28 September 2020

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online

Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, and her shadows

Please note: In order to not cause any unnecessary delay, we kindly ask for written answers to each individual question, no general replies, or grouping of several questions, please. Deadline for replies: **Friday, 2 October, noon.** The staff level meeting on Monday, 5 October, will provide for a first opportunity to follow-up on the answers provided. The list below is not intended to be exhaustive and should not prevent the rapporteur or her shadows from raising additional questions and issues at a later stage.

This non-paper prepared by the Commission's services aims to provide explanations with regard to the technical elements of the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, in response to comments and questions received from the European Parliament's rapporteur Birgit Sippel, MEP and the shadow rapporteurs.

This non-paper is based on the relevant Commission proposal and does not present any new positions with regard to that proposal.

The fact that certain examples of technologies are provided in this non-paper must not be considered as meaning that they are necessarily covered by the proposed Regulation (conversely, the fact that certain technologies are not mentioned, does not mean that they are necessarily not covered), and must not be interpreted as the Commission or its services taking position, as to whether any data processing using these technologies complies with Union law.

Birgit Sippel, S&D, rapporteur

Lack of impact assessment

The proposal is not accompanied by an impact assessment, although according to the inter-institutional agreement, there should be one. There is only one exception in Art.

12 of the inter-institutional agreement, according to which 'IAs must not lead to undue delays in the law-making process or prejudice the co-legislators' capacity to propose amendments'. The European Electronic Communications Code was adopted in December 2018. Since then, it was known that so called over the top providers would fall within the scope of the ePrivacy directive by the end of 2020. What is more, the adoption of the Code happened a long time before any COVID-19 related work restrictions would be put in place.

► 1. Why was there no time to do an impact assessment in the beginning of 2019 and why is this proposal only coming now?

Response of the Commission's services:

This proposal has two key features: that it is limited in time, and that it seeks only to maintain the status quo by introducing a targeted temporary derogation from certain provisions of the ePrivacy Directive pending the adoption of long-term legislation. The Commission is already working on a proposal for a long-term framework, which will be accompanied by a full impact assessment. This proposal does not introduce a new legal basis for processing.

The fact that the revised definitions in the European Electronic Communications Code (EECC) would prevent certain companies from continuing current voluntary practices for the detection and reporting of child sexual abuse online and the removal of child sexual abuse material was made known to the Commission's services by industry only after the adoption of the Code in December 2018, and after the adoption of the new proposal for an ePrivacy regulation. As a result, the issue regarding those voluntary practices was not addressed in any of the impact assessments for these proposals.

Once it became aware, the Council then considered addressing this issue in the e-Privacy regulation proposal, including by a standstill clause, which would have had a similar effect as the proposed interim Regulation. This solution was clearly dependent on the progress made by the co-legislators on the ePrivacy proposal. The Commission has supported the co-legislators and pushed for a quick adoption of the ePrivacy Regulation before 21 December 2020, the date on which the EECC definitions will enter into application. However, its adoption before that date is unlikely.

The Commission therefore concluded in July 2020 that, in view of the date of 21 December 2020, the best route was the adoption of a targeted temporary derogation from certain provisions of the ePrivacy Directive through standalone legislation.

As the Commission explained in the explanatory memorandum of its proposal, in view of the policy objective and the time-sensitive nature of the issue, there were no other materially different policy options available. In particular, the measure intends to introduce an interim and strictly limited derogation from certain provisions of the e-Privacy Directive, pending the adoption of long-term legislation. The long-term legislation will be proposed in the second quarter of 2021 as announced in the EU strategy for a more effective fight against child sexual abuse and will be accompanied by an impact assessment.

Legislative mapping of current practices

The Commission is justifying the need for this regulation with the different national approaches by Member states when it comes to measures to detect CSAM online.

► 2. Since there is no impact assessment, can the Commission provide a complete mapping of the different national rules and practices currently in place regarding the detection of CSAM?

Response of the Commission's services:

The Commission's services are currently finalising a mapping of such rules in Member States and it will be transmitted to the European Parliament as soon as it is completed.

It should be noted that the proposed Regulation seeks to create a temporary derogation from certain provisions of the ePrivacy Directive in relation to activities that are not currently within the scope of the Directive, but which will come within its scope upon the entry into application of the definitions of the European Electronic Communications Code on 21 December 2020.

Article 15 of the ePrivacy Directive permits Member States to restrict the scope of certain rights and obligations provided for in the Directive through national legislation, which serves one of the listed purposes and meets the requirements of necessity and proportionality. Individual Member State legislation regarding the detection and deletion of CSA online would likely lead to fragmentation across the single market, and it is unlikely that national measures would be adopted by all Member States by 21 December 2020. A Union wide derogation from the application of provisions of the ePrivacy Directive for certain processing activities can only be adopted by Union legislation.

Subsidiarity

The deadline for national parliaments to raise subsidiarity objections will expire in mid-November. As this proposal provides for a derogation of confidentiality of communications, this might pose constitutional problems for some Member states.

► 3. Do you expect any reasoned opinions from the national parliaments in this regard, objecting to your proposal? And how would this interfere with the timeline, given that we are not allowed to have a final vote on the text until the 8 weeks deadline has expired?

Response of the Commission's services:

The proposal focuses on maintaining the status quo with temporary and strictly limited rules derogating from the application of certain articles of the e-Privacy Directive to

services that are not currently covered by it. Of course, the national parliaments have the right to deliver reasoned opinions and this right and the timeline will be respected. The Commission's services are optimistic that the timeline can be respected so that the envisaged date for adoption and entry into force before 21 December can be met. It will also be important to recall that this is a temporary measure and full consultation and impact assessment will accompany the future proposal for a long-term framework.

Impact of the proposed legislation on future mandatory legislation for the scanning for child sexual abuse content

The draft proposal claims to be a temporary derogation from the ePrivacy directive. However, the temporary aspect does not necessarily become clear when reading Article 1 on the subject matter. The explanatory memorandum further states that "The duration of the derogation is limited to a time period strictly necessary to adopt the long-term legislation." However, this is not mentioned in the draft regulation: Art. 4 of the proposed regulation simply states that it shall be applicable "until 31 December 2025".

► 4. Why is the Commission so generous in the period of application of the temporary derogation, especially bearing in mind that the new legislation is supposed to be presented in the second quarter of 2021 already? How advanced is the preparation of the new proposal (timetable)? Why can't we have a shorter period of application of the proposed temporary Regulation?

Response of the Commission's services:

The proposed Regulation does specify, in recital 16, that 'In case the long-term legislation is adopted and will enter into force before [31 December 2025], that legislation should repeal this legislation.' This sets out clearly that the long-term legislation should contain a provision explicitly repealing the present proposed Regulation.

The Commission has indeed committed, in the strategy of 24 July 2020, to proposing the long-term legislation by the Q2 2021. The preparation of this proposal is currently underway, including the preparation of a detailed impact assessment.

The sunset date of 31 December 2025 was chosen so as to be certain to ensure sufficient time for the adoption and entry into application of the long-term legislation, and to avoid the risk that the interim legislation would cease to apply during the legislative procedure, necessitating consideration of another interim measure. For reasons of legal certainty, the proposal contains a fixed date.

Lack of safeguards in the proposal and possible breach of GDPR

a) According to Art. 15 of the current ePrivacy directive, only *Member states* can restrict the scope of the ePrivacy directive, not the Union. However, as the GDPR trumps the ePrivacy and according to the GDPR, *Union or member state* law may

restrict certain principles, I could in general accept that the Union proposes legislation in this area.

b) However: Any legislation that were to restrict the scope of the ePrivacy for law enforcement purposes has to respect the conditions of directive 95/46/EC which was replaced by the GDPR. And according to Art. 23 GDPR Union or Member State law may restrict by way of a legislative measure certain rights stemming from the GDPR when such a restriction respects the essence of the fundamental rights and freedoms. Very importantly, Art. 23 (2) contains a legal obligation for any such a law to contain specific safeguards, including at least:

(a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

► 5. Where are these safeguards in the proposed derogation? How is a proposed piece of legislation legal under the GDPR and the ePrivacy directive if it does not contain this list of safeguards?

Response of the Commission's services:

The proposed Regulation would be based on Articles 16 and 114 TFEU and provides for a temporary and strictly limited derogation from certain provisions of the ePD for the processing of personal and other data for the purpose of combatting child sexual abuse online by certain number-independent interpersonal communications services (NI-ICS) providers.
The present proposal does not restrict any rights stemming from the GDPR. Providers of number-independent interpersonal communications services who undertake these voluntary activities remain fully subject to all of their obligations under the GDPR, without exception. The Commission does not take a position on the legality of these voluntary practices by operators; the assessment of such legality falls into the competence of the national DPAs. The proposed Regulation would not create a legal basis for any processing activities. Instead, it only ensures that certain processing activities, which are currently subject to GDPR conditions and safeguards, will remain subject to the GDPR and will not become subject to Articles 5(1) and 6 of the ePrivacy Directive and the national law transposing those provisions on 21 December 2020. Since this proposal does not restrict in any way the rights under the GDPR, Article 23 GDPR is not relevant for the proposed Regulation.

The proposed Regulation does, however, specify certain additional safeguards. In particular, the proposal requires that service providers benefitting from the derogation must publish annual reports on the measures they implement, including information on the technologies deployed, the rate of false positives, and the number of cases identified. The proposal also requires that service providers delete processed data

immediately (except where child sexual abuse online has been detected), and that the measures be strictly limited to processing for the purposes of detecting and deporting child sexual abuse online and removing child sexual abuse material. In any case, where the provider's activities do not meet all of the conditions laid down in Article 3 of the proposed regulation, those activities will not fall within the scope of the derogation and Articles 5(1) and 6 of the ePrivacy Directive will apply to them in the same way in which they would in the absence of the proposed Regulation.

c) In Digital Rights and Tele 2, the ECJ quashed the data retention directive amongst others because the directive did not provide for any *objective criterion* by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences, and which, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, could be considered to be sufficiently serious to justify such an interference.

Furthermore, Directive 2006/24/EC did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, did not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provided that each Member State was to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements, and it did not lay down a specific obligation on Member States designed to establish such limits (points 5962 of Digital Rights case, see also cases Tele2 Sverige and Watson C-203/15and C-698/15).The Court considered that all these essential safeguards were not found in that piece of legislation and accordingly it was declared invalid.

► 6. Where can one find these safeguards in the current proposal? If not, why not? And how is this in line with the cited ECJ case law?

Response of the Commission's services:

The above-cited case related to an obligation imposed (through national legislation) upon service providers to process data. The proposed Regulation would not impose any obligation upon service providers to process data and would not create a new ground for processing of personal data. It would introduce a targeted and temporary derogation from certain provisions of the ePrivacy Directive, which currently do not apply to the activities in question, in order to ensure that those activities remain allowed to the extent that they currently comply with Union law.

The derogation in the proposed Regulation applies only in relation to data constituting child sexual abuse online, as defined in Article 3.

The proposal lays down a set of conditions to be fulfilled and safeguards that apply in order to delimit the activities, which fall within the scope of the derogation.

Question on GDPR and recital 6

Recital 6 of the proposed legislation seems to suggest that as of 20 December 2020, the GDPR will cease to apply to the processing of personal data by providers of number-independent interpersonal communications services. However, this seems to be in direct contraction to recital 10 which states the opposite.

► 7. Could you please clarify what is meant with recital 6?

Response of the Commission's services:

The proposed Regulation provides for a temporary and strictly limited derogation from the applicability of Articles 5(1) and 6 of the e-Privacy Directive (ePD) for number-independent interpersonal communications services that have used specific technologies and conducted activities to detect and report child sexual abuse online and remove child sexual abuse material on their services before this Regulation enters into force.

Under the proposed Regulation, which would apply for a limited period of time, the GDPR will therefore continue to apply to these activities, which is explained in Recital 10 of the proposal. Recital 10 further specifically notes that providers of these services remain subject to any requirement to carry out an impact assessment under Article 35 of the GDPR. As explained in recital 17, providers of NI-ICS are subject to the specific obligations set out in the ePD with regard to any other activities that fall within its scope.

