Comments of the services of the Commission on some elements of the Joint Opinion of the European Data Protection Supervisor and the European Data Protection Board (EDPS-EDPB) on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Council Law Enforcement Working Party (LEWP)

This non-paper prepared by the Commission's services aims to provide explanations with regard to the proposal for a Regulation on preventing and combating child sexual abuse.
This non-paper is based on the relevant Commission proposal and does not present any new positions with regard to that proposal.

1. BACKGROUND

On 11 May 2022, the European Commission published a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (the 'proposal')[1]. In line with Article 42(2) of Regulation (EU) 2018/1725[2], the Commission requested a Joint EDPB/EDPS Opinion on the proposal.

The Joint EDPB/EDPS Opinion on the proposal (the 'Joint Opinion') was adopted on 28 July 2022. While supporting the goals and intentions behind the proposal, the Joint Opinion expresses serious concerns about its impact on individuals' privacy and personal data.

In response, the following sections provide further details on certain aspects.

2. BALANCING ALL RIGHTS

The need to balance all the fundamental rights at stake is at the core of the legislative proposal. When it comes to preventing and combating child sexual abuse online, these fundamental rights are, notably:

- the right to physical and mental integrity of children (Article 3 of the EU Charter of Fundamental Rights (the 'Charter')), the prohibition of torture and inhuman and degrading treatment (Article 4 Charter), their right to such protection and care as is necessary for their well-being (Article 24 Charter), their right to respect for their private and family life (Article 7 EU Charter) as well as to protection of their personal data (Article 8 Charter);
- the right to respect for private and family life (Article 7 Charter), to protection of personal data (Article 8 Charter), and the freedom of expression (Article 11 Charter) of the other users of the online services concerned;
- the freedom to conduct a business (Article 16 Charter) of the online service providers that fall within the scope of the proposal.

The Joint Opinion acknowledges (point 10) that, in the context of the measures set out in the proposal, not only the fundamental rights of the users are at stake, but also those of the children, including the positive obligations of relevant public parties to protect the children's rights recognised by the Court of Justice, among which is children's right to privacy[3].

Under the case law of the Court of Justice, the seriousness of the reasons to limit the exercise of fundamental rights determines not only *whether* there can be such a limitation (justification), but also *to what extent* such a limitation can take place (proportionality)[4]. In other words, the aim of combating particularly serious crime and protecting children against

1 COM(2022) 209 final.
2 OJ [2018] L 295/39.
3 Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126-128.
4 E.g. Case C-817/19, *EU PNR*, para. 115-116.

particularly serious interferences with their fundamental rights is key for the proportionality assessment.

Children are a particularly vulnerable category of persons, and the violation of their right to privacy and other rights through the dissemination of child sexual abuse material online is grave and known to have lifelong consequences for the victims. Moreover, tackling the solicitation of children ('grooming') is especially important given that it can help prevent such particularly serious violations of children's rights from taking place.

In light of this, the proportionality assessment of the detection obligation should take account of:

- on the one hand, the limitation of privacy of a larger group of online users which may result from a *judicial* or *independent administrative order* issued based on an assessment of necessity and proportionality – including the balancing of all fundamental rights at stake - to counter a significant risk of child sexual abuse on the service;
- on the other hand, the violation of the privacy of a smaller but particularly vulnerable group of users (i.e. children), who have the right to such protection and care as necessary for their wellbeing according to the EU Charter;
- as well as the significant impact of that violation on the long-term wellbeing of the child victim;
- and also the fundamental rights of service providers (freedom to conduct business). These are particularly important with respect to the determination of measures to be taken, according to the case law of the Court of Justice[5]. The Joint Opinion (e.g. in points 27 and 36) expresses reservations on the use of open-ended terms such as 'significant risk' or service used 'to an appreciable extent' for the purpose of online child sexual abuse, arguing that these might compromise legal certainty. In this respect, it should be borne in mind, however, that Article 16 of the Charter can make it necessary to use open-ended terms, as this allows the service providers to determine the specific measures to be taken in order to achieve the result sought. The Court has also recognised the need to keep pace with changing circumstances as a valid reason for using open-ended terms[6].

