May 18, 2022

RE: Feedback on the European Commission's proposed regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 2022/0155 (COD)

To whom it may concern:

I am a Research Scholar at the Internet Observatory at Stanford University, Stanford, California, USA. I write in my personal capacity to provide feedback on the above-named proposal for a regulation regarding child sex abuse (CSA) (hereafter "the Proposal").[1] The Proposal is of great concern to me because my research focuses on analyzing government policies, in the U.S. and elsewhere, that relate to encryption and/or electronic surveillance by law enforcement. I also study online service providers' techniques for detecting and combating abuse (including CSA) on their services, including on end-to-end encrypted services.

I am a signatory of a recent joint statement by a group of cybersecurity experts, organizations, and companies opposing the proposed regulation.[2] That statement described how the Proposal, which covers CSA imagery (known and new) as well as grooming, is incompatible with the provision of end-to-end encrypted services. The statement warned of the devastating impacts the Proposal would have on digital security and user privacy. It recommended instead incentivizing alternative measures that address CSA while protecting user privacy, such as facilitating user reporting of CSA material. I write separately to underscore some of the points made in that joint statement and to draw the Commission's attention to relevant research.

The Proposal Would Violate the Fundamental Rights of Child Users of Online Services

First, the Proposal fails to acknowledge that mandating the monitoring of all online communications, both public and private (including on end-to-end encrypted services), for CSA and grooming content does not just affect the rights of adults and businesses – it implicates the fundamental rights of children, too. The "Fundamental rights" portion of the Proposal refers to "the **fundamental rights of the users** of the services at issue," including "in particular, the fundamental rights to respect for privacy (including confidentiality of communications …), to protection of personal data and to freedom of expression and information."[3] The Proposal weighs these rights against the "fundamental rights of the children" including child victims' rights "to

[1] The public version dated 11 May 2022 is available at https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF.
[2] Available at https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/.
[3] Proposal, *supra* n.1, at 12.

respect for private … life, right to protection of personal data and the right to the integrity of the person."[4] After a surprisingly brief discussion, the Proposal concludes that the latter considerations justify the severe and widespread intrusions upon the fundamental rights of hundreds of millions of people that would result from the implementation of this Proposal.

This discussion pits the rights of children in opposition to the privacy and free expression rights of users without recognizing that children, too, are among the "users of the services at issue." Such an oversight is especially bizarre given that the Proposal would mandate the detection of child grooming, which necessarily requires that a child user be party to a digital communication.

By imposing a mandatory monitoring requirement for all online communications and effectively outlawing end-to-end encrypted services, the Proposal would violate children's fundamental rights, including the rights to respect for privacy (including communications confidentiality), protection of personal data, freedom of expression and information, and integrity of the person. That is, **the Proposal would violate the very rights of children that it seeks to protect.**

The role of encryption in protecting children's fundamental rights has been recognized by UNICEF. In an October 2020 working paper titled *Encryption, Privacy and Children's Right to Protection from Harm*,[5] UNICEF's Office of Research - Innocenti emphasized the importance of including children's privacy rights in policy discussions about child safety. It cautioned states against enacting policies undermining encryption in the name of protecting children, given the vital role that encryption plays in protecting children's privacy, security, and safety. While the paper is worth reading in full, I wish to bring to the Commission's attention the following especially pertinent excerpts:

- "End-to-end encryption is necessary to protect the privacy and security of all people using digital communications channels. This includes children…" (p. 3)
- "[T]he goal of ensuring that children's rights are safeguarded in the digital age involves fulfilment of their rights to both privacy and protection from sexual abuse and exploitation. Privacy is often treated as a secondary right. Thus, debates around end-to-end encryption have tended to assume that a safety-maximizing solution (or even a privacy-minimizing solution) is the best way to keep children safe, which is not always the case." (p. 5)
- "[E]ncryption is fundamental for any democratic and rights-respecting state to protect its citizens, including children who are increasingly gaining access to digital communications platforms." (p. 6)
- "Encryption is also critical to ensure children's safety." (p. 6)

[4] *Id.* at 13.
[5] Available at https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf.

- "Children have a right to be protected from sexual abuse and exploitation wherever it occurs, including online … At the same time, end-to-end encryption by default on … digital communication platforms means that every single person, whether child or adult, will be provided with a technological shield against violations of their right to privacy and freedom of expression." (p. 8)
- "In the end, we need to appreciate that the right to protection includes ensuring privacy and security." (p. 13)
- "[I]t is incorrect to suggest that children will have their rights better respected if digital communications platforms remain unencrypted…" (p. 13)
- "Certainly, violations of a child's right to protection from sexual abuse and exploitation have severe and often lifelong consequences. For some, the consequences of privacy, security and data protection risks can also be severe, long-term." (p. 13)

As the UNICEF paper acknowledges, it is an incredibly difficult challenge to develop a policy for protecting children from online (and offline) harm in the digital age without unnecessarily, inappropriately, and disproportionately infringing upon other coequal rights. That said, the Proposal fails to strike the appropriate balance. It openly admits that it would violate users' fundamental rights in multiple ways, but fails to reckon with children's inclusion among those users. This oversight impermissibly omits a crucial consideration that must be weighed among the numerous interests that come into play when evaluating whether and how to restrict multiple fundamental rights of individuals in a democratic society in the name of crime prevention.