Recital 6 of the proposal clarifies the current situation, i.e. prior to 21 December 2020 and does not contradict the statement contained in recital 10. As from that date, the ePrivacy Directive, which particularises and complements the GDPR, will apply to number-independent interpersonal communications services. The GDPR will continue to apply to the extent that there are no specific provisions in the ePrivacy Directive. The protection of the confidentiality of communications (Article 5) is one of the provisions where the ePrivacy particularises the GDPR. Based on the Opinion 5/2019, the DPAs declared themselves competent to evaluate any processing of personal data also if it falls under the ePrivacy Directive.

Hashing technology and encryption

According to the proposal, only "well-stablished technologies regularly used by providers" (Art. 3 a) can be used for the detection of CSAM.

► 8. In order to use hashing technologies, where would the encryption need to be broken, at what point of the communication the interference would have to take place? On the level of the device, on the server?

Response of the Commission's services:

This proposed Regulation does not address or directly relate to encryption. The Commission's services are not aware of any service providers using hashing technology in end-to-end encrypted communications.

► 9. Which measures would be used to counterbalance security threats to users by malicious third parties, especially taking into account that these users might be children?

Response of the Commission's services:

It is not clear what is meant by the above reference to 'security threats to users by malicious third parties' in this context. Should this be related to the question of encryption, the proposal does not create any security threat, but instead seeks to create a derogation from certain rules of the ePrivacy Directive. If further details can be provided, the Commission's services would be happy to provide a more substantive response.

► 10. How do you conciliate your proposal with the ECJ case law stipulating that providers of electronic communications may not use systems of general monitoring (case Scarlet v. sabam)?

Response of the Commission's services:

The Court of Justice in Scarlet v. SABAM[1] ruled that relevant Union legislation 'must be interpreted as precluding an injunction made against an ISP which requires it to install a system for filtering all electronic communications passing via its services…' In doing so, it interpreted a number of provisions of EU law, most notably Article 15(1) of the e-Commerce Directive[2], which prohibits the establishment of a general monitoring obligation. The proposed Regulation does not oblige service providers to undertake any general monitoring or indeed any other processing activities, but instead relates only to voluntary measures for the detection and reporting of child sexual abuse online and the removal of child sexual abuse material. Therefore, the proposal does not lead to any violation of the prohibition of general monitoring obligation laid down in Article 15(1) of the e-Commerce Directive, as interpreted by the Court of Justice in the abovementioned case. Since the proposed Regulation leaves the e-Commerce Directive unaffected, the said prohibition would continue to apply.

[1] Judgment of 24 November 2011, Scarlet Extended, C-70/10, EU:C:2011:771

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 - 0016.

Extension of scope to solicitation of children

a) **criminal law aspects**: Art. 6 of Directive 2011/92/EU (child sexual abuse directive) establishes minimum sanctions for the solicitation of children. However, Art. 3 of the proposed derogation from the ePrivacy directive does not make a reference to the child sexual abuse directive, but introduces its own definition of solicitation of children. In particular, one has to notice that the new definition of solicitation introduced in the regulation does *not* include the notion of the "age of consent" of the child, which is however a constituent element of the relevant provision in the child sexual abuse directive.

► 11. How does the Commission justify this departure from the criminal law provisions of the child sexual abuse directive?

Response of the Commission's services:

At the outset, it must be emphasised that the proposed Regulation is not a criminal law instrument.

In relation to the different wording used in the proposal versus the Child Sexual Abuse Directive, this was necessary because the Directive does not contain the required definitions. Nonetheless, the Commission has attempted to create definitions in this proposal which mirror the Directive as closely as possible, to benefit from established definitions to the maximum extent. Indeed, Articles 2(2)(a) and (c) are direct references to definitions in the Directive, which are clear and unambiguous.

In the case of solicitation, the definition laid down in Article 6 of the Directive is not specific enough for service providers to use in practice.

If Article 6 of the Directive were to apply, service providers would have to establish the existence of such material acts leading to a meeting offline, which is necessarily to be done by the law enforcement, prosecuting authorities and/or (ultimately) judges in court proceedings.

Therefore, an appropriate definition had to be created, which appropriately reflects the current voluntary practices of service providers which this proposal aims to cover and retains as much as possible relevant elements of Article 6(2) of the Child Sexual Abuse Directive.

Therefore, the definition proposed in this regulation specifies a number of key actions that offenders typically employ when soliciting children for the purposes of child sexual abuse. Hence, it deviates from the Article 6 definition of grooming. The definition in the proposal consists of two constituent elements: first, it sets out that the purpose of the solicitation must be to engage in sexual activities with a child or to produce child sexual abuse material. Secondly, in addition to specifying the purpose of the solicitation, the definition specifies that the solicitation must consist of one of three concrete actions, namely luring the child with gifts, threatening the child, or exposing them to pornographic material.

The second component aims to more specifically describe grooming behaviour. The overall process of grooming has been described as (1) forming a relationship with a child, (2) creating a feeling of exclusivity and secrecy and reducing risks of discovery, and (3) changing the child's perception of what is normal in a relationship with an adult.[3] This last part has been described as "desensitization and reframing": Desensitization entails desensitizing the children to sexual contact (e.g. by sharing adult or child pornographic images); reframing consists of presenting sexual activity between children and adults as if it were normal or even beneficial to the child later in life. The cycle of entrapment and creation of secrecy is often performed through isolation of the child, e.g. by making it seemingly impossible for the child to seek outside help by convincing the child that others would punish the child for actions already undertaken with the perpetrator.

Of these steps, many are difficult to identify as objectionable behaviour per se. However, the desensitization, which often takes the form of sharing sexualized images to make it seem normal, was an element that can be objectively and precisely described and possibly also be more easily identified. In addition, the element of pressure that is often employed to prevent a child from seeking outside help and to force it into meeting with the perpetrator or sharing self-generated images, also is a decisive point in the process that was both objectionable in and of itself and that could be identified.

As a result, the Commission has identified these typical steps that may occur in a grooming situation in order to clarify the scope of the exception to the largest extent possible.

► 12. How can the legal basis used for this draft regulation, 114 TFEU (internal market) and 16 TFEU (data protection), be used to define material criminal law in EU member states?

Response of the Commission's services:

This proposed Regulation is not a criminal law instrument. It does not criminalise any acts, define any offences or penalties and does not create, alter or otherwise affect criminal law provisions at the national or Union level. The proposal exclusively concerns a derogation for service providers in relation to certain voluntary processing activities.

Articles 114 TFEU (ex Article 95 TEC) is an appropriate legal basis for the proposed Regulation, given that it provides for a temporary derogation from certain provisions of the ePrivacy Directive, which was adopted on the basis of Article 95 TEC. In addition, in this particular case the adoption of national measures derogating from the ePrivacy Directive involves a significant risk of fragmentation likely to negatively affect the internal market, further justifying the use of Article 114 TFEU as a legal basis.

[3] See, e.g., the description of cybergrooming on the site of the German UBSKM; the Commission can also provide a list of studies if desired.

In addition, since an electronic communication involving a natural person will normally qualify as personal data, Article 16 TFEU, which concerns the processing of personal data, is also an appropriate legal basis.

► 13. Will the new legislation on CSAM also be a Regulation based on the same legal basis?

Response of the Commission's services:

The EU strategy for a more effective fight against child sexual abuse, adopted on 24 July 2020, includes a commitment that, by Q2 2021, the Commission will propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities.

The preparation of this proposal, including a detailed impact assessment, is currently underway. As part of this impact assessment, the appropriate form and legal basis will be assessed, which must be done in the light of the objective and content of the envisaged measures. Given that this process is not yet concluded, the Commission's services are not currently in a position to comment on the form or legal basis of such a proposal.

b) **technology used**: According to the proposal, only "well-stablished technologies regularly used by providers" (Art. 3 a) can be used for the detection of CSA.

► 14. Could you name the companies that would be considered to produce "well-established" technologies under this draft regulation? Would it be possible to use another newly developed software if it provides the same or higher safeguards under this regulation?

Response of the Commission's services:

It is not possible to provide a complete list of all the companies producing these technologies but some examples can be given below. It should be recalled that the fact that certain examples are provided in this non-paper must not be considered as meaning that they are necessarily covered by the proposed Regulation (conversely, the fact that certain technologies are not mentioned, does not mean that they are necessarily not covered), and must not be interpreted as the Commission or its services taking position, as to whether any data processing using these technologies complies with Union law.

The use of these or other technologies is and remains subject to them being compatible with the GDPR and any other applicable law. It should also be noted that some technologies/implementations are developed by individual companies or organisations, while others are developed in collaboration, and it is not unusual for custody to be transferred to another organisation such as THORN to manage free licensing for other companies subject to safeguards.

- Hashing technology (e.g. PhotoDNA, PhotoDNA for Video)

- Text analysis technology (e.g. Project Artemis)

Please see question #39 for more details on the technologies used.

The NCMEC annex contains a list of all companies that reported to NCMEC in 2019, which used technologies to detect child sexual abuse online. It should be noted that the concept of electronic service as used by NCMEC might not be equivalent to the definition of number-independent interpersonal communications service as defined in the EECC.

***

Recital 11 of the draft regulation states that scanning for cyber grooming should "*not* include systematic filtering and scanning of communications containing text but only look into *specific communications* in case of *concrete elements of suspicion* of child sexual abuse."

► 15. How do you define "concrete elements of suspicion"? Is this the open "such as" list in Art. 3 c of the proposed regulation? For example: What will happen if I send an email to my shadows stating that we will have a meeting on the child sexual abuse issue? Is this sufficient element of suspicion? Could the software detect the context?

Response of the Commission's services:

The term 'concrete elements of suspicion' in recital 11 is indeed linked to the requirements of Article 3(c) of the proposal, which require that 'the technology used to detect solicitation of children is limited to the use of relevant key indicators'. However, it should also be noted that the requirements of Article 3(c) do not apply in isolation, but together with the other requirements of Article 3, including that the technology 'is in itself sufficiently reliable in that it limits to the maximum extent possible the rate of errors'.

Context is indeed a key element in determining whether a communication may constitute solicitation. For this reason, the requirement that the technology limits the rate of errors to the greatest extent possible is an important one to minimise the likelihood of a communication being inappropriately flagged.

► 16. Will this email be reported? And more importantly: To whom will it be reported? There is no provision in the regulation that a positive hit could only be sent to EU law enforcement authorities. Could a positive hit be shared with private entities who are or say that they are active in the fight against child abuse and with law enforcement of third states under this regulation (for example with NCMEC in the US)?

Response of the Commission's services:

With regard to reporting, the derogation under the proposed Regulation is limited to reporting of child sexual abuse online and, as such, applies only to data which falls

under the definition contained in Article 2(2) of the proposed Regulation. As such, it would be expected that the communication in this example – even if erroneously picked up by any technology – would not be reported.

In general terms, there is currently no obligation in EU law to report child sexual abuse online, and this is a matter which may be addressed by the legislation to be proposed in Q2 2021 under the Commission's strategy of 24 July 2020. US service providers, if they choose to voluntarily detect child sexual abuse, are obliged under US federal law to report to NCMEC any visual depiction of apparent child pornography or other content relating to the incident such report is regarding. This obligation applies irrespective of the location of the users concerned, and NCMEC forwards reports to relevant law enforcement authorities in the US and other countries. NCMEC received over 725 000 such reports concerning the EU in 2019 which it forwarded to the relevant law enforcement agencies in the EU. Under the present proposal, providers of number-independent interpersonal communications services could continue to detect and report child sexual abuse online to relevant organisations, including to NCMEC, after 21 December 2020.

► 17. Which technology exactly is currently in use to detect the "solicitation of children" that does *not* amount to a systematic filtering? Please describe how it works.

Response of the Commission's services:

The technology to detect solicitation of children tends to use a combination of relevant key indicators such as keywords and objectively identified risk factors such as age difference or frequency of messaging to a certain group of users, to determine a risk score for the conversation to be possible grooming.

According to the information available to the Commission's services, in the case of Microsoft's grooming technology, it evaluates and "rates" conversation characteristics and assigns an overall probability rating. This rating can then be used as a determiner, set by individual companies implementing the technique, as to when a flagged conversation should be sent to human moderators for review.

In terms of accuracy, Microsoft's tool is 88%+ accurate in the automated detection part, according to Microsoft.

