open language when referring to the safeguards to not condition the legislative drafting, where those safeguards will be spelled out in detail. Instead, it refers to "possible" safeguards, and focuses on the purposes and reasons why the safeguards are needed (i.e. to ensure transparency, accountability, etc).

The report is also not clear on which exemptions are foreseen for **SMEs** under the various options. The impact analysis mentions that for smaller companies the human "verification could be left to the expertise of the EU Centre" (p.36, p.44). The SME test indicates that (certain?) "obligatory measures will not apply to SMEs, which offer services that are predominantly or exclusively used by adults" (p.303). The report should clearly identify upfront the envisaged exemption measures and subsequently assess the resulting impacts (see below in box 6). Moreover, there seems no dedicated analysis on the (additional) costs resulting for the EU centre from taking over the human verification for SMEs.

OK, annex 11 will be reviewed to state upfront the exemptions foreseen for SMEs under the various options and then assess the resulting impacts.

The costs resulting for the EU centre from taking over the human verification for SMEs

are already included in the staff costs. The volume of CSA online originating from SMEs is expected to be relatively small compared to that of the larger service providers, and it could be covered as part of the centre tasks to review reports from service providers (in particular those containing new CSAM, which would require systematic human review).

This will be clarified in the report.

6. IMPACTS

6. Impacts
While the report has made an effort to quantify compliance costs for the obliged service providers and costs for public authorities, the quantification of the benefits seems to rely on a single US study. There is no assessment of the robustness of the study and no information on whether it has been peer reviewed and can be safely extrapolated to an EU context. As the estimates derived from this study are critical for the identification of the preferred measures and the assessment of their proportionality the report should make an additional effort to explore whether there is other research confirming the assumptions and methodology behind the study. Alternatively, an expert review could be envisaged to reduce the uncertainty around the reliability of the estimated benefits. In any event, the report needs to provide greater clarity on how the annual benefits number of EUR 7.5 billion has been estimated and how this has led to the option specific benefit calculations provided in tables 7, 11 and 24. The quantification of benefits is estimated based on a single US study because no similar study relating to the EU, the European region or to particular Member States is known to have been published. While other studies relating to several countries have been published (most frequently the US), the study by LeTourneau et al. is the most recent, is peer reviewed and comprehensive. There is some evidence that economic costs as a result of violence against children in high-income countries are similar from one country to another. The report and annex 4 will be updated to: 1) clarify that the study cited has been peer reviewed; 2) provide a more detailed summary of the methodology of the study; 3) clarify that the use of US data in the context of approximating the cost in the EU can be justified. The lack of EU-specific studies is an important gap in knowledge in the fight against child sexual abuse in the EU. Such studies should be undertaken, and would fit in well with the **Centre's role in funding and supporting research** under both its prevention and assistance to victims functions. The report should better assess **trade-offs**, e.g. detection vs data protection and privacy. It should present sound arguments on the balance to be found between circumvention of data protection and privacy to protect children. The proposed options also address interpersonal communications: the report should elaborate on the level of intrusiveness into fundamental rights (privacy, data protection, freedom of expression) of the tools used to detect the different forms of CSAM – known or unknown – and grooming (p.33 acknowledges the higher invasiveness of text analysis tools). The risk of misusing the tools for purposes other than the fight against CSA should also be assessed (p.23 annex 2). The report describes (e.g. pages 37 to 39, and throughout section 6.1.3. on fundamental rights impact) the various fundamental rights at stake. The balance cannot be presented as one between circumvention of data protection and privacy on one hand and protection of children on the other because the sharing of images and videos of children being abused represent a gross violation of their rights to privacy and data protection. The report will further elaborate on the level of intrusiveness of the detection of the different forms of CSA online (known and new CSAM and grooming), as well as on the risk of misusing tools for purposes other than the fight against CSA.