Automated Scanning Is Not the Only, or Best, Way to Detect Grooming

Beyond the troubling omission of child users' privacy, data protection, integrity, and free expression rights from its fundamental rights analysis, the Proposal also concerns me because it makes unsupported claims about the necessity of detecting grooming via the automated scanning of the contents of interpersonal communications – an intervention the Proposal admits is highly intrusive and sensitive.[6] Contrary to the Proposal's claims, I recently published research in a peer-reviewed journal that demonstrates the prevalence of multiple anti-grooming techniques among online service providers. My research supports the viability of other options for abuse detection besides automated content monitoring, such as tools for user reporting.

My research surveyed a group of online service providers about the "trust and safety" techniques they employ to detect, prevent, and mitigate abuse on their services.[7] Some of the survey participants provide end-to-end encrypted messaging services; others do not. Collectively, the providers included in my analysis serve over two billion users, representing a significant

[6] Proposal, *supra* n.1, at 14-15.
[7] Pfefferkorn, R. (2022). Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers. *Journal of Online Trust and Safety*, *1*(2). https://doi.org/10.54501/jots.v1i2.14. Available at https://tsjournal.org/index.php/jots/article/view/14.

percentage, possibly a majority, of the world's internet users.[8] My survey asked which technique, of the three options given, the participating providers considered most useful for detecting various categories of abuse. The 12 abuse categories I listed included a category I called "child sexual exploitation" (CSE), which was defined to include grooming and enticement (but not imagery).[9] The three options given were metadata analysis; user reports; and automated scanning of the contents of communications – the technique that would be mandated by the Proposal.

I found no consensus among the survey participants about which technique is most useful for detecting CSE, i.e., grooming. Overall, user reporting and automated scanning were deemed equally useful for detecting grooming.[10] Even among the subset of survey respondents that said they currently employ automated scanning to detect abuse (a subset that necessarily excludes end-to-end encrypted service providers), just as many said that either metadata analysis or user reporting is most useful against CSE as said automated scanning is.[11]

These findings rebut the Proposal's claim that "scanning is often the only possible way to detect [grooming]."[12] My research shows that there are multiple grooming detection techniques already in use by online service providers. Not only is automated scanning far from being the *only* option available for detecting grooming, it is not universally considered the *best* option, either. My research reveals significant ambivalence about how best to detect grooming among those closest to the issue: online service providers that already work to detect child safety offenses on their services – services which, as said, collectively serve billions of users.

Mandating the constant proactive monitoring of the online communications, private and public, of everyone in the European Union is an extraordinary proposal.[13] Extraordinary proposals require extraordinary support. But the Proposal provides no support for the claim that automated scanning is the only way to detect grooming – a claim my research disproves. I know you are aware of my article, because you cite an earlier draft version of it in Section 5.2 of the Impact Assessment Report accompanying the Proposal.[14] Yet you ignored my exhortation to you:

---

[8] *Id.* at 6-7.
[9] *Id.* at 9.
[10] *Id.* at 14-16.
[11] *Id.* at 15-16.
[12] Proposal, *supra* n.1, at 14.
[13] Extraordinary and plainly illegal: even setting aside its violations of multiple fundamental rights, the Proposal also quietly admits (on p. 5) that it is inconsistent with "[t]he e-Commerce Directive and the [Digital Services Act, which] prohibit Member States from imposing on providers of intermediary services general obligations to monitor or to actively seek facts or circumstances indicating illegal activity." The Proposal weakly tries to explain away this inconsistency by claiming that "the precise contours of that prohibition" are not yet "clear" and that the Proposal "aims to comply with the underlying" *spirit* of the ban on general monitoring obligations, as though that excuses the flagrant contravention of the *letter* of those regulations (*id.*).
[14] Available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en.

> It is urgent that regulators understand the shortcomings of automated abuse detection … Irrespective of their dubious legality, [my] results indicate that … automated scanning mandates may not fix the problems that governments intend them to solve. … [G]overnments seeking to reduce the online prevalence of [CSA and other abuse] (without degrading the rights of their citizens) should start by incentivizing more providers to implement strong reporting tools before requiring [automated content scanning].[15]

The Commission's Proposal is not only illegal and an unacceptable violation of the rights of free people in a democratic society, it also is unlikely to succeed at its goals. It repeatedly acknowledges the obvious and massive downside of erasing Europeans' – including children's – ability to have private conversations online, yet it overestimates the expected upside by which it attempts to justify this shocking plan.

The proposed regulation must not go forward. Children deserve to be protected, online and off. But sacrificing the hard-won freedoms that are once again under threat in Europe is not the way.

Sincerely,

Riana Pfefferkorn
San Francisco, California, USA

[15] Pfefferkorn, *supra* n.7, at 20-21.