See annex for an overview of the technologies used to detect child sexual abuse online

► 18. What age difference would be considered a "risk factor" according to your proposal? How do you factor in the fact that the age of sexual consent is different among Member States?

Response of the Commission's services:

The exact age difference that would contribute to flagging a message for review depends on the type of technology and on the set-up parameters used. These parameters vary according to the situation (which may include the different ages of

sexual consent in Member States). This is why the exact age difference is not specified in the proposal. Moreover, pursuant to Article 3(b) of the proposed Regulation, the derogation applies on the condition that the technology used is in itself sufficiently reliable in that it limits to the maximum extent possible the rate of errors regarding the detection of content representing child sexual abuse, and where such occasional errors occur, their consequences are rectified without delay.

► 19. Can you give concrete examples of "key words" that you have been presented with that are currently used to detect solicitation of children online?

Response of the Commission's services:

According to Microsoft, key phrases used together, such as "how old are you," "are your parents home" and "can we meet" can trigger a flag, if coupled with other proprietary information examined in the algorithm.

The makers of these tools are wary to share details of "regular expressions," as this is not something that would be possible to have in the public domain. As soon as these expressions are known, offenders would adjust their tactics to try to evade these tools.

► 20. Will the scanning for solicitation of children require retrospective searches and therefore the retention of communication by providers as, in contrast to hashing technology, solicitation of a child is something you would only be able to establish over time?

Response of the Commission's services:

No. According to Microsoft, the technology is based on "historic" chats, as opposed to "real-time" chats, with "historic" dating typically no more than a day. With that information, the tool offers risk scores for the conversation, which would trigger an alert over a certain threshold.

<u>Definition of "child" and of "sexual consent" and "consent" under the GDPR</u>

There is no definition of "child" or the "age of sexual consent" in the proposed regulation. The GDPR, on the other hand, gives Member States a certain freedom to stipulate as of which age children can give consent to engage in online activities such as using a messenger app.

► 21. Does the draft regulation rely on the definitions of the child sexual abuse directive for the terms of "child" and "sexual consent"? If so, does this mean that we will have diverging definitions across member states what is a child and what is the age of sexual consent and what is the age as of which children can consent to use a messenger?

Response of the Commission's services:

Articles 2(2)(a) and 2(2)(c) of the proposal refer directly to definitions in the 2011 Child Sexual Abuse Directive, and the Directive's definition of 'child' ('any person below the

age of 18 years') is therefore applicable in these cases. Neither the GDPR nor the Child Sexual Abuse Directive harmonise age of consent (for data or sexual activities respectively).

The proposed Regulation does not refer to the 'age of sexual consent'.

► 22. Can the Commission provide us with a <u>comprehensive legislative mapping</u> of the difference between Member states as to these definitions?

Response of the Commission's services:

Member States are required to transpose the provision of the 2011 Child Sexual Abuse Directive into their national legislation, therefore the definition in Article 2(a) of the Directive of 'child' as 'any person below the age of 18 years' applies to all Member States.

<u>Consensual sexual activities between peers</u>

Art. 8 of Directive 2011/92/EU provides that Member states can foresee certain derogations for sexual activities where they are consensual and happen between peers, who are close in age and degree of psychological and physical development or maturity, in so far as the acts do not involve any abuse.

► 23. Can the Commission say which Member states have made use of this derogation and how this will interplay with this proposal, especially in case national rules on this differ, also taking into account diverging national rules on the age of sexual consent?

Response of the Commission's services:

Art. 8 of the Child Sexual Abuse Directive, as explained also in Recital 20, seeks to account for "consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies." Such consensual sexual activities, as a matter of principle, should not be criminalised. The Directive thus takes account of the fact that the age of legal liability for criminal behaviour is lower than 18 (e.g. 14 in Germany).

The existence of such a derogation does not affect the scope of the present proposal, which does not constitute criminal law. In such situations, e.g. if two children start sending each other images of themselves engaged in sexual acts with each other, the content might be identified as suspected child sexual abuse. Once reported to law enforcement, the existence of any criminal behaviour would be assessed. In Member States that have chosen to implement the derogation, no investigation would be pursued and the data would be deleted.

Data retention

The draft regulation does not include clear provision on data retention - According to Art. 3 e) of the draft regulation, "the relevant data" can be retained to respond for any proportionate request by law enforcement and other relevant public authorities.

► 24. How long will providers be allowed or required to retain communications data and personal data under this proposal? Who will decide what is proportionate? Couldn't this lead to different implementations by the Member States and thus fragmentation?

Response of the Commission's services:

The proposed Regulation requires as a general rule the immediate erasure of relevant data, yet allows for limited retention where necessary. Specifically, it allows for relevant data to be retained only for the time period necessary to respond to proportionate requests from law enforcement and other relevant public authorities, to block the concerned user's account and to create hashes.

The present proposal does specify that any data processed for the purpose of detecting and reporting child sexual abuse online or removing child sexual abuse material must be immediately deleted, with the sole exception of cases where abuse has been detected and confirmed as such.

The duration of the data retention period is a matter of national law, subject to applicable requirements stemming from other provisions of EU law.

► 25. Can the Commission explain what is meant by ""other relevant public authorities" and under what precise conditions and safeguards would they be able to access the "relevant data" and for what precise purposes?

Response of the Commission's services:

The use of the term 'other relevant public authorities' is intended to refer to authorities acting in the in the public interest against child sexual abuse who may have a legitimate interest in requesting the further preservation of the data concerned. These might include, for example, judicial authorities, or authorities involved in mutual legal assistance. This proposal does not create a legal basis for access to data by such authorities. As such, any access to data by these authorities would be subject to the usual applicable safeguards.

Use of data by law enforcement authorities

► 26. Under which legal regime national law enforcement authorities will deal with any positive hits? What happens if for example the national definition of solicitation of children, as transposed from the child sexual abuse directive, differs from the definition proposed in the draft regulation? For example, would

it be possible for German law enforcement authorities to request data and information from an Italian provider under this proposal?

Response of the Commission's services:

These issues are all outside the scope of this proposed Regulation.

Javier Zarzalejos, EPP, shadow

1. On the scope
1.1. Child prostitution

► 27. Why do the definitions in art. 2 of the proposal only single out 'child pornography' and 'pornographic performance'? Why was 'child prostitution' (art. 2(d) of Directive 2011/93/EU) not explicitly covered?

Response of the Commission's services:

The scope of the proposed Regulation, as set out in the strategy of 24 July 2020, is strictly limited to voluntary activities to detect and report child sexual abuse online and remove child sexual abuse material. The Commission considers that, insofar as behaviour constituting child prostitution under the 2011 Child Sexual Abuse Directive takes place online, it will in principle falls within the definitions of solicitation and pornographic performance in Article 2(2) of the proposed Regulation. Where behaviour relating to child prostitution takes place offline, this is outside the scope of the present proposal, as online service providers cannot reasonably be expected to have knowledge of offline behaviour and their voluntary measures do not relate thereto.

1.2. Known and unknown child sexual abuse content

According to the proposal, the temporary derogation should be replaced by the legislative proposal expected to be presented in Q2/2021. Based on the COM's Child abuse strategy, the legislation should include mandatory detection, removal and reporting of known child sexual abuse content.

► 28. Is our understanding correct that the scope of the new Regulation would thus be narrower than the temporary derogation from ePrivacy as the latter does not limit voluntary action to known content? In other words, wouldn't this mean that, following the adoption of the new Regulation, online grooming and the detection/removal of content that has not been identified as illegal would not be possible anymore?

Response of the Commission's services:

In the strategy the Commission does indeed commit to proposing, by Q2 2021, 'the necessary legislation to tackle child sexual abuse online effectively **including** by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities' (emphasis added).

As such, the scope of this long-term instrument is not expected to be limited to requiring relevant service providers to detect and report known child sexual abuse material, and it is not excluded that other measures may be included within the scope

of tackling child sexual abuse online effectively. The preparation of this proposal is currently underway, and will be subject to a detailed impact assessment which will help to determine the precise scope of the measures to be included. Irrespective of the final scope of the long-term legislation, the proposed Regulation will cease to apply on 31/12/2025 at the latest.

2. On technologies that can be used

The proposal refers to "state-of-the-art technology" and lays down criteria and safeguards such as human oversight and "common use" by the industry that have to be met. Moreover, it states that the technology should have existed before the entry into force of the regulation, although "further evolution in a privacy friendly manner" should be taken into account.

► 29. We acknowledge that the Regulation does not want to prescribe the use of specific technology but rather offer some flexibility to providers. However, the definition as it stands is rather vague and risks legal uncertainty, also for oversight bodies who would have to assess if technology used fulfils the criteria. For the sake of legal certainty, shouldn't the focus rather be on low error rates rather than on "common use"?

Response of the Commission's services:

It is important that any processing activities benefiting from the proposed derogation should indeed have low error rates, and for this reason Article 3(b) specifies that any technology used must limit 'to the maximum extent possible the rate of errors'.

► 30. Why is there a limitation to technology which existed before the entry into force of the Regulation? As we see with the TCO Regulation, the adoption of laws can take years. In the meantime, new technologies - which might be even more accurate in detecting content linked to child sexual abuse - might be developed in the meantime but could not be used.

Response of the Commission's services:

There is no universally accepted single technology, hence the language is such to accommodate this situation.
The text as it stands is a delicate balance of trying to ensure that the technology currently used can continue to be used while at the same time not closing the door to this existing technology evolving, so that improvements on those technologies that can make them less privacy intrusive can still be acceptable. The evolution of existing technologies towards more privacy-friendly versions of these technologies after the entry into force of the Regulation is allowed/not prohibited, as recital 11 indicates.

At the same time, the proposed Regulation would not apply to new technologies, which are not well established and regularly used before the entry into force of the proposal,

because of the interim and targeted nature of the proposed rules and the need for legal certainty as to which technologies are covered.

3. On the limitation of the application of the derogation until December 2025

► 31. In light of the uncertainty regarding the timetable of the negotiations on the ePrivacy Regulation and the future Regulation providing mandatory rules, would it not be better not to set an end-date?

Response of the Commission's services:

The proposed interim Regulation is not directly linked to the negotiations of the ePrivacy Regulation. However, the Commission strongly expects that the ePrivacy Regulation be adopted and enter into force much earlier than December 2025.

The proposed interim Regulation is temporary in nature for proportionality reasons. It aims to bridge the interim period until the long-term legislation to tackle child sexual abuse online, to be proposed in Q2 2021, is put in place while ensuring the respect of fundamental rights, including the rights to privacy and the protection of personal data. The clear end date of 31 December 2025 will ensure that the proposed Regulation does not become a permanent one. If the long-term legislation is adopted earlier, it would repeal this temporary legislation. The Commission's intention in coming forward with a long-term framework quickly is to enable the co-legislators to conclude on the legislation well before the end of 2025.

4. Other information request

► 32. Current state of the implementation of the Child Abuse Directive by each of the Member States?

Response of the Commission's services:

The Commission opened last year infringement procedures against 23 Member States for possible non-conformities in relation to the Child Sexual Abuse Directive.

The majority of issues concern situations in which the Commission had not received sufficient information from the Member State to ascertain the conformity of national law with the Directive, rather than major issues that require immediate action from Member States to fix.
Common issues concern the areas of **prevention** (in particular prevention programmes for offenders and for people who fear that they might offend), **criminal law** (especially the definition of offences and level of penalties), and **assistance, support and protection** measures for **child victims.**

► 33. Legislative measures taken by the Member States pursuant to Article 15(1) of Directive 2002/58/EC?

Response of the Commission's services:

The Commission services are not currently in a position to provide a complete mapping of the different national rules and practices currently in place regarding the detection of CSAM among Member States. The Commission's services have recently requested comprehensive information from the Member States and could make this available to the European Parliament once it is available.

It should be noted that the proposed Regulation seeks to create a temporary derogation from certain provisions of the ePrivacy Directive in relation to activities that are not currently within the scope of the Directive, but which will come within its scope upon the entry into application of the definitions of the European Electronic Communications Code on 21 December 2020.

Article 15 of the ePrivacy Directive permits Member States to restrict the scope of certain rights and obligations provided for in the Directive through national legislation which serves one of the listed purposes and meets the requirements of necessity and proportionality. Individual Member State legislation regarding the detection and deletion of CSA online would likely lead to fragmentation across the single market..