Technical solutions that could allow the detection of child sexual abuse while offering a level of privacy similar to end-to-end encryption are described in annex 8. However, the report leaves the choice open as an analysis of technical solutions to ensure a high level of privacy while dealing with CSAM in encrypted environments would have to be made in the ongoing horizontal process on encryption. The fundamental rights impact regarding the preservation of data protection and privacy is therefore incomplete, as ascertained on page 31 "Solutions would therefore need to be carefully considered".

As indicated above, the legislation would determine in a clear and comprehensive way the minimum conditions and safeguards that the technology should meet before the mandatory detection of child sexual abuse online would apply also to encrypted content. This includes conditions to ensure privacy and security. The horizontal process has a different objective, as it seeks to ensure law enforcement access to any kind of information, rather than a check as to whether CSAM is being exchanged or grooming is taking place.

The above clarifications will be added to the report, and the fundamental rights impact will be updated accordingly.

The report acknowledges that **companies** will have to face costs in technological developments or acquisition and maintenance, infrastructure expenditure and expert staff recruitment and training and that **SMEs** will be particularly affected (p.34). However, the SME test in annex 11 fails to fully consider the risk of creating barriers for newcomers and favour big platforms. Mitigating measures such as the provision of the detection tools for free are foreseen (p.302, annex 11), but these do not provide a full solution. In particular, they would not remove the need for SMEs to conduct human review on the detection of new CBAM (options D and E) and grooming (option E). This implies high costs, which would seem to constitute a significant entry hurdle. The report should consider mitigation measures for this area, as well.

The report indicates that for smaller companies the human "verification could be left to the expertise of the EU Centre" (p.36, p. 37, p.42). This mitigating measure will also be indicated in the SME test (annex 11).

In addition, the report should strengthen the analysis of potential impacts on SMEs. It should quantify the costs (or explain why this is not possible), elaborate on possible barriers to entry and further develop the assessment of alternative mechanisms and mitigating measures including the pros and cons of introducing a voluntary vs a mandatory approach.

OK, cost estimates for SMEs will be added to annex 11, as well as further details on barriers to entry and mitigating measures.

In the same vein, the report should identify potential conflict of laws between US and EU emerging from detection and reporting obligations (p.25 and the interest of this file in US – the majority of contributions to the IIA i.e. 11 out of 41 (27%), came from US) and indicate how stakeholders' views on this issue have been taken into account.

The report contains a reference to the possible obligations for US service providers to make reports both in the EU and in the US (p. 46). Rather than a "conflict of laws", these reporting obligations could lead to reporting to both the EU centre and NCMEC, its counterpart in the US. The report states that technical (IT) solutions would need to be implemented to ensure that there is no duplication of reports received by law enforcement

agencies in the EU.

Some stakeholders suggested that, in order to avoid duplication of reporting, any obligation to report to an EU organisation should include an exemption for providers which already report to NCMEC. This exemption would have several negative consequences, notably:

- a major increase in the volume of reporting to NCMEC, a US organisation, with major financial and operational consequences, as a result of EU legislation requiring mandatory detection; and
- the processing of large volumes of EU user data outside the EU, by an entity not bound by EU law.

The report will be updated to incorporate the considerations above, indicating how stakeholders' views have been taken into account.

The report should assess the burden for businesses and public administration, and include an overview table of these estimates. It should also consider the impact on the measures that have already been introduced by some Member States.

The burden for businesses and public administration under each of the retained policy measures is currently summarised in the second table of annex 3 (p. 54), with detailed analysis presented in annex 4. If needed, a summary table with the burden for business and public administration under the preferred option could be added to the main report.

The impact on the measures that have already been introduced by some Member States will be added to the report to the extent that this information is already available.

The summary table in annex 3 should distinguish between administrative costs and other costs.

The summary table will be revised to divide the rows for each measure between administrative costs and other costs, retaining the current division of columns (one-off and recurring costs for citizens, businesses and administrations).

The report should clarify why options (e.g. A, p.29 or B, p.30) not addressing the problem drivers have been retained.

In line with the requirements to ensure proportionality, and that any proposed EU action goes only as far as necessary, the options assessed in the report take a graduated approach, with an increasing level of obligations and intrusiveness. It is only after a detailed analysis of these options that it is possible to determine those that better address the problem drivers while ensuring necessity and proportionality.