3. NO GENERAL AND INDISCRIMINATE OBLIGATIONS

The Joint Opinion suggests that the detection orders to be issued under the proposal entail measures that are general and indiscriminate in nature (see e.g. points 12, 53 and 55). In this context, the following elements should be considered:

1) The obligations are *order-based*. Detection of both (known and new) child sexual abuse material ('CSAM') and grooming can only take place based on a specific order issued by judicial or independent administrative authorities, relating to an individual case of a service falling within the scope of the proposal that is at a significant risk of being abused for the transmission of CSAM.

2) The obligations are *risk-based*. Detection orders are issued based on an individualised assessment for the service in question of the level of risk of specific types of online child sexual abuse occurring on a specific service. They can be issued only where there is a significant risk of the service in question being misused for the criminal activities in question. Moreover, prior to the possible issuance of a detection order, other mitigation measures have to be considered, including where applicable the ones that have been considered and

5 E.g. Case C-401/19, *Poland v EP and Council*, para. 75.

6 Ibid, para. 74.

implemented based on the Regulation (EU) 2022/2065[7] ('DSA'). An order can be issued only once mitigation measures have been determined to be insufficient to lower the risk in question sufficiently.

3) The obligations are *targeted*. The proposal contains an express requirement, whenever possible, to target and specify the obligations as much as possible, inter alia by focusing only on a relevant part or component of the service. Moreover, the detection obligation can only be imposed in respect of a narrow group of (particularly serious) criminal offences, namely, the dissemination of 'known' or 'new' child sexual abuse material as well as grooming. By extension, only some particular aspects of the communications concerned are affected, such as only material constituting child pornography or pornographic performance – meaning in practice: photos and videos – in relation to the dissemination of 'known' and 'new' child sexual abuse material. To note in this respect the role of the EU Centre, which manages and provides a list of indicators concerning the targeting of communications, in accordance with strict requirements set out in law. Furthermore, in respect of grooming, the detection orders concern exclusively communications where one of the users is a child.

4) Fourth, the obligations are *time-limited*. They apply only for a predetermined, limited period of time. And even during that limited period, reporting and review obligations also apply, which could lead to adjustments where necessary.

5) Finally, the obligations are *graduated* in function of the nature of the activities and the risks for the fundamental rights at stake. For instance, what constitutes a 'significant risk' justifying the issuance of a detection order varies depending on whether the obligation in question aims to combat the dissemination of 'known' child sexual abuse material, the dissemination of 'new' child sexual abuse material or grooming.

Rather than entailing obligations that are general and indiscriminate in nature, the detection obligations that may be issued in individual cases under the proposal are better compared with forms of targeted obligations of the type that the Court of Justice did deem permissible in the context of its data retention case law. In that case law, it clarified that such targeted obligations could, inter alia, affect certain geographical areas objectively considered to be at risk[8]. Rather than relating to a geographic space, in this case it concerns a specific 'online space' objectively considered to be at risk.

4. COMPLIANCE WITH THE CHARTER

It is settled case law of the Court of Justice that the fundamental rights to respect for private and family life (Article 7 of the Charter) and to protection of personal data (Article 8 of the Charter) are not absolute, but must be considered in relation to their function in society[9].

Pursuant to Article 52(1) of the Charter, the exercise of these fundamental rights may be limited, provided the limitation:

- is provided for by law (the proposed regulation will be a legislative instrument);
- is justified by an objective of general interest recognised by the EU or to protect the rights and freedoms of others;
- respects the essence of the rights in question;

[7] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[8] See e.g. Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 144-150. See also Joined Cases C-793/19 and C-794/19, *SpaceNet*, para. 112.