Sophie In't Veld, Renew, shadow

Definitions:

► 34. Can the Commission explain why the definition of "grooming" in the proposal differs from the one set out in Article 6 of Directive 2011/92/EU?

Response of the Commission's services:

The definition of solicitation in Article 6 of the Child Sexual Abuse Directive is not entirely applicable to the current voluntary activities of companies, since it requires not just the existence of a proposal to meet offline but also material acts leading to a meeting offline, which falls outside the scope of said voluntary activities.

If Article 6 of the Directive were to apply, service providers would have to establish the existence of such material acts leading to a meeting offline, which is necessarily to be done by the law enforcement, prosecuting authorities and/or (ultimately) judges in court proceedings. It is neither possible for providers to establish such facts outside the "digital sphere" – especially. not by means of technology.

Therefore, an appropriate definition had to be created, which appropriately reflects the current voluntary practices of service providers which this proposal aims to cover and retains as much as possible relevant elements of Article 6(2) of the Child Sexual Abuse Directive.

The activities listed in Article 2 (2)(b) of the proposal reflect the activities that are being detected by the service providers by for example relying on a combined assessment of behaviour-based signals such as messaging frequency, request for imagery or indication for planning in-person meetings.

For further details, please also see the Commission's response to Question 11 above.

Scope:

The proposal mentions that the *"Sole objective of this Regulation is to enable the continuation of certain existing activities aimed at combating child sexual abuse online".*

► 35. Can the Commission explain <u>which</u> exact activities it refers to? Which providers of number-independent interpersonal communications services fall under the scope of this Regulation?

Response of the Commission's services:

The activities referred to in the proposed Regulation are the processing of personal and other data in connection with the provision of number-independent interpersonal communications services strictly necessary for the use of technology for the sole purpose of removing child sexual abuse material and detecting or reporting child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse, subject to the conditions specified in Article 3 of the proposed Regulation.

The scope of Article 3 is limited to number-independent interpersonal communications services (NI-ICS), which can provide services on videos, images, text messages, as well as VoIP calls (to the extent that the latter are relevant).

► 36. Does the Commission consider that the criteria such as *"well-established", "regularly used", "state of the art"* meet the requirement of clear and precise rules in the light of the fundamental right to respect for private life and the relevant ECJ-case law? If so, can it explain how?

Response of the Commission's services:

Article 3 of the proposal provides for a series of safeguards. In particular, it seeks to ensure that the technologies used are the least privacy-intrusive and must have been well-established and regularly used by number-independent interpersonal communications services providers prior to the entry into force of the proposed Regulation. This is reflected in the wording of "state of the art", "well-established" and "regularly used". Recital 11 provides further explanations regarding the technologies.

► 37. Could the Commission please shed light on the interplay between Article 3(a) and 3(d) considering, inter alia, that point (a) requires the processing to be "proportionate" while point (d) requires the processing to be "limited to what is strictly necessary"?

Response of the Commission's services:

Article 3 provides for a series of safeguards to ensure that technologies benefitting from the derogation meet the standards of the best practices currently applied, and thereby limits the intrusiveness to the confidentiality of communications and the risk of circumvention.. While point (a) defines requirements that apply to the technologies used and requires processing to be proportionate, point (d) refers to the data processing and requires processing to be necessary. Point d) can be seen as a specification of the overall proportionality requirement in point a). Both necessity and proportionality are part of the proportionality test under Union law.

"The types of technologies deployed should be the least privacy-intrusive in accordance with the state of the art in the industry and should not include systematic filtering and scanning of communications containing text but only look into specific communications in case of concrete elements of suspicion of child sexual abuse."

► 38. Can the Commission explain how concrete elements of suspicion of child abuse can be detected in text if there is no systematic filtering and scanning of communications? How can solicitation of children specifically be detected if there is no systematic filtering or scanning? How can it be made sure that only specific communications in case of concrete elements of suspicion of child sexual abuse are detected? Can the Commission provide a list with key indicators for solicitation of children, beyond the two mentioned in Art 3(c)?

Response of the Commission's services:

The sentence above, included in Recital 11, was intended to refer only to text analysis for the purpose of detecting grooming situations, ensuring that grooming can only be detected when a combination of keywords and other concrete elements of suspicion of child sexual abuse are used (e.g. age difference, frequency of messaging to a certain group of users, etc), rather than solely based on keywords, for which the rate of false positives would likely be much higher.

Specific indicators used may vary from one technology to another. Some illustrative examples can be given, however they should not be taken to be descriptive of a single particular technology.

These indicators may include: a conversation taking place between an adult and a child who are not known to one another; or voluminous attempts by an adult user to contact underage users. These are just a few indicators that might be useful in developing a concrete suspicion. It should be noted that, in general, a concrete suspicion would be established using not just a single key indicator, but several key indicators which taken in combination are deemed to rise above a risk threshold.

► 39. Can the Commission give an overview of current technologies deployed to detect child sexual abuse material, known and unknown material, and grooming, including the precise criteria used, the rates of convicted criminals, false positives rates and shortcomings per technology used?

Response of the Commission's services:

Please see annex.

► 40. Does the scope of the proposal cover detecting illegal content in private clouds, for example by photo DNA ?

Response of the Commission's services:

The scope of the present proposal is strictly limited to number-independent interpersonal communications services. Private clouds are in principle storage and therefore normally not number-independent interpersonal communications services. The qualification of the service depends of course on the facts of the individual case.

► 41. Which algorithms are currently being used by providers of number-independent interpersonal communications services to detect CSAM and grooming? Is there any human review of such algorithms?

Response of the Commission's services:

The algorithms typically use artificial intelligence (AI) and machine learning and a combination of relevant key indicators such as keywords and objectively identified risk factors such as age difference or frequency of messaging to a certain group of users, to determine a risk score for the conversation to be possible grooming.

If the risk score is above a certain threshold, the exchange is sent to human review.

According to Microsoft, the purely automated detection through their grooming tool is 88%+ accurate.

For all processes, human review has to be ensured. The human review reduces the error rate to close to zero. Human review is already in place even for the most accurate technologies such as hashing.

Encryption:

Last week we received a note from the Commission on encryption. Several *"key considerations"* were set out for *"solutions for targeted lawful access by law enforcement and judiciary authorities to information in end-to-end encrypted communications, while ensuring that privacy and data protection is respected."*

Orders to access encrypted electronic communication must be targeted to specific individuals or groups of individuals in the context of the investigation of a specific crime, and be proportionate. They must be issued or be subject to prior validation by a judiciary authority. Transparent reporting procedures, as well as appropriate review and redress mechanisms are necessary. Technical solutions constituting a weakening or directly or indirectly banning of encryption will not be supported.

► 42. How does that relate to this proposal? If there is no systematic filtering or scanning of communications, but technical solutions currently employed by providers should be able to continue, how can encryption then not be directly or indirectly weakened?

Response of the Commission's services:

This proposed Regulation does not address or directly relate to encryption. The proposal creates a derogation to ensure that service providers may continue existing voluntary activities for the detection and reporting of child sexual abuse online and removal of child sexual abuse material.

The Commission's services are not aware of any service providers using hashing technology in end-to-end encrypted communications.

The Commission's services ' position on encryption remains unchanged and is reflected in the Commission's services note on encryption. Encryption, together with other measures, is crucial for protecting information, including personal data and reducing the impact of data breaches and security incidents but also allowing for secure identification systems. Encryption software should not be weakened or be made vulnerable (no "back-doors") and we should promote the principles of "security-by-design" and "privacy-by-design". However, the use of encryption should be without prejudice to the powers of competent authorities to safeguard national security and to prevent, investigate, detect and prosecute criminal offences, in accordance with the procedures, conditions and safeguards set by law.

► 43. Does the Commission consider that a judiciary authority would need to validate the activities mentioned in the proposal prior to breaking encryption? If not, why not?

Response of the Commission's services:

The proposal does not cover in any way encryption or lawful interception and therefore does not change current legislation related to those matters.

Safeguards:

► 44. Which actors get access to data obtained in case there is a concrete suspicion of child sexual abuse? How is it made sure that this is limited to what is necessary?

Response of the Commission's services:

Where the provider concludes that child sexual abuse online has been detected, the provider may then report the suspected abuse to relevant authorities. In general terms, there is currently no obligation in EU law to report child sexual abuse online, and this is a matter which may be addressed by the legislation to be proposed in Q2 2021 under the strategy of 24 July 2020. US service providers, if they choose to voluntarily detect child sexual abuse, are obliged under US federal law to report to NCMEC any visual depiction of apparent child pornography or other content relating to the incident such report is regarding. This obligation applies irrespective of the location of the users concerned, and NCMEC forwards reports to relevant law enforcement authorities in the US and other countries. NCMEC received over 725 000 such reports concerning the EU in 2019 which it forwarded to the relevant law enforcement agencies in the EU. Under the present proposal, providers of number-independent interpersonal communications services could continue to detect and report child sexual abuse online to relevant organisations, including to NCMEC, after 21 December 2020.

► 45. How will the Commission effectively enforce this Regulation, and how will it ensure that the burden of enforcement will not fall on the shoulders of

individual citizens who have suffered harm as a result of this measure, and who have to litigate in order to defend their rights?

Response of the Commission's services:

The individuals whose rights might be affected have the right to an effective remedy in accordance with Article 47 of the EU Charter of Fundamental Rights.

In addition, national supervisory authorities will be competent for the monitoring of the application of the proposed Regulation, including as to whether the conditions for its applicability of the derogation and the related safeguards are respected.

Moreover, as the GDPR is applicable where the conditions for the derogation are met, the national data protection authorities (DPAs) are also competent to the extent that personal data are processed. Therefore, all relevant provisions regarding safeguards, appeals and complaint mechanisms of the GDPR also apply.

► 46. Which possibilities for appeal/complaint mechanisms for those affected by "false positives" or otherwise wrongly suspected are foreseen?

Response of the Commission's services:

The proposal does not foresee review and redress mechanisms for users affected by the service providers' activities in question. Moreover, the onus should not be on the user to prove he or she is innocent, but the onus should be on the service provider to ensure the technology used is reliable. It is also noted that in practice, most if not all providers will notify the user once an image is removed and foresee a review possibility. Concerning review requests with regard to grooming, there are no known instances of where such a request has been lodged.

► 47. Does the Commission consider that prior consultation of the data protection supervisory authority is necessary where updates are installed that will modify the technology used by the service provider?

Response of the Commission's services:

As noted in recital 10 of the proposed Regulation, the GDPR would continue to apply to voluntary measures (also those that meet the conditions of Article 3 of the proposal) for the detection and reporting of child sexual abuse online and removal of child sexual abuse material, to the extent that such measures involve the processing of personal data. The national DPAs are competent for the monitoring of the correct implementation of the GDPR provisions (incl. on prior consultation). Article 36 of the GDPR provides that the controller should consult the national DPA if the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures mitigating that risk. Article 35 provides for conditions when the data protection impact assessment is necessary. If the processing is likely to result in a high risk and in particular when new technologies are used, data protection impact assessment should be carried out. DPAs may add such a possibility to their lists of processing where impact assessment is required, if they deem necessary.

Data retention:

► 48. Over what period of time should relevant data be stored and are these storage periods in line with the requirements of ECJ case law? Or is there a maximum storage period for the separated material?

Response of the Commission's services:

This proposal does not set any rules on data retention.

The proposal foresees that the data need to be erased immediately, unless child sexual abuse online is detected and objectively confirmed as constituting child sexual abuse online. In the latter case, the data can only be retained for as long as necessary for the specific activities listed, which are in line with the objectives of the proposed Regulation.

Furthermore, various situations require different retention periods (e.g. reporting, providing evidence for LEAs, etc.). Therefore, the proposal does not contain a fixed time period for the situations where data may exceptionally need to be retained for a limited period of time.

The existence of any possible obligation to retain data as well as the duration of the data retention period is a matter of national law, subject to the need to comply with any other applicable provisions of Union law.

Transparency:

► 49. How and where will providers of number-independent interpersonal communications services publish annual reports? Does the Commission agree that a standardised questionnaire helps to get standardised, quantitative statistics instead of only case studies (such as the case with PNR)? Will the Commission publish a review report including an evaluation of the annual reports published by the providers? Which measures will the Commission take in case providers fail to publish a report, or have not published all required information?