The above clarifications will be added to the report.

The report should be clear about the analytical methods, data sources, underlying assumptions as well as uncertainties and limitations of the analysis. In particular:

While many assumptions are justified, there are several assumptions – key to the quantified results – that are not explained. The report should provide justification for all assumptions, in particular the assumption which determines the number of companies in scope (footnote 122).

OK, the report will provide justification for the assumptions made to determine the

number of companies in scope, given the limitations imposed by the lack of available data.

Apart from the issues regarding the data sources mentioned in boxes 2 and 5, the report should provide more precise references from relevant annexes. While there are many references, these are not sufficiently precise to be helpful. The report should be self-standing.

OK, the report will be reviewed to include more precise references from relevant annexes.

The summary of costs and benefits provided in Tables 2 and 3 in p.44 of the report does not seem to match with the figures given in Table II of Section 2 of annex 3 (p.54) and are not to be found in annex 4. Clear reference to their source in annex 4 should be provided.

The figures given in Table II of Section 2 of annex 3 are the same as those appearing in Table 2 on p44 of the report. The figures in Table 3 on p44 are calculated by adding the relevant measures under each option. Annex 4 will be updated to show the calculations and the report will be updated to more clearly explain the calculations and refer to their source in annex 4.

As mentioned, the report should explain how the benefits have been estimated, how robust the estimates are and whether the figures provided (table 4, p.45 + table 24, p.108 of annex 4) are based on an extrapolation of US data (7.5 bn EUR).

OK, as mentioned above, the report and annex 4 will be updated with those clarifications.

The source of figures and estimates in the quantitative analysis (annex 4, section 3, p.83) should be validated with other sources such as dedicated studies undertaken by the EP Research Service (pp.6-7 annex 1).

Many of the figures and estimates used for the quantitative analysis are outside the scope of sources such as the dedicated study of the EP Research Service listed in the bibliography. Additional efforts will be made to try to find sources that cover a similar scope as the quantitative analysis, and which could help as references to validate the assumptions made. Where possible, the quantitative analysis uses data from highly reliable sources, such as historic data from NCMEC, which is used to estimate the potential number of reports in the future, and data from Eurostat.

As regards the 25% staffing costs top-up relating to staff wellbeing, the report should explain whether this in line with the best practice in other serious crime areas (e.g. terrorism) and at national level (p.274, annex 10).

Several organisations active in the fight against child sexual abuse at EU and national level (e.g. law enforcement agencies, hotlines and other civil society organisations) provide dedicated support for the well-being of personnel, in particular to those employees who are required to view CSAM. Similarly, there is a recognised need for such support for content moderators in industry. Best practice in relation to staff wellbeing in other serious crime areas such as terrorism will be explored further and incorporated to the report where relevant.

7. COMPARISON OF OPTIONS AND PROPORTIONALITY

7. Comparison of options and proportionality

The comparison of options does not comply with the standard assessment criteria. The coherence criterion is missing, which seems problematic given the horizontal policies on encryption, the digital single market policies and the potential conflict with US obligations (p.46). Protection of fundamental rights has been identified as a specific objective and should thus be part of the effectiveness assessment and comparison (along the other specific objectives) and not a self-standing criterion. It is also not clear why a separate comparison criterion on international relations has been added. It seems more appropriate to assess also this aspect as part of the effectiveness analysis (even though it was not developed as a key issue in the problem definition and no specific objective is clearly linked to it).

The section on the comparison of the options should provide detail on the methodology chosen to rank the different options and an explanation for given scores. More specific comments:

- Annex 10 indicates that all criteria were given the same weight in the assessment of the options for a centre (p.284). However, neither the report (p.45) nor annex 4 provide information about how the various criteria weighed to calculate rankings.

  OK, this information will be added to the report and annex 4.

- The baseline score should be "0". According to scores in table 5, options A and B turn to be "cheaper" than the baseline; however the narrative contradicts this as it indicates that except for the baseline, all options would generate some additional administrative costs (p.47).