[9] E.g. ibid, para. 120 ; Case C-817/19, *EU PNR*, para. 112.

- is proportionate, in that it is *suitable and necessary* to achieve the objective pursued and corresponds to the *least intrusive means* available to reach it and if the risks to the fundamental rights do not outweigh the benefits of the measure.

In the view of the Commission services, there are good grounds to conclude that the proposal meets all of these criteria.

1) Justification

It is common ground that combating crime can justify limitations to the exercise of the fundamental rights contained in Articles 7 and 8 of the Charter[10]. That holds true all the more in respect of criminal offences that the Court of Justice has acknowledged to be 'particularly serious'[11]. In addition, as explained above, the proposed detection measures are also justified in view of the need to protect the fundamental rights of the children.

Indeed, the Court of Justice has acknowledged that precisely this need to protect minors gives rise to *positive* obligations under the Charter[12]. That means that, as part of the overall balance to be struck, the relevant public authorities are *bound* to take measures to protect the fundamental rights of children. The Joint Opinion acknowledges this in a general comment (point 12), but it subsequently does not appear to take account of this fundamental premise when analysing the proposed measures.

2) Essence of the rights

The Joint Opinion (point 11) notes that '[t]he essence of a right is affected if the right is emptied of its basic content and the individual cannot exercise it' and that '[t]he interference may not constitute, in relation to the aim pursued, such a disproportionate and intolerable interference, impairing the very substance of the right so guaranteed'. It concludes (in point 12) that 'measures permitting the public authorities to have access on a generalised basis to the content of a communication are more likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter'.

The Commission services consider that given that interference with the content of communications is particularly sensitive, appropriate limits and safeguards are called for, but this does not mean that said measures would be precluded *per se*. Moreover, as expanded on below, the processing of metadata can be as sensitive as measures affecting the content of the communications[13]. Therefore, the assessment relating to the essence of the right cannot be simplified to a rule precluding any measure affecting the content of the communications whilst permitting other measures. Rather, a case-by-case assessment is required.

In this respect, the following elements clarify how the proposal respects the essence of the fundamental rights mentioned.

1) As explained in section 3, the detection obligations to be issued under the proposal do not entail obligations that are general and indiscriminate in nature. As indicated in the Joint Opinion (point 12), in line with the case law[14], the assessment of whether obligations are general and indiscriminate in nature can in some cases play a role in connection to the assessment of whether the essence of the right is at stake.

10 E.g. Case C-817/19, *EU PNR*, para. 122.
11 Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154.
12 Ibid, para. 126-128.
13 Ibid, para. 117.
14 Case C-362/14, Schrems I, para. 94.

2) As acknowledged in the Joint Opinion (point 12), in some of its case law, the Court of Justice referred to the *acquisition of knowledge* of the content[15]. Under the proposal (see Article 10(3)(b) and page 14 of the Explanatory Memorandum), no such knowledge would be obtained, as automatic detection would be conducted on a hit/no-hit basis, i.e. it would only be capable of flagging a correspondence between one item of content and an indicator of online child sexual abuse included in the list kept by the EU Centre without an actual analysis of the data communicated.

3) Considering the limits and safeguards provided for in the proposal and in the absence of any retention (other than in very specific cases) and actual analysis of the data communicated (other than a 'hit/no hit' system), there is no possibility of obtaining a *full overview* of the private lives of the persons affected. According to the Court of Justice's more recent case law, it is specifically such allowing of a full overview that would affect the essence of the right[16].

4) Finally, in the present case, the content of the communications – when it corresponds to online child sexual abuse - is the *very object* of the criminal offences in question. Thus, the content is not relevant with a view to deducing indications of possible criminal activities taking place elsewhere (offline); rather, the very fact that the content is exchanged can constitute the criminal offence, notably in the case of dissemination of 'known' and 'new' child sexual abuse material. In a different context, the Court of Justice has accepted the need to tackle illegal content online effectively, including in principle through specific measures entailing the filtering of online communications of large amounts of users[17].