Response of the Commission's services:

Under the proposed Regulation, service providers benefitting from the proposed Regulation would need to publish annual reports. They could do so for instance online.

In general terms, quantitative, as well as qualitative information is important in the context of understanding the effectiveness of the technologies used as well as the scale of child sexual abuse online. Article 3, and the related Recitals, require a series of quantitative data. While there could be some benefit to standardised questionnaires in the recording of such data, it should also be noted that due to the differences between the various technologies used, including particular implementations, a standardised questionnaire may not be able to capture all relevant data.

The national authorities would be competent for the enforcement of this proposed Regulation, in particular in respect of its scope and whether the conditions in Article 3 are met.

In addition, oversight of service providers' activities in relation to the processing of personal data is within the competence of the relevant national supervisory authorities.

In the event that a service provider fails to meet a condition listed in the proposed Regulation, it will principally be for the competent authorities to take any appropriate action where necessary. In this respect the application of the derogation provided for in the proposed Regulation is conditional on compliance with the cumulative requirements of Article 3.

Patrick Breyer, Greens, shadow

1. The Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse state that "*'child sexual abuse material' would arguably encompass a narrower set of acts than 'child pornography', since the latter could go beyond the representation of an act of sexual abuse against a child. This is precisely where the term 'child sexual exploitation material' becomes particularly important, because it encompasses material that sexualises and is exploitative to the child although it is not explicitly depicting the sexual abuse of a child.*"

► 50. Does the Commission agree that the proposed regulation should use the term "child sexual exploitation" instead of "child sexual abuse" because it is to encompass all kinds of "child pornography"?

Response of the Commission's services:

In the case of the proposed Regulation, the scope of the derogation is restricted to "child sexual abuse" as defined in Article 2(2), including the material defined as 'child pornography' in the 2011 Child Sexual Abuse Directive. As described in the Luxembourg Guidelines, '"child sexual abuse material" is used to describe a subset of "child sexual exploitation material" where there is actual abuse or a concentration on the anal or genital region of the child.' The Commission services observe that, based upon this description, the term 'child sexual abuse material' is the terminology which most closely matches the definition of 'child pornography' in the 2011 Directive. While the term 'child sexual exploitation material' would imply a broader scope, this might introduce additional legal uncertainty, potentially affecting error rates in detection technology.

► 51. Apart from E-Mail and Messaging services, which types of services constitute "number-independent electronic communications services"? For example, are online games, services such as Skype, the provision of Internet access, by fixed line or by wifi, dating apps, apps used to find and communicate with people in the neighborhood, based on the user's location, "number-independent electronic communications services" and covered by the scope of the proposed regulation?

Response of the Commission's services:

Art. 2(5) of the European Electronic Communications Code (EECC),[4] states that 'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s)

[4] Directive (EU) 2018/1972, Articles 2(5) and (7)

and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service'. Art. 2(7) states that 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans'.

Whether a service constitutes a number-independent interpersonal electronic communications service will depend on the specifics of that service, and so it is only possible to respond to the examples above in general terms. Recitals 15-18 of the EECC provide guidance in that respect.
In particular:

Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service. These elements have to be assessed on a case-by-case basis.

-the provision of internet access services (either by fixed line, Wi-Fi or mobile) cannot be considered as NI-ICS;

-the communications features of dating apps may constitute NI-ICS, unless they are merely ancillary features;

-communications apps may constitute NI-ICS.

► 52. Which companies (e.g. Facebook) currently providing number-independent electronic communication services filter communications content for previously classified CSEM (child sexual exploitation material), to the knowledge of the Commission? (please provide names of companies!)

Response of the Commission's services:

According to the information available to the Commission's services , companies which currently voluntarily detect known child sexual abuse material in their number-independent interpersonal communication services include Facebook, Google, and

Microsoft. PhotoDNA, one of the most used tools to detect previously known CSAM, is used by more than 150 organisations (service providers, child protection organisations, law enforcement authorities and other public authorities) across the globe.
See annex for a list of companies that reported to NCMEC in 2019, using technologies to detect child sexual abuse online.

► 53. Which number-independent electronic communication services **(e.g. Facebook messenger) filter communications content for** previously classified **CSEM, to the knowledge of the Commission? (please provide names of services!)**

Response of the Commission's services:

According to the information available to the Commission's services , number-independent electronic communications services which currently voluntarily detect known child sexual abuse material in their services include Facebook Messenger, Gmail, Yahoo Messenger, and Kik Messenger.

► 54. Which companies currently providing number-independent electronic communication services filter communications content for yet unknown CSEM (child sexual exploitation material), to the knowledge of the Commission? (please provide names of companies!)

Response of the Commission's services:

The Commission's services do not have a list of such companies. According to NCMEC, in 2019, there were **40 000 images** and more than **100 000 videos** sent to law enforcement agencies in the EU that had not been seen before, from all services reporting to NCMEC (including number-independent interpersonal communications services, hosting service providers, and other services, see annex). 27% percent of the reports concerning the EU containing potentially new image files stemmed from a chat, messaging, or email service, in absolute numbers 3 756 reports.[5] Please see annex on NCMEC data for more details. A report may contain multiple images and videos.

► 55. Which number-independent electronic communication services **filter communications content for** yet unknown **CSEM, to the knowledge of the Commission? (please provide names of services!)**

Response of the Commission's services:

See response to previous question.

[5] As explained in response 51 not all 'chat services' do necessarily constitute number-independent interpersonal communications services. According to NCMEC, their classification of "chat" refers to services they know are only messenger or where the premise of the platform is specifically for chatting.

► 56. Which companies currently providing number-independent electronic communication services search communications content for potential grooming/solicitation, to the knowledge of the Commission? (please provide names of companies!)

Response of the Commission's services:

According to the information available to the Commission's services, such companies include Microsoft, which has made their technology available to other organisations via Thorn, and Facebook.

► 57. Which number-independent electronic communication services **filter communications content for potential** grooming/solicitation**, to the knowledge of the Commission? (please provide names of services!)**

Response of the Commission's services:

According to the information available to the Commission's services , number-independent electronic communications services which currently voluntarily detect grooming/solicitation in their services include Microsoft's Xbox. Recital 17 of the EECC clarifies that, in exceptional circumstances, a service should not be considered to be an interpersonal communications service if the interpersonal and interactive communication facility is a minor and purely ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. As elements of an exemption from the definition the terms 'minor' and 'purely ancillary' should be interpreted narrowly and from an objective end-user's perspective. An interpersonal communications feature could be considered to be minor where its objective utility for an end-user is very limited and where it is in reality barely used by end-users. An example of a feature that could be considered to fall outside the scope of the definition of interpersonal communications services might be, in principle, a communication channel in online games, depending on the features of the communication facility of the service. These elements have to be assessed on a case-by-case basis.

In 2019, there were more than **11 000 reports** concerning grooming/solicitation sent to law enforcement agencies globally. 61% (6 818)of these reports occurred within a chat, messaging, or email service, while an additional 36% (4 040) of incidents occurred on a social media or online gaming platform that had messaging or chat capability. 240 reports concerned the EU, of which 23% (55) occurred within a chat, messaging, or email service, i.e. services which normally qualify as number-independent interpersonal communications services, while an additional 75% (180) of

incidents occurred on a social media or online gaming platform (where messaging is possible according to NCMEC)-.[6] For more details, see the NCMEC report in annex

► 58. How many users per day are affected by the searches, and how many of them actually share CSEM?

Response of the Commission's services:

The Commission's services do not possess this information, which would require an exhaustive analysis of all number-independent interpersonal communications services operating in the Union.

► 59. Where algorithms/AI are used to detect yet unknown **CSEM, how many messages per day are flagged by the algorithms for possible CSEM content?**

Response of the Commission's services:

The Commission's services do not possess this information, which would require an exhaustive analysis of all number-independent interpersonal communications services operating in the Union.

► 60. Where algorithms/AI are used to detect yet unknown CSEM, what is the rate of false positives for algorithms mostly used (i.e. of 100 hits flagged by the algorithm how many turn out to actually contain CSEM)?

Response of the Commission's services:

According to Thorn, its Safer tool has an accuracy of 99% in the detection of unknown material in its automated part, before the hit is sent to human review, where the accuracy reportedly increases to practically 100%.

► 61. Where algorithms/AI are used to detect potential grooming/solicitation**, how many messages per day are flagged by the algorithms for possible grooming?**

Response of the Commission's services:

The Commission's services do not possess this information, which would require an exhaustive analysis of all number-independent interpersonal communications services operating in the Union. See response to question #57.

► 62. Where algorithms/AI are used to detect potential grooming/solicitation, what is the rate of false positives for algorithms mostly used (i.e. of 100 hits flagged by the algorithm how many turn out to actually constitute grooming)?

Response of the Commission's services:

[6] As explained in response 51 not all 'chat services' do necessarily constitute number-independent interpersonal communications services. According to NCMEC, their classification of "chat" refers to services they know are only messenger or where the premise of the platform is specifically for chatting.

According to Microsoft, the purely automated detection through their grooming tool is 88%+ accurate. This process is always subject to human review, where the accuracy reportedly increases to practically 100%.

► 63. What percentage of reports received by NCMEC is actually forwarded to law enforcement agencies?

Response of the Commission's services:

To the Commission's services' knowledge, all the reports that NCMEC receives that concern the EU are forwarded to law enforcement agencies in the EU.

► 64. Which technologies are currently used to detect

known CSAM images and videos;

unknown CSAM images and videos

solicitation?

Please provide a full list of products, manufacturers and sources of known material (hash databases).

Response of the Commission's services:

It is not possible to provide a complete list of products, manufacturers and sources of known material, however the following non-exhaustive list can be provided. The inclusion of any given technology/tool in this list should not be considered an endorsement. Neither should the fact that a given technology/tool may not be listed be taken to indicate that it is necessarily disqualified from the scope of the proposed derogation or otherwise unsuitable.

Technologies used include Microsoft's PhotoDNA[7], PhotoDNA for Video[8] and Project Artemis[9]; Facebook's PDQ[10] and TMK+PDQF[11]; Google's Content Safety API[12]. YouTube CSAI Match[13] and Google AI technology[14]; CloudFlare's CSAM Scanning Tool[15]; and Thorn's Safer[16]. In addition to tools designed with the detection of child

[7] PhotoDNA
[8] How PhotoDNA for Video is being used to fight online child exploitation
[9] Microsoft shares new technique to address online grooming of children for sexual purposes
[10] Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer
[11] Ibid
[12] Fighting child sexual abuse online
[13] YouTube CSAI Match
[14] Using AI to help organizations detect and report child sexual abuse material online
[15] Announcing the CSAM Scanning Tool, Free for All Cloudflare Customers
[16] Safer: building the internet we deserve

sexual abuse online as one of their primary objectives, many other generic tools can be used for these purposes (e.g. various hashing algorithms).

Hashes of known material may be maintained by reporting hotlines (e.g. NCMEC[17], the Internet Watch Foundation Hash List[18]), by law enforcement (e.g. Interpol International Child Sexual Exploitation Database[19], UK Child Abuse Image Database[20]), by service providers[21] or by other organisations (e.g. THORN Industry Hash Sharing Platform[22]) and, where appropriate and lawful, these hashsets may be made available to service providers.

► 65. Have these or similar products been used or are they used to also detect other types of content, e.g. terrorist content online, copyrighted content? If so: Does the Commission accept that those detections would no longer be possible after 21st December 2020?

Response of the Commission's services:

The scope of the proposed Regulation is strictly limited to the voluntary detection and reporting of child sexual abuse online and removal of child sexual abuse material. The detection of the types of content mentioned above is outside the scope of the proposed Regulation. PhotoDNA and Microsoft's anti-grooming technology is made available to other organisations under strict licensing conditions for the sole purpose of the fight against child sexual abuse. The ePrivacy Directive fully applies to all other activities of number-independent interpersonal communication services falling within the Directive's scope, as spelled out in recital 17 of the proposal.

► 66. Will the Commission agree that the proposed legislation will serve its purpose only if it complies with fundamental rights and if the processing described is in line with the GDPR?