  OK, the scoring system will be adjusted to reflect a score of 0 for the baseline option and the narrative will be revised and adjusted accordingly.

- On effectiveness, it is not clear why options E and D score so much higher compared to C, though the estimated decrease in child sexual abuse (30% vs 25%) is quite similar.

  Whereas option C imposes obligations to detect only known CSAM, options D and E, impose additional, cumulative obligations to detect new CSAM and grooming. As described in Section 6.1.1, the detection of new CSAM and grooming, by their nature, provide much greater added value in terms of the ability to identify and rescue children from ongoing or imminent abuse. As such, the positive social impact under options D and E is considered to be higher than option C.

- On efficiency, it is not clear why options C and D receive a very similar score, though the costs for service providers are more than twice as high for D and also substantially higher for public authorities (see table 3). It is also not clear why options A and B receive positive scoring when the narrative (p.47) and table 3 indicate additional costs.

  OK, the scoring on efficiency will be reviewed and updated accordingly to ensure better consistency with the rest of the analysis.

- On international relations, it is not clear what justifies the remarkable difference in the

scoring between options C and D/E.

Options D and E have been scored higher on international relations as the measures under those options are anticipated to have significant benefits for third countries. In particular, the mandatory detection of new CSAM (options D and E) and of grooming (option E) are expected to lead to a significant increase in the number of reports of these types. 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 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).

A more consistent and refocused set of assessment criteria should allow a more balanced comparison based on the three standard criteria (including in table 5). The annex 4 tables should be amended accordingly (including as to the baseline point above).

OK, the assessment criteria will be revised as described above, and will be reflected in relevant sections of the report and annexes.

The report should also provide more information on the quantitative comparison of options (section 7.2). It should explain the analytical method (e.g. are the costs and benefits discounted?) and be clear on what categories of costs and benefits are included in the figures (e.g. are the costs of establishing the EU centre included?). “Total (savings)” in table 7 should be rephrased into “Total (net benefit)”.

OK, additional information on the analytical method and categories of cost and benefits will be added to the report, and “savings” will the rephrased to “net benefit”.

The report should better explain the choice of the **preferred option** and provide details of what it entails e.g. choice of centre type as per annex 10. Although option C appears to have the highest net benefit (Table 7, p.49), why is option D chosen if it scores worse and goes beyond? Should this choice not left to the political decision maker?

The report aims to provide a fair assessment of the identified policy options, and to finally make a **recommendation** as to the preferred option, having regard to the ability of the option to address the problem drivers, as well as the associated costs and impacts in other areas such as fundamental rights. The final policy choice is left to the political decision maker.

As shown in Table 7, option C appears to have the highest net benefit in purely monetary terms. Importantly, as described in sections 6.2 and 7.2.2, the quantitative assessment is limited by a lack of data and should not be interpreted as accurate estimates. Although option C would have a higher net economic benefit than option D, the overall benefits for option C are still expected to be significantly lower than under option D, as shown in the same table (i.e. €18.8b, vs €22.5b). In addition, as set out in the qualitative comparison in section 7.1, option D has the highest overall qualitative score.

The report should also consider how the preferred option would be coherent with ongoing initiatives in the cyber security area. This should include inter alia references to the Digital Services Act, which aims to regulate online intermediaries and service providers.

OK, reflections on coherence with ongoing initiatives in the cybersercurity area and in particular the Digital Services Act will be added to section 8 on the preferred option.

Comparison of EU centre options

The comparison of the four forms of implementation options in annex 10 contains a number of important shortcomings, which question the selection of the preferred option.

The criteria used to compare the centre implementation options are not sufficiently clear and partly missing (e.g. coherence). It is not clear why financial and administrative costs are not part of the efficiency considerations. On the usefulness of fundamental rights as comparison criteria see the comments above.

The methodology used to attribute benefit scores to the implementation choices reported in table 11 (p.283) is not transparently explained and its application raises a number of serious concerns:

- The baseline should always score "0". It is striking that option "O" receives in the summary table on p.285 always a "-3" for all assessment criteria, even for the "economic impact", where it has according to table 10 no costs.