3) Proportionality of restrictions

In the view of the Commission services, the limitation on the exercise of the abovementioned fundamental rights resulting from the proposal is proportionate:

(i) As shown in the Impact Assessment accompanying the proposal[18], detection of online child sexual abuse is *suitable* to achieve the aim of effectively tackling the particularly serious criminal offences at issue and protecting the aforementioned fundamental rights of children, in particular as detection of known CSAM prevents their re-victimisation while detection of new CSAM and grooming can allow the rescuing of children from ongoing or imminent abuse.

(ii) The criterion of *necessity* is respected by framing detection as a last resort measure. All service providers within its scope have to comply with risk assessment and risk mitigation measures. It is only when, notwithstanding the mitigation measures taken, a significant risk of use of the service in question for the purpose of child sexual abuse remains, that they will be ordered to detect online child sexual abuse. Detection orders can only concern providers of publicly available interpersonal communication services and of hosting services, i.e. providers that may present a real risk of misuse of their services for the purpose of grooming or CSAM dissemination and must be issued by a judicial or independent administrative authority.

(iii) Furthermore, for reasons explored in the Impact Assessment accompanying the proposal (see also its Recital 2), the Commission is of the view that imposing obligations on service providers of the type set out in the proposal is the *only* manner to effectively combat

---

15 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, para. 39

16 Case C-817/19, *EU PNR*, para. 120.

17 See e.g. Case C-18/18, *Facebook Ireland*. Whilst it is true that this judgment related to hosting (and not interpersonal communications) services, it should be borne in mind that the content exchanged via hosting services is not necessarily 'public' in nature and that the judgment contains no limitation to only the 'public' parts of the (very large) social media service at issue.

18 See point 2.1.1 of the impact assessment, brining evidence in support of the claim that online CSA is often only discovered thanks to the efforts of online service providers to detect CSAM on their services, and to protect children from being approached by predators online.

the particularly serious crimes in question and to protect the rights of the children affected, which can justify the taking of more intrusive measures[19]. Detection obligations are framed in the proposal in a way that ensures that they do *not go beyond what is necessary* in each case. The procedure to issue a detection order involves compliance with pre-determined criteria, only after several steps and with the involvement of several authorities. The composite nature of the process is directed at ensuring the proportionality of each detection order in terms of interference with the right to data privacy:

- Whenever required by Articles 35 and 36 of the GDPR *and* in any event in all cases of planned detection orders concerning grooming, the provider must carry out a prior data protection impact assessment and ask the opinion of the competent data protection authority on its draft implementation plan.
- The Coordinating Authority has to ensure that its request for a detection order is as targeted as possible (whenever possible, detection orders should only concern sub-components of the service, if the indication of a significant risk only concerns such sub-component and if technically feasible).
- Coordinating authorities are also required to obtain the opinion of the EU Centre and are required to take into account the availability of sufficiently reliable detection technologies when determining whether to issue a detection order. The final decision on whether to issue a detection order belongs to a judicial or independent administrative authority. These authorities are expressly required to ensure an objective and unbiased balancing of **all** the fundamental rights involved.
- Grooming detection orders can only concern communications where one of the users is a child below the age of 17 (the highest age of sexual consent in the EU).
- Providers have to report on the way detection is conducted, including in terms of fundamental rights impact, to Coordinating Authorities. Where necessary, the orders have to be adjusted. Also, more generally, Coordinating Authorities are charged with supervising compliance, using their investigative and punitive powers under the proposal where necessary.
- Redress is ensured, both for affected service providers and affected users.

(iv) there are *no less intrusive alternative measures* to targeted detection orders that can achieve the aforementioned objectives in an equally effective manner.

In particular, with respect to grooming detection in interpersonal communication services, metadata collection and processing also intrudes on a person's private life and right to data protection, while at the same time being insufficiently effective for the present purposes. The limited effectiveness is linked to the fact that grooming interactions are not characterised by behavioural patterns that can be identified through metadata analysis: they are one-to-one conversations and the only way to become aware of their illegal nature is to detect grooming patterns in their content.