Response of the Commission's services:

The Union legislation must comply with the fundamental rights forming part of the Union law. Personal data processed within the scope of the derogation provided for by the proposed Regulation, must be in line with the GDPR. The Commission does not take a position on the conformity of the current voluntary practices by operators with the GDPR, which falls into the competence of the national DPAs.

[17] Is Your Explicit Image Out There?
[18] Hash List
[19] Global efforts to identify child abuse victims via INTERPOL boosted with Microsoft technology
[20] Child abuse image database
[21] Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values
[22] Industry Hash Sharing – Reporting Child Sexual Abuse Content

► 67. Can the Commission share the assessment of its legal service with regards to the proportionality and necessity of the proposed legislation on scanning all communication content of all users, in particular in light of the CJEU case-law on data retention and Schrems?

Response of the Commission's services:

This proposal, as any legislative proposal adopted by the Commission, has been assessed by the Commission's legal service. That assessment covered all relevant legal aspects, including compliance with the Union legal principle of proportionality.

This proposal does not create a new legal ground for processing or modify the existing legal basis in relation to data retention or international data transfers.

► 68. The derogation would exempt certain activities of providers from the e-Privacy Directive, but those would then fall into the scope of the GDPR. Did the Commission assess whether the current practices to detect CSEM/solicitation are in line with the GDPR, particularly regarding the general and indiscriminate nature as well as the disclosure of personal data to NGOs and law enforcement agencies in third countries that lack an adequate level of data protection?

Response of the Commission's services:

The enforcement of the GDPR is entrusted to the national data protection authorities. The proposed Regulation only provides a derogation from the application of certain provisions of the ePrivacy Directive and does not create a legal basis for the described processing. The proposed Regulation does not take a position on the legality of the current practices, which falls into the competence of the national DPAs.

The primary purposes of this proposal is to enable service providers to continue certain voluntary activities to report child sexual abuse online. The proposal sets out the behaviours and material which constitute child sexual abuse online in the definition of that term in Article 3.

The Commission's services have not conducted a detailed assessment of the data protection aspects of current practices to detect and report child sexual abuse online and remove child sexual abuse material.

► 69. Can the Commission share the assessment of its legal service with regards to compliance with the GDPR in terms of (at least)

purpose limitation,

data minimisation,

data protection by design and by default,

the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child,

proportionality and necessity of the data processing

Response of the Commission's services:

This proposal, as any legislative proposal adopted by the Commission, has been assessed by the Commission's legal service. That assessment covered all relevant aspects, including compliance with the GDPR.

This proposal does not create a new legal ground for processing or modifys the existing legal basis in relation to data processing.

Relevant service providers are obliged to ensure their processing of personal data is in compliance with GDPR obligations at all times, and oversight of this processing is the responsibility of the relevant data protection authorities.

► 70. Can a Regulation establish derogations from a Directive, which has been transposed into Member State law? Will this mean that the relevant provisions in Member State law would be inapplicable, based on the Regulation?

Response of the Commission's services:

As a Regulation, the proposed legal act would be binding and directly applicable in all Member States, and would introduce a derogation from Articles 5(1) and 6 of the ePrivacy Directive.

► 71. Does the Commission agree that communications data are in the same category as special categories of data in the meaning of Article 9 GDPR?

Response of the Commission's services:

Some of the communications data may indeed qualify as a special category of personal data in the meaning of Article 9 GDPR. In any case, the GDPR is fully applicable (including safeguards).

► 72. How many CSEM have been reported by companies so far? How many of the NCMEC reports to EU law enforcement authorities have resulted in

1/ the decision not to open a criminal investigation
2/ criminal investigations
3/ arrests
4/ convictions
5/ saving abused children?

Response of the Commission's services:

According to the information available to the Commission's services, the past few years have seen a dramatic increase in reports of child sexual abuse online concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.): from 23 000 in 2010 to more than 725 000 in 2019, which included more than 3 million images and videos. A similarly dramatic increase has occurred globally: from 1 million reports in 2010 to almost 17 million in 2019, which included nearly 70 million images and videos. Overall, according to NCMEC, 73% of these reports stemmed from a chat, messaging, or email service. 69% of the reports concerning the EU stemmed from a chat, messaging, or email service.

In total, companies have reported to NCMEC **431 million images and 99 million videos** containing CSEM using technologies to detect child sexual abuse online, , including all types of service providers (including number-independent interpersonal communications services, hosting service providers, and other services, see annex).

Law enforcement does not systematically compile the statistics requested. The following sample cases from across the EU and beyond illustrate the key role that the voluntary activities of the type to be covered by the proposed Regulation play in rescuing children from ongoing abuse and arrest offenders:

Sample cases in Denmark:

- Case # 1:
  - Following reports from KIK alerting of the distribution of child sexual abuse material through **KIK Messenger**, Danish authorities arrested, a Danish national in his forties with no criminal record.
  - During preliminary examination of his mobile phone, Danish police found several recordings of himself abusing his **10 year old daughter**.
  - The **10 year old victim was rescued** and the suspect is undergoing criminal proceedings.

- Case #2 - Operation Umbrella[23]:
  - Facebook reported to the National Center for Missing and Exploited Children (NCMEC) the distribution of videos via **Facebook Messenger**[24] depicting a Danish boy and a girl who were engaged in sexual activity.
  - NCMEC forwarded the case to Denmark via Europol.

[23] This case was also included in the 2018 Internet Organised Crime Threat Assessment, p. 32, Europol.
[24] The case was also reported in the media (in English).

- Over 1000 people had distributed the videos to one or more people via Facebook Messenger and were charged for distribution of child pornography.
- This operation, still ongoing, is the single **largest operation ever** against child sexual abuse in Denmark.

Sample cases in Sweden

- Case # 1:
  - Swedish police received a NCMEC report alerting that one person had shared two child pornographic images on **Facebook Messenger** of material known to the police.
  - Swedish police carried out a search at the suspect's home and found child sexual abuse material in hard drives.
  - The material included the suspect **abusing his stepdaughter**, who was **rescued** in the operation.
  - The suspect was sentenced to nine years in prison for, among other things, gross rape against children.
- Case # 2:
  - Swedish police received a report from the National Child Exploitation Coordination Centre in Canada in which a person was sharing child sexual abuse material through **KIK Messenger**.
  - A house search was conducted in which child sexual abuse material was found.
  - Thanks to the investigation, **nine Swedish children** were identified.
  - The suspect was sentenced to four years in prison for different child pornography offenses.
- Case # 3:
  - Swedish police received a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
  - The investigation revealed that a female suspect was producing child sexual abuse material with the children of her romantic partners and sharing it with another male.
  - Further investigation revealed a network of two other female producers and three male consumers of child sexual abuse material.
  - **11 victims** were identified and rescued, ranging from ages 2 to 14 when the crimes occurred, out of more than 50 victims in total.

Sample case in Ireland (Matthew Horan case[25])

- Law enforcement in Ireland received in 2013 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The material was detected by Microsoft when Matthew Horan used a **Gmail** account to send child sexual abuse material to an email address on **Microsoft's** platform.
- The report led to an investigation in which it was discovered that Horan had been sexually exploiting children.
- Irish police identified **six victims** in Ireland as a result of the investigation.

[25] The case was also reported in the media.

Sample case in Romania[26]

- Romanian police received in 2016 a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
- The investigation revealed that a mother had been abusing her **9 year old daughter** for more than a year and sent the material generated in the sexual abuse to her boyfriend (not the father of the girl) in England.
- The mother was arrested and **her daughter was rescued**.

Sample case in Spain

- Law enforcement in Spain received a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The investigation by law enforcement in Spain led to the arrest of one person, who actively shared online with other child sex offenders the child sexual abuse material he produced.
- The person arrested produced that material by abusing children within his family circle.
- Given the gravity of the situation, law enforcement focused on locating the victims, eventually **rescuing 2 children** within the family circle.

Sample cases in Austria

- Case # 1
  - Austrian law enforcement received in 2019 a report from NCMEC submitted by Facebook alerting of the distribution via **Facebook Messenger** of images and videos of minors performing sexual acts.
  - The investigation led to the identification of a Slovak citizen living in Austria who forced minors through the threat of violence to produce images and videos of themselves performing sexual acts and to send them to him. The material was also distributed online to other users.
  - The report led to the identification of all **30 victims.** The suspect was arrested and convicted to five years of imprisonment.
- Case # 2
  - Austrian law enforcement received in 2019 a report from **KIK Messenger** alerting of the distribution of child sexual abuse material.
  - The investigation led to the identification of an Austrian citizen.
  - The search of his house and further investigations revealed that he sexually abused his **2 year old daughter,** who was **rescued**.
- Case # 3
  - Austrian law enforcement received in 2019 a report from **Snapchat** alerting of the distribution of child sexual abuse material.
  - The investigation led to the identification of an Austrian citizen who had forced several female minors to produce nude images of themselves and provide them to him, under the threat of making publicly available images and videos he made in the bathroom of a soccer field while acting as a referee.
  - The report led to the identification of a **large number of victims**.

[26] The case was reported in the media, see here and here.

Sample cases in France:

- Case # 1:
  - French police received in 2018 a NCMEC report submitted by Facebook alerting of the distribution of child sexual abuse material via **Facebook Messenger**.
  - The investigation revealed that the offender provided **PlayStation codes** to young boys in exchange of child sexual abuse material.
  - The offender was arrested. There were around **100 victims**.

- Case # 2:
  - French police has received a number of cases from NCMEC submitted by KIK alerting of the distribution of child sexual abuse material via **KIK Messenger.**
  - The cases typically involve multiple offenders (up to **20 offenders** per case).
  - The cases have led to **multiple arrests**.

Sample case in Greece

- Greek police received two NCMEC reports submitted by Yahoo! informing about a user who exchanged child sexual abuse material via **Yahoo!'s messenger** service.
- The house search of the offender revealed that he was also in contact, via Skype, with individuals (mothers of underage children) in the ASEAN region and was sending money to them so they would send him indecent pictures of their underage children.
- The ASEAN authorities were notified of all the details.

Sample case in Bulgaria

- Law enforcement in Bulgaria received in 2018 a report from the National Child Exploitation Coordination Centre alerting of the distribution of child sexual abuse material through **KIK Messenger**.
- The report led to a criminal investigation in which two mobile phones from a suspect were seized, containing 517 video files with child sexual abuse material.
- The material included videos with **brutal scenes of child sexual abuse** with a child around **2 years old**.

Sample case in Germany:

- German Federal Police received a NCMEC report in July 2019 submitted by Facebook alerting of the distribution via **Facebook Messenger** of material showing the sexual abuse of a very young girl.
- The NCMEC report also indicated that the material could have been recently produced.
- The report led to a criminal investigation and a house search in which a suspect was incriminated with abusing **his 4 year old daughter, and his 10 year old son**, who were **rescued and safeguarded**.

Sample case in the Czech Republic

- Law enforcement in the Czech Republic received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**, initiated by **Google**.
- The report led to a criminal investigation in which a 52 year old man was arrested following a house search, where additional child sexual abuse material was found.
- This person had abused **2 girls** and recorded the abuse. The 2 girls were identified and rescued.

Sample case in Estonia

- Law enforcement in Estonia received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The report led to a criminal investigation in which a person was arrested for exchanging and possessing child sexual abuse material.

Sample case in the UK

- Law enforcement in the UK received a **Twitter** referral via NCMEC regarding the use of direct messages to send and receive child sexual abuse material.
- Following dissemination of an intelligence package to UK Police, the suspect was arrested.
- Safeguarding measures were taken in respect of the suspect's **3 children** who resided with him.

Sample case is Switzerland

- Law enforcement in Switzerland received in 2016 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**, initiated by **Google**.
- The report led to a criminal investigation in which a 45 year old man was arrested following a house search, where additional child sexual abuse material was found.
- The man was also suspected of **abusing his niece (child).** The suspect had also filmed minors secretly and provided the videos to other people.

Sample cases in the US

- Case # 1 (Kevin R. Hyde case)[27]:
  - US law enforcement received in 2017 a report from NCMEC submitted by **AOL** alerting that the owner of an email address had on at least 25 occasions sent an email to himself at three different IP addresses and which had images attached to them, many of which appeared to contain child sexual abuse.

