Position on the draft Interim CSAM derogation (2020/0259) from certain provisions of the ePrivacy Directive

Facebook welcomes the collective efforts of the EU institutions on the proposal for a temporary derogation from certain provisions of the e-Privacy Directive for combatting child sexual abuse material online (the "Interim CSAM derogation"). However, unfortunately several material issues with the Interim CSAM derogation remain outstanding. The net effect, both legally and practically, is that these outstanding issues impact the ability of web-based communication services to legitimately continue their voluntary detection of child sexual abuse online.[1]

Therefore, we would like to share our concerns with the current draft text of the Interim CSAM derogation, in the hope that these issues can be addressed in the final agreed text.

(1) Traffic Data and Safety

In March 2019, we presented our privacy focused vision[2] for social networking, where we made the distinction between (i) private messaging services as intimate spaces (akin to a "living room") and (ii) broader social networks that facilitate telling all your friends about something, or using your voice on important issues (similar to a "town hall"). When it comes to private messaging, we said we believed that people should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.

With that in mind, people's private communications should be secure. End-to-end encryption prevents anyone other than the sender and the receiver of a message from seeing its contents, and so we believe our encryption roadmap is very much aligned with the objective of the EU's ePrivacy rules to ensure the respect for private life. For that reason, we welcome the European Parliament's position on the ePrivacy Regulation where the Parliament highlights the critical importance of encryption as a tool to protect against unauthorised access to communications data.

We are committed to designing strong prevention, detection, and reporting systems for messaging services that provide users with industry-leading privacy while working to protect people from exposure to child safety abuse material. For example, WhatsApp (which has been end-to-end encrypted since 2016) is designed to protect the most fundamental and private use cases (which is the contents of people's private messages and calls) with end-to-end encryption. Our plans to encrypt Facebook Messenger and Instagram Direct Messaging will follow the WhatsApp model. Specifically, WhatsApp uses a combination of other signals -- including user reports, unencrypted account-level information, account-level metadata and,

[1] Facebook also notes the recent paper published by We Protect.
[2] https://about.fb.com/news/2019/03/vision-for-social-networking/

critically, in this context, certain pieces of traffic data -- to help keep users safe and to prevent our services being misused to cause harm.

Accordingly, our continued ability to process communications traffic data is critical for our prevention, detection and reporting work to keep people safe from exposure to CSAM, and we believe that the processing of traffic data for this purpose should be expressly permitted by the Interim CSAM derogation and the future ePrivacy Regulation.

(2) Concrete suspicion

Recital 11 of the draft Interim CSAM derogation stipulates that technologies should only look into specific communications in cases where there are concrete elements of suspicion of child sexual abuse. This requirement fails to have regard to the fact that this is not how *any* of the technology currently used by service providers works. It is only by applying the available technology -- such as processing certain traffic data -- that systems can make a determination on what might warrant further investigation or examination. In other words, it is only by applying the technology broadly that we can arrive at a position where we can form a concrete suspicion of activity related to child sexual abuse.

In addition, Recital 5(a) of the Parliament's text also raises serious concerns about whether any kind of proactive detection can occur at scale. This would negatively impact all companies' ability to apply any of the available technologies effectively.

(3) Accuracy and reliability

The current text of the Interim CSAM derogation, in Article 3(1) sub (b), requires that the technology used to identify online child sexual abuse material is sufficiently reliable in that it limits the rate of errors where a communication is wrongly identified as child sexual online abuse to, at most, 1 in 50 billion (i.e. "false positives"). This requirement is inhibitive and we are not aware of any peer review evidence attesting to the fact that any technology used by any company today meets this bar. Accordingly, a maximum error rate of 1 in 50 billion is unachievable and would, in effect, preclude any company from continuing with any kind of communications data processing for safety.

This maximum error rate of 1:50 billion is a material restriction and may inadvertently limit the legitimate processing of data for detecting or reporting online child sexual abuse. An overly prescriptive false positive rate could have a severe chilling effect on the ability of service providers to continue making referrals that include key pieces of data.