Indeed, in a different context related to general and indiscriminate retention of subscriber and user data, the Court of Justice has noticed the potential intrusiveness of metadata collection and recalled that:

> 'traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of

[19] Cf. Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154.

> the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, *information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'*.[20]

Metadata analysis can lead service providers to take measures against 'suspicious' accounts, e.g. by disabling them. However, without any access to the content of the conversation, it does not allow them to verify whether the exchange is likely to be grooming and should be reported. Hence, the objectives of protecting the potential victim from imminent abuse and to bring perpetrator to justice cannot be met through metadata analysis only.

In light of the above, it is important to note as well that any decision concerning the opening of investigations or prosecutions is taken based on a human, individualised assessment of the situation. Not by private parties, but by the competent law enforcement authorities, in accordance with the applicable law. No decision is taken based on the result of the hit/no-hit automated detection carried out and the subsequent reports by the service providers. In fact, this reporting process, too, is subject to specific requirements set out in the proposal (Articles 12-13) and also involves verification by the EU Centre ensuring that the reports to the competent law enforcement authorities are not manifestly unfounded (Article 48).

5. AVAILABILITY OF EFFECTIVE AND PRIVACY PROTECTIVE DETECTION TECHNOLOGIES

Regarding detection technologies, the Commission services would bring some clarifications in particular on three points:

1) Data protection by design and by default

Point 83 of the Joint Opinion indicates 'the Proposal does not make any express reference to the principle of data protection by design and by default, and does not provide that technologies that are used to scan text in communications must not be able to deduce the substance of the content of the communications'.

On this point, the requirement set by the proposal (Article 10) that technologies should 'not be able to extract any other information from the relevant communications than the information strictly necessary to detect [online child sexual abuse], using the indicators referred to in paragraph 1' effectively corresponds to the requirement 'that technologies […] must not be able to deduce the substance of the content of the communications'. As technologies must make use of the mandatory list of indicators kept by the EU Centre, they can only flag a match between the content scanned, on the one hand, and one of the indicators of child sexual abuse created, managed and provided by the EU Centre, on the other. Automatic detection is conducted on a hit-no-hit basis without any possibility for the technology to 'understand' the content of conversations or collect any further knowledge or information besides the existence of a match as described above.

2) Availability of technological solutions

According to point 85 of the Joint Opinion, '[t]he Proposal assumes that several kinds of technological solutions may be used by service providers to execute detection orders', but the availability and scalability of relevant technologies are not straightforward, especially in relation to new content and grooming.'

[20] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117 (emphasis added).

In this regard, Article 7 of the proposal requires Coordinating Authorities and issuing authorities to take into account the availability of sufficiently reliable technologies before requesting a detection order, to avoid the situation whereby a provider would receive a detection order that they cannot implement because of the lack of effective and deployable technologies. Indeed, no detection order is to be issued should it be impossible for the requirements of Article 10 to be met in a given case.

Moreover, the consultations conducted by the Commission services in preparation of the proposal have highlighted that technological solutions that allow for the detection of all types of child sexual abuse do exist. As noticed in the Joint Opinion, those technologies differ based on the type of content to be detected ('known' CSAM, 'new' CSAM or grooming). In particular:

a) For 'known' child sexual abuse material

Technologies used to detect 'known' CSAM are typically based on hashing. Hashing technology is a type of digital fingerprinting. The hashing and matching process involving converting a known item of CSAM image into a unique (and non-reconvertible) 144 digit signature. The process is built on the similar concept of digital fingerprinting as originally developed for application in the detection of malware and copyrighted content. The unique digital fingerprint (number-series) extracted from an item of known CSAM (e.g. an image or a video) is added to a hash list (i.e. a list of indicators of known CSAM). Whenever the technology checks an item, it will check *exclusively* whether its digital fingerprint corresponds to one that is already in the list. No other information needs to be collected or processed.