  OK, the baseline score will be changed to 0 in all cases. Since the scores are used to carry out a comparison among the various options, this does not change the differences in scoring among the various options.

- It is not clear which part of the overall benefits is attributed to the centre and which to the mandatory obligation options for service providers (see comments above). How have the qualitative social impact scores been determined?

  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. Additional clarifications will be added to report to indicate how each particular score was determined, based on the above considerations.

  Please see above comments in main issue for discussion #4 in relation to the origin of the overall benefits.

- Why is it assumed that option D (with a score of 3) is 200% more effective in decreasing CSA costs when compared to the Europol option B (with a score of 1)? What is the supporting evidence for this finding?

  As described above, the effectiveness/social impact criterion concerns how effectively the various implementation options 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.

  Whereas Europol (regardless of the implementation option) will play a key role in the follow up to the detection and reporting of child sexual abuse online by service providers, its ability to contribute to prevention and assistance to victims would be limited, as discussed above and in various parts of the report and annexes. An

independent entity would not have these limitations, and therefore its effectiveness/social impact are likely to be higher.

- How can the efficiency of option D be so positively assessed in the absence of sufficient operational and institutional details (including the possible statute of its employees) for this option?

When it comes to fundamental rights, it is striking that the effectiveness scoring in ensuring security and victim protection for option A remains pretty low while reaching the same score for fundamental rights as option B despite the fact that under the latter option the estimated decrease of crime is twice as high.

Since option A will focus on prevention and assistance to victims through practical measures, the interference with fundamental rights would be limited. At the same time, its effectiveness/social impact is comparatively lower.

Option B includes the function of supporting detection and reporting of CSA online, and therefore its effectiveness/social impact is higher. The fundamental rights impact is positive but not as high as that of the independent entity given the limitations of Europol to act as an independent and neutral facilitator of the process to detect, report and remove child sexual abuse online (see comments in box 5).

As regards the Europol options, it is not clear why coordination of necessary prevention and victim support measures (including swift removal of victims' images from the internet) cannot be effectively established. Why would the build-up of non-law enforcement expertise (possibly based on an amended mandate) be more challenging than for a new body? What are the doubts on its capacity to ensure transparency and accountability given its track record as a public body? What are the stakeholder views on Europol's stated "perception of partiality" (p.262)?

Please see comments on Europol with regard to prevention and victims' assistance roles, as well as the perception of impartiality in box 5. More information on related stakeholder views will be added to the report.

8. FUTURE MONITORING AND EVALUATION

8. Future monitoring and evaluation
The monitoring system entails a large number of indicators. Some criteria for success (e.g. level of satisfaction of assisted victims, number of reports, feedback on reports, etc. p.52) are envisaged to measure it. The future evaluation should also check whether risks in terms of data protection and privacy have realised. Indeed, the data protection and privacy aspects will be a key component of the future evaluation. The corresponding article in the legislative proposal will explicitly refer to it.