[27] As reported in the press release from Queens District Attorney, see here.

- The police alleged reviewed the thirteen videos and sixteen images included with the report and found that they depicted young girls ranging in age **from three years old to approximately ten years** old being sexually abused.
- A search warrant was executed at the suspect's residence and various computer and electronic equipment were seized. The suspect allegedly stated to police, **that he created the account in 2015 for the purpose of downloading child pornography of children**, that he would **email the images and videos to himself** to save, that he would trade images containing child exploitation with other individuals through his email and that he created another account to save the images.

- Case # 2 (Rev. W. Thomas Faucher case)[28]:
  - US law enforcement received in 2018 a report from NCMEC alerting of the distribution of child sexual abuse images by **email**.
  - The report led to a criminal investigation that revealed that the email account belonged to a retired Catholic priest who had expressed a desire to have sex with boys, had "satanic desires," and that "the thought of killing someone" was exciting to him.
  - More than 2,500 illegal files containing violent child pornography were recovered from Faucher's computer, cell phone, and Dropbox account.
  - Authorities also revealed the priest shared his fantasies with other pedophiles online.

- Case # 3 (Dabbs Postma case)[29]:
  - US law enforcement received in 2017 a report from NCMEC submitted by Facebook alerting of the exchange between two users via **Facebook Messenger** between Aug. 4 and Oct. 25 of **hundreds of photos and videos** containing child sexual abuse.
  - The report led to a criminal investigation in which Postma's home was searched. The police found a video showing him abusing **a young girl**.
  - Postma admitted to producing child pornography and having a sexual relationship with the girl, who was safeguarded.

- Case # 4 (Juan Rolando Lafuente case)[30]:
  - US law enforcement received in 2018 a report from NCMEC submitted by Facebook alerting of the exchange between two users via **Facebook Messenger** of child sexual abuse material.
  - The report led to a criminal investigation in which the police found in Lafuente's computer images of nude children performing sexual acts and in his phone videos of children engaging in sexual activity.
  - The suspect (59) was arrested and charged with two counts of possession of a photograph of sexual performance by a child and two counts of promoting pornography by a child.

---

[28] The case was reported in the press, see here.
[29] The case was reported in the press, see here.
[30] The case was reported in the press, see here.

- Case # 5 (Thomas William Barnes case)[31]:
  - US law enforcement received in 2017 a report from NCMEC submitted by **Yahoo** alerting of the sharing of child sexual abuse material via **email.**
  - The report led to a criminal investigation in which the police searched the suspect's computer and found multiple folders of child sexual abuse material.
  - The suspect, 67-year-old Thomas William Barnes, was a former spokesman for Florida's child welfare agency. He was charged with multiple counts related to child pornography.

► 73. Do all Member States deal with NCMEC reports in the same way or are there differences? (please explain)

Response of the Commission's services:

As the cases above illustrate, NCMEC reports are a key source of leads for law enforcement agencies in the EU to rescue children from ongoing abuse and to arrest perpetrators. In general, when law enforcement in Member States receive a NCMEC report marked as priority (e.g. imminent danger to children or ongoing abuse), all Member States prioritize these reports.

That said, the concrete and detailed ways in which Member States deal with other type of reports varies, based on national law, capabilities and procedures applicable to the Member State's law enforcement and judicial authorities.

► 74. What is the assessment of the Commission on the capacity of the police and justice departments in the Member States to ensure a follow up of NCMEC reports, including the capacity to evaluate confiscated data? What is needed in order to provide sufficient capacity? Are there differences between the Member States?

Response of the Commission's services:

The Commission's services recognise that the large volume of reports currently received by Member States' authorities from NCMEC represents a significant challenge in terms of capacity in terms of both human resources and the available technological and legal tools. For example, in cases where a NCMEC report relates to data stored in another country, particularly a third country or a Member State which does not participate in the European Arrest Warrant, mutual assistance processes can lead to significant delays in progressing investigations and prosecutions.

[31] The case was reported in the press, see here.

As highlighted in the EU strategy for a more effective fight against child sexual abuse, adopted on 24 July 2020, effectively fighting child sexual abuse also requires **cutting edge technical capacities**. Some national investigation teams lack the necessary knowledge and/or tools e.g. to detect child sexual abuse material in a vast number of seized photos or videos, to locate victims or offenders, or to conduct investigations in the darknet or in peer to peer networks. To **support the development of national capacities to keep up with technological developments**, the Union provides funding to Member States through the **Internal Security Fund** (ISF-Police)[32]. In addition, the Union also provides funds under **ISF-Police** through Union Actions, which include, for example, calls for proposals and procurement to fight the **online and offline** aspects of child sexual abuse. Examples of projects funded in the 2018 call for proposals include AviaTor, which specifically focuses on supporting Member States to effectively manage NCMEC reports. A **new call for proposals** in the area of combatting child sexual abuse will take place by the end of **2020.** The Commission also funds **research** projects under **Horizon 2020** to support the development of national capacities (in law enforcement and other areas) to fight against child sexual abuse, including the management of NCMEC reports (see for example GRACE project). Future calls for proposals to fight these crimes will open under the new **Horizon Europe** framework programme on research and innovation.

► 75. Are there statistics on the volume of CSEM exchanged via secure, interception-proof channels in the past years?

Response of the Commission's services:

The Commission's services do not have such statistics. The Commission's services are not aware of any service providers using hashing technology in end-to-end encrypted communications.

► 76.Why is there no requirement in the proposal to create communications content hashes on device?

Response of the Commission's services:

The scope of the proposal is strictly limited to enabling current voluntary measures to continue, subject to compliance with certain conditions and on a provisional basis. The imposition of any obligations upon service providers to process data is outside the scope of the proposal. The imposition of an obligation to create hashes of content, whether on- or off-device, is consequently also out of its scope.

[32] More information is available here.

► 77.Why is there no requirement in the proposal to clearly indicate the filtering to the user, and to flag it to the competent data protection authority for possible investigation?

Response of the Commission's services:

The processing of any personal data under the proposed derogation is and remains subject to the requirements of the GDPR, including the GDPR's obligations to provide data subjects with information relation to the processing of personal data.

► 78. Why is there no requirement in the proposal regarding the maximum permissible rate of false positives of the algorithm used, independent certification/audit of the algorithm, public reporting of the number of false positives?

Response of the Commission's services:

The proposal includes a requirement for service providers benefiting from the derogation to report the number of false positives on an annual basis.

The proposal foresees that existing technologies for the detection and reporting of child sexual abuse online and the removal of child sexual abuse material may continue to evolve to further enhance privacy protections (e.g. by further reducing the error rate in the automatic detection part). Article 3(a) specifies that the processing must be must be limited to technologies 'that are in accordance with the state of the art used in the industry and are the least privacy-intrusive'. The proposed wording allows for a standard which can evolve to be less-privacy intrusive over the lifetime of the proposed Regulation.

► 79. Why is there no requirement in the proposed legislation for the provider to perform a human verification of a "match" before disclosing content to third parties?

Response of the Commission's services:

According to the information available to the Commission's services , in practice, where voluntary measures for the detection of child sexual abuse online result in a 'match', service providers typically also require human review before a report is made.

► 80. Why is there no requirement in the proposed legislation to notify users whose content has been examined by a human to allow for judicial review?

Response of the Commission's services:

The processing of any personal data under the proposed derogation is and remains subject to the requirements of the GDPR, including the GDPR's obligations to provide data subjects with information relation to the processing of personal data.

NCMEC cites the following reasons for the rising number of CSEM reports: Wide-spread voluntary adoption by service providers of upload filters; growing international scope of child sexual abuse; generally increased use of U.S.-based social media, mobile-based apps, and chat and photo-sharing programs by members of the public from around the world; decreased financial and access barriers to using the Internet to facilitate storing and sharing of data.

► 81. Does the Commission agree that these are the main causes for the rising number of reports?

Response of the Commission's services:

The President and Chief Executive Officer of NCMEC, in his statement to the United States Senate Committee on the Judiciary[33], stated that multiple factors 'contribute to the exponential increase in reports to NCMEC's CyberTipline, including the following:

- Wide-spread voluntary adoption by ESPs (Electronic Service Providers) of new technologies to locate and remove child sexual exploitation content from their platforms and services;
- Growing international scope of the crime;
- Increased use of U.S.-based social media, mobile-based apps, and chat and photo-sharing programs by members of the public from around the world; and
- Decreased financial and access barriers to using the Internet to facilitate storing and sharing ever-larger volumes of child sexual abuse images and videos.'

The Commission's services note that the term "electronic service providers", as used in the relevant US law, is a broader term than the term "number-independent electronic communication services", as used in relation to the proposed Regulation.

[33] Statement by John F. Clark, President and Chief Executive Officer, National Center for Missing and Exploited Children, for the United States Senate Committee on the Judiciary "Protecting Innocence in a Digital World", July 9 2019

Cornelia Ernst, GUE, shadow

► 82. We would like to have a full list of national laws providing for derogations pursuant to Art. 15 of the e-privacy directive, clarifying their exact scope and limits. In order to understand whether there is more than just a theoretical reason to act, it is essential to understand why most Member States did not (or do not intend to) use such a derogation provided by the e-privacy directive.

Response of the Commission's services:

The Commission's services are not currently in a position to provide a complete mapping of the different national rules and practices currently in place regarding the detection of CSAM among Member States. The Commission's services have recently requested comprehensive information from the Member States and could make this available to the European Parliament once it is available.

It should be noted that the proposed Regulation seeks to create a temporary derogation from certain provisions of the ePrivacy Directive in relation to activities that are not currently within the scope of the Directive, but which will come within its scope upon the entry into application of the definitions of the European Electronic Communications Code on 21 December 2020.

Article 15 of the ePrivacy Directive permits Member States to restrict the scope of certain rights and obligations provided for in the Directive through national legislation which serves one of the listed purposes and meets the requirements of necessity and proportionality. Individual Member State legislation regarding the detection and deletion of CSA online would likely lead to fragmentation across the single market, and it is unlikely that all Member States would adopt such a legislation before 21 December 2020.

► 83.This is even more essential considering the lack of an impact assessment and/or consultation with stakeholders. We would like to have a clarification on the assessment of subsidiarity and proportionality conducted by the Commission before presenting the proposal, and at least a full list of companies and stakeholders consulted.

Response of the Commission's services:

The Commission's assessments of subsidiarity and proportionality of the proposal are set out in the accompanying explanatory memorandum.

Regarding the principle of subsidiarity, EU action may only be taken if the envisaged aims cannot be achieved by Member States alone. EU intervention is needed to maintain the ability of providers of number-independent interpersonal communications services to voluntarily detect and report child sexual abuse online and remove child sexual abuse material, as well as to ensure a uniform and coherent legal framework for the activities in question throughout the internal market. Lack of EU action on this issue would risk creating fragmentation, should Member States adopt diverging

national legislation. In addition, such national solutions would most probably not be able to be adopted by 21 December 2020 in all Member States. Therefore, the objective cannot be effectively reached by any Member State acting alone.

Regarding proportionality, the proposal complies with this principle as it will not go beyond what is necessary for the achievement of the set objectives. It introduces a targeted and temporary derogation from Articles 5(1) and 6 of the ePrivacy Directive in order to ensure that certain measures can continue and maintain the status quo. As a derogation, it should be interpreted narrowly whilst safeguarding the effectiveness of this new legal act.Number-independent interpersonal communications services will remain subject to the e-Privacy Directive with regard to all their other activities (and provisions). The proposal contains safeguards to ensure that technologies benefitting from the derogation meet the standards of the best practices currently applied, and thereby limits the intrusiveness to the confidentiality of communications and the risk of circumvention.

For these reasons, the Commission believes that the principles of subsidiarity and proportionality are satisfied.

The consultations engaged in by the Commission included the public consultation on the EU strategy to fight child sexual abuse, as well as direct engagement with industry and other stakeholders, both prior to and since the publication of the proposal.

The responses to the public consultation are available online[34] and include a wide variety of NGOs, companies and international organisations, many of which emphasised the key role that technology can play in the fight against child sexual abuse. The Commission's services have also directly engaged with several major providers of number-independent interpersonal communications services such as Microsoft, Facebook and Google.