Many declinations of hashing technology exist, including Microsoft's PhotoDNA, which is the most widely used tool of this type. The rate of false positives is estimated at no more than 1 in 50 billion[21], based on testing. PhotoDNA has been in use for more than 10 years by over 150 organisations globally[22] including service providers (Microsoft, Facebook, Twitter, Apple), NGOs (e.g. NCMEC, Internet Watch Foundation) and law enforcement entities in the EU (e.g. Europol, DE, SE and others). In these 10 years, the tool has been used daily and analysed hundreds of billions of images without any accuracy concerns being raised.

Video and audio hashing is analogous to image hashing: it uses the same process of extracting hash signatures and comparing various frames in a video with audio feed. An example is Google's Content ID, which searches for copyright infringing material on YouTube.

b) For 'new' child sexual abuse material

'New' CSAM is detected through Artificial Intelligence (AI) classifiers (e.g. Thorn's Safer tool, Google's Content Safety API, and Facebook's AI technology) that are trained using 'known' CSAM and that are, therefore, enabled to find analogous content. These technologies have a relatively high accuracy rate and their use can only improve their accuracy even further. In this respect, the high quality/clear labelling of the 'known' CSAM datasets used to train algorithms to produce AI classifiers is key. Safer classifiers are retrained every six months, with over 2 billion files having been processed through the classifier to date. This refinement is complemented by ongoing mining for examples of false positives to continually retrain classifier and refine its accuracy.

---

21 Testimony of Hany Farid, PhotoDNA developer, to House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers, 16 October 2019

22 Microsoft provides PhotoDNA for free. Organisations wishing to use PhotoDNA must register and follow a vetting process by Microsoft to ensure that the tool is used by the right organisations for the exclusive purpose of detecting child sexual abuse material. The tool can be used to detect child sexual abuse material in various services (e.g. hosting, electronic communications) and devices (e.g. by law enforcement to detect known child sexual abuse material in a suspect's device).

Bringing the list of AI classifiers under the supervision of a central and public supervisory body, *i.e.* the EU Centre, subject to legal requirements, will lead to a significant improvement in terms of transparency and quality of the dataset used to produce AI classifiers and in terms of accuracy rates of such classifiers.

Importantly, AI classifiers can be *set* to detect material that corresponds to new CSAM *with a predetermined rate of accuracy*. Hence, *it is possible to calibrate them to only detect material that has an extremely high (e.g. 99.9%) chance of being CSAM.* This would entail an extremely low error rate, but also a relatively high amount of new CSAM left undetected.

c) <u>For grooming</u>

Tools for the detection of grooming in text-based communications (e.g. the tool developed under Microsoft's Project Artemis in collaboration with The Meet Group, Roblox, Kik and Thorn) make use of technologies solely to detect patterns which point to possible concrete elements of suspicion of online child sexual abuse without being able to deduce the substance of the content other than signs of grooming. The technique is applied to text-based chat conversations. Conversations are rated on a series of characteristics and assigned an overall rating, indicating the estimated probability that the conversation constitutes grooming. Much as for 'new' CSAM, it is possible to set the grooming detection tools so that they are instructed to only detect conversations that have an extremely high chance of being grooming. The availability of a reliable database of confirmed grooming conversations from different types of services is expected to significantly improve accuracy rates of existing tools.

3) Human review in relation to grooming

Point 86 of the Joint Opinion notes that grooming detection technologies would have, according to the Impact Assessment accompanying the proposal, an 88% accuracy rate[23]. 'EDPB and EDPS consider that, with such a high risk processing, 12% failure rate presents a high risk to data subjects who have been subject to false positives, even when there are safeguards in place to prevent false reports to law enforcement. It is highly unlikely that service providers could commit enough resources enough to review such a percentage of false positives.'