9. CONSULTATION, INFORMATION BASE AND METHODOLOGY

9. Consultation, information base and methodology
The report should improve the presentation of stakeholder consultation in annex 2. The annex records the feedback on the inception impact assessment (41 contributions, p.25). However, the details of the Public consultation and reference to its 603 contributions are only available in Section 2 of this annex. Why is this information not also in Section 1.1.2? OK, that information will also be included in section 1.1.2. Moreover, the granularity of the assessment of the Public consultation, a factual summary report and statistical information are not included except in footnotes. OK, this information will be added to annex 2. Furthermore, the report should explain why the duration of the Public consultation was reduced to 8 weeks (p.9 annex 2). OK, the report will explain why the consultation had to be reduced to 8 weeks due to timing constraints and how this was still a reasonable period given the multiple relevant consultations that had already taken place in the previous 8 months. Stakeholder views, including from targeted consultation, should be presented in a transparent way throughout the report and especially in the analysis of impacts and the selection of the preferred option. It should be clear who has said what, and how concerns have been taken into account, in particular where views by category of stakeholders differ (e.g. general public does not agree, annex 2, p.16; mandatory vs voluntary detection, pp.25-26). OK, the report will be revised to ensure that stakeholders' views are presented also in the analysis of impacts and the selection of the preferred option. The information provided in boxes in the report should be supported by figures in annex 2 (e.g. views on the EU centre on p.22). OK, figures will be added, supporting the information provided in boxes. Annex 2 aggregates majority views and disregards alternatives advocated by minority groups. Moreover, not all views recorded as percentages add up (e.g. p.20, p.24 of annex 2). OK, annex 2 will be reviewed to ensure higher granularity in the presentation of the different views, and to ensure that all percentages add up. Intergovernmental organisations have been considered among key stakeholders. A 2nd targeted survey aimed at gathering "Data regarding reports of child sexual abuse online received by law enforcement authorities" provided details about e.g. content of the report. In view of the fact that NCMEC produces most reports for EU (p.31 annex 2), a dedicated meeting took place with experts from this US center in March 2021 (p.43 annex 2). Have NCMEC experts contributed to the other consultation activities? Yes, NCMEC contributed to the inception impact assessment consultation (29 December

2020). In addition to the meeting in March, there has been continuous bilateral exchanges before and during the preparation of the impact assessment, as NCMEC is a key source of data and a key stakeholder in the fight against child sexual abuse online.

The report refers on p.37 to views regarding economic impacts shared in the inception impact assessment. Has none of the 603 contributions to the Public consultation addressed this kind of impact?

As indicated in annex 11, some of the respondents to the open public consultation expressed their concerns regarding the economic impact for small and medium-size companies. It was further highlighted that specific care should be taken not to impose excessive costs and technical burdens on SMEs and smaller operators. A 'one-size-fits-all' solution should be avoided. The contributions will be reviewed again in case there were other references to economic impacts.

10. PRESENTATION

10. Presentation
The report is well-structured and contains required elements and annexes. It provides a wealth of information, generally well documented. However, basic terms are not clearly explained (e.g. difference between "CSA content"-"online content"- CSAM, hashing systems, grooming, hotline, etc.). The report should provide clear definitions, in particular of what Child sexual abuse online is. In view of the number of technical terms, the report would benefit from a glossary. OK, a glossary will be added, explaining upfront those technical terms and acronyms. If used, **acronyms** should be spelled out the first time they are used (e.g. APIs p.34 – spelled out on page "Application Programming Interfaces" on page 54 annex 4, end-to-end encryption (E2EE) on p. 12). The report should also replace or explain certain specific **jargon** that is not necessarily understood by the non-expert reader, such as "actionable" (p.10), "trusted flagger programmes" and "common hashing systems" (p.11). "Hash" is explained in footnote 95 but the reader needs to reach page 41 of the report to understand. Given the technical nature of online elements of the initiative, it is advisable to undertake a language check with the aim of ensuring sufficiently plain and accessible language. It also merits a review along the Commission style guide (e.g. 528k images, p.5). OK, the report will be revised to ensure that all acronyms are spelled out the first time they are used and to ensure that the language is further plain and accessible, and along the Commission style guide. The report could do without annex 7 as the usefulness of its detail in an analytical document is questionable. During the consultations, and in particular during the 8 months of inter-institutional negotiations for the interim derogation, it became clear that a number of stakeholders were not aware of evidence that showed that the efforts by service providers to detect child sexual abuse online led to tangible results, including victims safeguarded and offenders arrested. This led to a questioning of efforts by service providers to detect these crimes in their systems. The cases compiled in annex 7, resulting from months of work with law enforcement authorities across the EU (since this data is not systematically gathered), aim to provide that important evidence. The actual cases therefore appear to be of key relevance as part of the evidence-base for the preparation of this legislative proposal, which precisely addresses the detection and reporting of CSA by service providers. The executive summary should reflect any changes made to the main report. OK, the executive summary will be reviewed to ensure that it reflects any changes made to the main report.