It is also important to highlight that a referral to a competent authority is not always the end goal of the application of these kinds of technology. Often, the application of this technology -- where it results in a suspicion about the intentions of a user -- can result in the limitation of certain features available to them, such as the ability to send a message to a minor by way of prevention. In other words, some user conduct may be concerning but would not rise to a level

that warrants -- or even permits -- a referral to a law enforcement agency. There is a spectrum of activity that *may ultimately* lead to conduct that warrants an external referral. However an inaccurate assumption that all uses of any technology for the purpose of preventing and detecting child sexual abuse would necessitate a referral to a competent authority could thwart the legitimate use of technology to deter types of behaviour that do not warrant an external referral, but nonetheless could be harmful to children.

(4) Definition of 'solicitation'

Facebook has developed techniques designed to thwart the grooming of minors which rely, in part, on the use of traffic data. For example, in order to prevent possible inappropriate interactions with children (IIC) from taking place between adults and minors on Messenger, certain account-level Facebook data, processed *in combination with some critical traffic data*, can help us to determine if we should restrict certain functionality or features for some Facebook users.

While we welcome the clear intention to clarify the Commission's definition of 'solicitation' in Article 2(b) to include grooming activities within the scope of the proposed derogation (by referring to Article 6 of Directive 2011/93) we believe that the definitions proposed are overly prescriptive and would fail to capture all forms of online grooming. This is because of the requirement that the interaction would include a proposal to meet, as well as "material acts leading to such a meeting", in order to establish the offense.

Such a narrow interpretation of grooming does not account for the harm a child may suffer over the course of the inappropriate interactions/grooming behaviour even in the absence of material acts leading to a meeting, or for the possibility that another individual could be solicited to make contact with a child.

(5) Unintended effects and conflicts of law

The Interim CSAM derogation should have regard to potential areas where unintended effects might be created, including conflict of law scenarios. For example, the Parliament's stated position in Article 3(1) sub (db) with a hard stop of three months could conflict with preservation obligations placed on US companies who are legally obliged to report CEI to NCMEC.

As another example, the European Parliament's stated position in Article 3(1) sub (ea) could be interpreted as *an obligation* to report *every* case of suspicion to law enforcement. The Interim CSAM derogation should, as previously mentioned, have regard for situations where the electronic communications service provider may restrict the functionality available to a user to try and prevent them from making contact with a minor which may result in harmful CSAM-related activity, but where the suspicion held by the Electronic Communications Services (ECS) provider would not meet the threshold of evidence required for a referral to law enforcement or other recognised organisations.

Secondly, this provision reads as though referrals to NCMEC would no longer be possible, as the reporting seems restricted to the competent national law enforcement authorities only. This has the potential to create a number of unintended consequences (on both a legal and practical/effectiveness basis). By way of example, US law mandates NCMEC as the exclusive recipient of CEI reports; a requirement on companies to report elsewhere (in parallel or exclusively) could expose US-based processors to violating US law for the transmission of the CEI. Moreover, under the current global process, NCMEC receives all referrals from such US-based processors and subsequently triages and passes that information to law enforcement authorities all over the world. NCMEC serves a critical function of investigation, escalation, and de-conflicting of reports, and mitigates the potential of duplicative-investigation of suspects/matters already addressed by other law enforcement agencies around the world. We believe this might be an unintended omission, as the words 'organisations acting in the public interest against child sexual abuse on a voluntary basis' (in addition to the reference to law enforcement') are referred to in every instance elsewhere throughout the text. Similarly, the text agreed by the Parliament references the establishment of a public register of organisations acting in the public interest against child sexual abuse; again, we believe it is of critical importance to include NCMEC.

Furthermore, the draft provisions in Recital 4a on localised age of consent rules barring reporting of imagery are not only a conflict of law issue but make assumptions about users which may not be known and thus may place an unreasonable burden on industry to determine a country of origin and unattainable precise age markers. Similarly, the draft provisions in Article 3(1) sub a XIII with exceptions for communications protected by professional privilege (e.g., attorney/client and doctor/patient) may be impossible for the service provider to determine and guarantee.