The Commission services consider it important to underline that the proposal endows the EU Centre with the role of filtering out manifestly false positives (i.e. manifestly unfounded reports) and giving individual feedback to service providers on the accuracy of their detection process. Hence, service providers are to ensure human oversight and review, but are neither the sole nor the main actor in charge of ensuring that manifestly false positives do not reach law enforcement authorities.

6. END-TO-END-ENCRYPTION (E2EE)

In relation to E2EE, point 101 of the Joint Opinion affirms that '[w]hile the Proposal states that it "leaves to the provider concerned the choice of the technologies to be […] the structural incompatibility of some detection order with E2EE becomes in effect a strong disincentive to use E2EE. The inability to access and use services using E2EE (which constitute the current state of the art in terms of technical guarantee of confidentiality) could have a chilling effect on freedom of expression and the legitimate private use of electronic communication services'.

In this regard, the Commission services consider it important to clarify the following points:

[23] Information provided by Microsoft on its Project Artemis grooming detection tool. It is important to note that an accuracy rate of 88% means that out of 100 online exchanges flagged as possible grooming, 88 are actually grooming. It does not mean that out of all the online exchanges taking place in the platform, 12% are wrongly flagged as grooming.

1) Technological neutrality of the proposal

The proposal neither incentivises nor discourages the use of E2EE. Recital 26 explicitly refers to this, adding that 'the provider concerned [has] the choice of the technologies to be operated to comply effectively with detection orders […]. That includes the use of end-to-end encryption technology, which is an essential tool to guarantee the security and confidentiality of the communications of users, including those of children'.

Point 101 of the Joint Opinion notes that E2EE 'constitutes the current state of the art in terms of technical guarantee of confidentiality'. However, the implementation of E2EE in a way that prevents the safeguarding of fundamental rights of children when a significant risk of child sexual abuse exists implies a *choice*. The Commission services reiterate that a balance must be struck between the various rights and interests at stake, notably protection of privacy of users and security of communications in general, and the need to prevent and tackle the undetected grooming of a vulnerable group of users (*i.e.* children) and the unchecked dissemination of material concerning the abuse of such children.

Based on the consultations conducted and as shown in its Impact Assessment, solutions that allow for child sexual abuse detection on E2EE services exist, while noting that further research into some of these methods may be needed, and more solutions could be developed with the right set of legislative incentives.

2) Absence of legal obstacle to the inclusion of E2EE services in the scope of the proposal

The fact that the proposal *does not exempt E2EE services* does *not* as such create legal difficulties.

First, the proposed regulation *neither obliges nor prevents providers from implementing E2EE on their services.* The proposal imposes an obligation of results in terms of performing detection obligations of online child sexual abuse where significant risks exists, which can only be effective if implemented throughout the digital space. It remains for the service provider addressed by a detection order to choose how to provide its services and also how to implement the detection orders, provided that all the safeguards set by the proposal itself are respected.

Secondly, E2EE certainly has acknowledged advantages in terms of protection of the fundamental rights to privacy and personal data protection as well as cybersecurity and can, as such, play a part in complying with EU legislation in these domains, such as the GDPR, the European Electronic Communications Code (EECC) and the NIS2 Directive. At the same time, there is no rule of EU law that specifically requires the use of E2EE or that grants providers the right to always use E2EE whenever they so wish. Whilst it is true that E2EE has advantages in terms of protection of the fundamental rights to privacy and personal data protection and can play a part in complying with the EU legislation implementing these rights, neither these rights nor that legislation mandatorily prescribe E2EE as such. Moreover, as mentioned, those rights are not absolute and can be subject to limitations where necessary and proportionate.