► 84. The COM clarified that such a temporary derogation aims to maintain the *status quo* of voluntary practices conducted by number-independent interpersonal communication service providers, to which GDPR would apply. We need, therefore, an analysis of the <u>current rules applicable to such practices</u>.

Response of the Commission's services:

Please see answer to question #82.

The Commission's services do not intend to take a position on the legality of current practices, as that is up to the relevant national authorities to assess on a case-by-case basis.
In particular, it is up to the data protection authorities to determine in each case whether the legal requirements of the GDPR are met.

[34] EU strategy to fight child sexual abuse

► 85. The COM clarified that DPAs will be responsible for the enforcement of the safeguards provided by the proposed regulation (since the voluntary practices would fall within the scope of GDPR). In this regard, we need specific data on complaints lodged with supervisory authorities concerning such practices and effective judicial remedies sought so far, as well as on investigations conducted (including their timeframe) and sanctions applied.

Response of the Commission's services:
The Commission's services are not aware of any complaints lodged with supervisory authorities concerning these practices, or of judicial remedies sought so far. Consequently, they are also not aware of any resulting investigations or sanctions.

► 86. Furthermore, it is important to understand what kind of control DPAs can exercise on the generalised screening of all communications. In other words, is it feasible in practice for a DPA to verify that the processing is 'strictly necessary' (Art. 3(d)), 'proportionate' and 'least privacy-intrusive' (Art. 3(a)), or that the technology is 'sufficiently reliable' (Art. 3(b))?

Response of the Commission's services:

The GDPR in its entirety will continue to apply to the processing done by these service providers for the purpose covered by this proposed Regulation, as this is the case at the moment. DPAs use elements of proportionality to assess compliance with GDPR already now.

► 87. The CJEU has clarified that when imposing measures having an impact on fundamental rights, EU law itself 'must lay down clear and precise rules governing the scope and application of the measure', calling for 'specific and adapted' rules and 'objective criteria' to limit such measures (*Digital Rights Ireland*). We need, therefore, clarification on the safeguards provided by the proposed regulation, particularly to what extent they provide for specific rules and objective criteria not to have an indiscriminate access to all communications.

Response of the Commission's services:

The specific case cited related to an obligation imposed by Union legislation (transposed into national legislation) to retain (i.e., process) data. The present proposal does not impose any obligation on service providers to process data.

However, the proposal does provide for a series of safeguards to ensure that technologies benefitting from the derogation meet the standards of the best practices currently applied, and thereby limits the intrusiveness to the confidentiality of communications and the risk of circumvention. Providers of number-independent interpersonal communications services should inter alia limit the error rate (false positives) to the maximum extent possible. Where these conditions are not met, the proposed derogation will not apply. That would mean, in turn, that the relevant provisions of the ePrivacy Directive will apply and will have to be complied with.

Version of 9/10/2020, subject to further updates

TECHNOLOGIES CURRENTLY USED BY PROVIDERS OF NUMBER-INDEPENDENT COMMUNICATIONS SERVICES TO DETECT AND REPORT CHILD SEXUAL ABUSE ONLINE AND REMOVE CHILD SEXUAL ABUSE MATERIAL IN THEIR SERVICES

This non-paper provides a high-level overview of some of the technologies currently used by providers of number-independent interpersonal communications services, to detect and report child sexual abuse online and to remove child sexual abuse material (in accordance with the Luxembourg Guidelines[35], material defined in relevant Union legislation as 'child pornography'[36] is referred to in this non-paper as child sexual abuse material (CSAM)).

The information in this non-paper is intended to provide useful context in relation to the proposed Regulation[37] which concerns the use of such technologies by providers of number-independent interpersonal communications services for the before mentioned purposes.

The fact that certain examples of technologies are provided in this non-paper must not be considered as meaning that they are necessarily covered by the proposed Regulation (conversely, the fact that certain technologies are not mentioned, does not mean that they are necessarily not covered), and must not be interpreted as the Commission or its services taking position, as to whether any data processing using these technologies complies with Union law.

The examples given below are some of the most widely used, and this is not intended to be an exhaustive listing. Many of these tools are made available to service providers, law enforcement and other organisations where a legitimate interest can be shown. Typically, these tools are combined with human review to ensure the maximum possible accuracy.

General considerations

1. These technologies answer the question "is this content likely to be child sexual abuse, yes or not?" not the question "what is this picture about? What is this conversation about?" In other words, the tools look for specific indicators of possible child sexual abuse.
2. In relation to the error rates, the actors involved have incentives to limit the rate of false positives.
3. Human moderation. The human review reduces the error rate to close to zero. Human review is already typically in place even for the most accurate technologies such as hashing.

---

35 Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse

36 Article 2(c), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

37 (COM/2020/568 final)

Known child sexual abuse material

Hashing technology is a type of digital fingerprinting, a technology also used for the detection of **malware.** It is widely used for the detection of material which has previously been confirmed as constituting child sexual abuse material. Many variations and implementations of hashing technology exist, including Microsoft's PhotoDNA[38], which is perhaps the most widely used tool of this type.

PhotoDNA has been in use for more than 10 years and it was developed by academics at Dartmouth College in cooperation with Microsoft. While the original PhotoDNA detects known CSAM in images, a version for detecting CSAM in videos is also available[39].

How it works[40]:

1) Detection:
   - The tool first identifies images above a certain size.
   - The tool focuses on images only and ignores text, i.e. it does not read the body of the email or extract any other information transmitted in the one-to-one message (it does not recognise faces in the images, or other contextual information). In other words, it does not answer the question "what is this message about?" but the question "is this image known?"
2) Creating a unique digital signature (known as a "hash") of the image (see figure below)[41], through the following process:
   1. Convert a full-resolution color image (top) to grayscale and lower resolution (bottom left);
   2. Use a high-pass filter to highlight salient image features (bottom center); and
   3. Partition the high-pass image into quadrants from which basic statistical measurements are extracted to form the PhotoDNA hash (bottom right).

   This hash is unique and irreversible, meaning that the image itself cannot be re-created from the hash.

38 Microsoft's information on PhotoDNA
39 How PhotoDNA for Video is being used to fight online child exploitation
40 See here for a visual explanation on how PhotoDNA works.
41 Reining on online abuses, Farid, H., Dartmouth College, USA, 2018

Figure 1: hashing process

3) Matching:
   - The hash is compared with those in a database of hashes of known child sexual abuse material. If the image hash is not recognised, no information is kept.
   - The main and largest database of hashes (around 1,5 million) is held by the National Center for Missing and Exploited Children, a public-interest, non-governmental organisation established by US Congress in 1984 to facilitate detection and reporting of child sexual abuse material.

- The criteria for an image to be converted into a hash added to the database of the National Center for Missing and Exploited Children is the following:
    - Children (prepubescent or pubescent) engaged in sexual acts.
    - The sexual contact may involve the genitals, mouth, or digits of a perpetrator; or it may involve contact with a foreign object.
    - An animal involved in some form of sexual behaviour with a pre-pubescent child.
    - Lewd or lascivious exhibition of the genitalia or anus of a pre-pubescent child.
    - Images depicting pubescent children contain children that have been identified by law enforcement (therefore ensuring that they are actually minors).
- Every hash has been viewed and agreed upon as being child sexual abuse material by two different experts at the National Center before it is included in the database.

PhotoDNA has a high level of accuracy. The rate of false positives is estimated at **no more than 1 in 50 billion**[42], based on testing. PhotoDNA has been in use for more than 10 years by over 150 organisations globally[43] including service providers (Microsoft, Facebook, Twitter, Apple[44]), NGOs (e.g. NCMEC, Internet Watch Foundation) and law enforcement in the EU (e.g. Europol, DE, SE and others). In these 10 years, the tool has been used daily and analysed hundreds of billions of images without any accuracy concerns being identified.

Other examples of hashing technology used for these purposes, and operating on similar principles, include YouTube CSAI Match[45], Facebook's PDQ and TMK+PDQF[46].

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

43 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).

44 More information is available here.

45 YouTube CSAI Match

46 Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer

Previously-unknown child sexual abuse material

Technologies currently used for the detection of new CSAM include classifiers and artificial intelligence (AI). A classifier is any algorithm that sorts data into labelled classes, or categories of information. Classifiers are also used in **spam filters**, which, while not identical in function., scan incoming emails for particular patterns and classify them as either 'spam' or 'not-spam.'[47]

In some instances, classifiers are a concrete implementation of pattern recognition in many forms of machine learning.

Examples of classifiers include those that can detect nudity, shapes or colours. Classifiers need data to be trained on and their accuracy improves the more data they are fed.

Thorn's Safer tool[48] identifies both known and unknown CSAM with perceptual hashing and machine learning algorithms. In particular, Safer identifies unknown CSAM using a machine learning classification model that returns a prediction for whether a file is CSAM. This classifier has been trained on datasets totalling hundreds of thousands images including adult pornography, CSAM, and various benign imagery and can aid in the identification of potentially new and unknown CSAM.

Content which is flagged by Safer is queued for review with content moderation tools, which allow the review and reporting verified CSAM, and the secure storage of content in accordance with regulatory obligations. Hashes of previously unknown CSAM are added to a database of hashes.

Safer reports **99% accuracy** for the detection of known and unknown material combined[49], and reports that 100 000 images of CSAM have been removed using Safer. Safer includes a False Positive API which allows its customers (i.e. companies and organisations) to report false positives found through detection services. This feedback is used to improve the tool.

Other tools making use of classifier and AI technology to detect previously unknown CSAM include Google's Content Safety API[50], and Facebook's AI technology[51].

In some cases, the search for unknown CSAM is undertaken if known CSAM has been found with that user. For example, Google and Thorn seem to use primarily the hash matching technology. Once the known CSAM is identified on an account, then it might use classifiers to assess the content of the account to identify if it has a high probability of containing CSAM.

---

47 See here, here and here for more information on spam filters. Spam filters are usually run with the receiving end-user's consent. Some spam filters look only at the subject line of the email.

48 Thorn's Safer tool.

49 See here.

50 Fighting child sexual abuse online

51 See here and here for more information on Facebook's tool to proactively detect child nudity and previously unknown child exploitative content using artificial intelligence and machine learning.

In other cases, the search for unknown CSAM with classifiers is undertaken in parallel to the search of known CSAM.[52]

Grooming/solicitation of children for sexual purposes

Tools for the detection of grooming in text-based communications make use of technologies for the analysis of text and/or analysis of metadata, which, while not identical in function, are also similar to the technology used in spam filters[53].

Tools of this type include the tool developed under Microsoft's Project Artemis[54], developed in collaboration with The Meet Group, Roblox, Kik and Thorn.

The technique is applied to text-based chat conversations. Conversations are rated on a series of characteristics and assigned an overall probability rating, indicating the estimated probability that the conversation constitutes grooming. These ratings can be used as a determiner, set by individual companies, to address flagged conversations for additional review.

The tool is made available to companies, law enforcement, NGOs and other government entities through Thorn[55] (Anti-grooming starter kit)[56]. All interested parties are required to fill out a brief questionnaire inquiring about their intent of use and will be subject to review by Thorn.

Microsoft has reported that, in its own deployment of this tool in its services, its **accuracy is 88%.**

---

52 See for example, How WhatsApp Helps Fight Child Exploitation. Examples of behavioural classifiers used are the speed/amount of users that join and leave a group, the frequency of group name change, or whether the group contains members previously banned.

53 For more information about content spam filters see here and here and for other spam filters see here and here. Spam filters are usually run with the receiving end-user's consent. Some spam filters look only at the subject line of the email.

54 Microsoft shares new technique to address online grooming of children for sexual purposes

55 Thorn

56 Anti-grooming starter kit

NCMEC data on companies and services reporting to it in 2019.

The annex contains a list of all companies that reported to NCMEC in 2019, which used technologies to detect child sexual abuse online. It should be noted that the concept of electronic service as used by NCMEC might not be equivalent to the definition of the electronic communication service as defined in the EECC, as it includes for instance also file sharing, forum or message board, marketplaces, etc[57].

2019 CyberTipline
Reports - Trends See

[57] Not all 'chat services' do necessarily constitute number-independent interpersonal communications services. According to NCMEC, their classification of "chat" refers to services they know are only messenger or where the premise of the platform is specifically for chatting.