(6) User information after closure of an investigation

The current text of the Interim CSAM derogation in Article 3(1) sub a XII includes a requirement that users are provided with certain information, and that such information may only be delayed if prejudicial to an ongoing investigation (and then only as strictly necessary, with users to be informed without delay after the investigation is closed).

This provision is problematic as service providers usually do not receive notice from law enforcement, judicial or other recognised bodies that a certain investigation has been closed. Accordingly, this makes it impossible or very difficult for service providers to meet this requirement. Nor can service providers determine when a disclosure would or would not result in a tip-off or interference with an ongoing investigation, and may dissuade providers from voluntarily detecting child sexual abuse.

Further, it should be considered that providing users with information in the two circumstances set out in the draft derogation might result in scenarios where the bad actor might harm a victim in retaliation for having made a user report of the abuse to the ECS provider. Furthermore, on a

practical basis, ECS providers might not have the means to contact a (former) user in the event they had been disabled from the platform due to harmful behavior.

(7) Prior DPA consultation

The draft text of the Interim CSAM derogation, as amended by the Council and the Parliament, proposes a role to the data protection supervisory authorities in consulting and approving technologies. The requirement for mandatory prior consultation (in what could be a lengthy consultation and approval process) introduced by Article 3(1) sub (a) would impede innovation and the ability of service providers to move quickly to roll-out new technologies in the fight against child sexual abuse online. As the nature of threats such as grooming and the distribution of child sexual abuse materials can evolve quickly, so too must our approach to tackling these threats.

Moreover, this requirement to consult is not consistent with the GDPR principles, which only requires consultation where the data protection impact assessment indicates that the processing would result in a high risk in the absence of further mitigation measures. Accordingly, we believe that both the proposal for the derogation, and GDPR requirements to undertake a data protection impact assessment, are already sufficiently prescriptive, with carefully weighed safeguards to ensure proportionality, to render prior consultation of DPA's superfluous. Accordingly, ex-post supervision by DPAs on the basis of data protection impact assessments should be sufficient, and ECS-providers remain equally accountable for technologies deployed.

Even though we believe the prior consultation requirement is superfluous, we welcome the clarity introduced in the Parliament text which preserves the One Stop Shop principle, under GDPR, for the purposes of the derogation. This is important because, should the requirement to consult remain (which we do not consider is necessary given the existing obligation of undertaking a privacy impact assessment), new technology would need to get approval from 27 DPAs, who may have contradicting views and requirements. This would further slow down and complicate the application of new technologies.

Conclusion

The European Commission[3] and child safety experts and organizations, such as the National Center for Missing and Exploited Children (NCMEC)[4], have noted that the ePrivacy Directive does not provide a legal basis to use child safety tools like scanning for child sexual abuse material. We have communicated our concerns with European policymakers regarding this lack

---

3 https://www.consilium.europa.eu/en/press/press-releases/2020/10/28/combating-child-abuse-online-council-ready-to-negotiate-a-temporary-measure/

4 https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety#:~:text=It's%20up%20to%20members%20of,detect%20online%20child%20sexual%20exploitation.

of legal basis and the implications of the ePrivacy Directive applying to the processing of electronic communications metadata for the detection and prevention of illegal and/or harmful content.

We recently announced[5] changes to Facebook Messaging Services in Europe which were legally necessary to comply with the ePrivacy Directive. The safety of our community is paramount, and we are advocating for changes to the law that keep the strong privacy protections and allow us to combat abuse. This includes the suggested changes, outlined in this position paper, that would permit us to use metadata to help keep people safe from exposure to child safety abuse material, while retaining important privacy protections.

We appreciate the opportunity to contribute to the policy-making process and look forward to continuing to work together with European policymakers and other stakeholders to ensure that the legislative framework successfully achieves the necessary balance between privacy and safety.

[5] https://about.fb.com/news/2020/12/changes-to-facebook-messaging-services-in-europe/