Thirdly, the proposed regulation provides that when a Coordinating Authority and the judicial or independent administrative authority requested to issue the detection order are determining whether to request to issue a detection order, they shall take into account the *availability of sufficiently reliable detection technologies in that they limit to the maximum extent possible the rate of errors regarding the detection and their suitability and effectiveness for achieving the objectives of the proposed regulation, as well as the impact of the measures on the rights of the users affected.* Hence, the proposed regulation requires taking into account the

availability of sufficiently reliable detection technologies prior to issuing a detection order. This also applies to providers offering E2EE services.

3) Arbitrary nature of a possible exclusion of E2EE services from the scope

First, if targeted detection, ordered on a case-by-case basis and striking a fair balance between the fundamental rights at stake, is necessary to ensure that the rights of children are protected, then this holds true independently of the particular technology used to provide the services in question. *Exempting some services from detection orders based on the choice of providers to recur to a specific encryption technology would effectively give any provider a possibility to opt-out from its detection obligations*. Naturally, the nature of the service involved might affect the outcome of the proportionality analysis, on a case-by-case basis.

Secondly, as E2EE services are no less at risk of online child sexual abuse than non-E2EE services, *exempting E2EE services from detection obligations would be arbitrary.*

Thirdly, exempting E2EE services would also *compromise the proposal's capacity to achieve its objective of preventing and combating (online) child sexual abuse*. This problem would worsen in time, as the current trend towards an increasingly broad uptake of E2EE can be expected to continue. By making it unsuitable to reach its aim, exempting E2EE services from the proposed detection obligations would also compromise the proportionality of the proposal.

Finally, exempting E2EE would *undermine the proposal's capacity to achieve its objective of ensuring a level playing field between players on the digital single market,* as some service providers would be subject to some obligations and some would be de facto exempted.

7. EXISTENCE AND PROPORTIONALITY OF AGE VERIFICATION TOOLS

According to point 92 of the Joint Opinion, '[t]he Proposal encourages providers to use age verification and age assessment measures to identify child users on their services. In this respect […] there is currently no technological solution that is capable of assessing with certainty the age of a user in an online context, without relying on an official digital identity, which is not available to every European citizen at this stage. Therefore, the Proposal's envisaged use of age verification measures could possibly lead to the exclusion of, e.g., young-looking adults from accessing online services, or to the deployment of very intrusive age verification tools, which might inhibit or discourage the legitimate use of the affected services'.

1) Age verification as one of several possible mitigation measures

As acknowledged in the Joint Opinion, the proposal 'encourages' the use of age verification and age assessment tools, as possible mitigating measures.

The proposed regulation requires that such measures need to be put in place by app stores and by providers of interpersonal communications services that have identified a risk of use of their services for the purpose of the solicitation of children.

In the case of app stores, they *have* to put in place 'age verification' measures, for two reasons:

(i) The identification of children among their users and the 'gatekeeping' function consisting of preventing them from accessing apps presenting a significant risk of grooming is the only obligation imposed on app stores under the regulation

(ii) Unlike other services, app stores have access by default to data concerning their users account (e.g. the name on the credit card used for purchases) that can provide strong evidence concerning their age, without any need to collect further information.

2) Availability of effective and privacy protective age verification tools

The Commission services' preparatory consultations prior to the adoption of the proposal have highlighted that a range of diverse and effective age verification and age assessment techniques are already available on the market[24]. Those involve the use of image, audio, video or text-based estimation techniques, or the capture of proofs if identity, credit card, online banking or telephone account verification. Further age verification tools are being developed, involving biometrics and machine learning measures, to increase the level of certainty in relation to age determination. Many age verification tools place a strong emphasis on user privacy and achieve their purpose without processing or transferring unnecessary data. It is also important to note that EU standards[25] are being developed in the field of age verification and that the euCONSENT project has been working to build a network of interoperable age-verification solutions to provide users with options and minimise the need to sign up to and share data with different services.

[24] See e.g. here a mapping of existing age verification methods, done in the context of the euCONSENT project.

[25] A request for EU standard on age verification/age assurance is one of the key actions for the Commission under the new Better internet for kids strategy (BIK+) - COM(2022) 212 final