EDRi

EUROPEAN DIGITAL RIGHTS

General views from EDRi on the proposed interim legislation and the upcoming long-term legislation

Child sexual abuse is a serious crime with extremely serious consequences for victims. All forms of violence against children online and offline must be effectively eliminated. In our opinion many effective measures to achieve that goal may be found outside of technology, ranging from public education and victim support to improved cross-border police cooperation. We welcome the Commission's work programme to secure Member State compliance with the many aspects of Directive 2011/92/EU. Many CSA websites are now hosted in Europe and we suggest that the Commission prioritise this non-technical work, and more rapid take-down of offending websites, over client-side filtering. Finally, existing legislation should be enforced: the European Parliament's Report' on the implementation of 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 (2015/2129(INI)) reported numerous flaws in Member States' implementation of the Directive that should be tackled immediately. The European Commission has the tools and powers to ensure that children's rights are protected when Member States fail to do so.

We would like to add one specific comment on **grooming** as a potential activity under the scope of the interim or new legislation**: The detection of new child sexual abuse material requires interpretation of the context.** We know for a fact this is (more or less) easy for humans, but extremely hard for computers. There are more than enough illustrative cases when filtering on copyright violations. It is possible to publish material which is protected by copyright, when one can fall back on an exception such as "citation" or "parody". When an automated filter considers the material, it will for sure notice the material is protected by copyright. It will, however, have a hard time determining whether an exception applies as well (and consequently to not flag it as a violation). **The reason why these filters fail so frequently, is because it requires an interpretation of the context. The same applies to grooming.** It requires an interpretation of the context in which a particular text appears. And again, this is hard for computers to do right. **When filters fail, legitimate speech is harmed.**

The **European Data Protection Supervisor's (EDPS)** Opinion on the Commission proposal concluded that the legislative should not be adopted in its original form as it did not meet the criteria of necessity and proportionality, and in particular because of the **lack of a specific legal basis and lack of clear and precise rules governing the scope and application of the measures in question, as well as the lack of adequate safeguards**.

Equally, the **European Parliamentary Research Service (EPRS)** has just issued a report on this topic saying that "i**nstead of using these techniques to monitor all private messages, their use should be limited to private messages of persons already under suspicion of soliciting child abuse or distributing CSAM**" (page 47) and that current practices may be sending data to countries with an inadequate level of protection (p. 44 of the report).

UNICEF is not particularly satisfied by these mass scanning practices either. A toolkit on Children's Online Privacy and Freedom of Expression published by UNICEF on scanning tools said that improving privacy and data protection for children is essential for their development and for their future as adults. The toolkit highlights that any monitoring tools should "bear in mind children's growing autonomy to exercise their expression and information rights".

Furthermore, the **UN Committee on the Rights of the Child** has adopted the **General comment No. 25 (2021)** on children's rights in relation to the digital environment (https://undocs.org/CRC/C/GC/25) has made clear that "children's participation [in the digital environment] does not result in undue monitoring or data collection that violates their right to privacy, freedom of thought and opinion" (para. 18), that "**[c]ontent moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy.**" (para. 56), that "[a]ny restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate." (para. 59), and that "**States parties should ensure that uses of automated processes of information filtering, profiling, marketing and decision- making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment**." (para. 61). Regarding encryption, the General comment states that "States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. **Such measures must be strictly limited according to the principles of legality, necessity and proportionality**" (paras. 70 and 75).

Finally, the legal Opinion by Prof. Dr. Ninon Colneric clarifies that "**generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter**".

Additional responses for two questions of the public consultation

Question: In your opinion, do current efforts to tackle child sexual abuse online strike an appropriate balance between the rights of victims and the rights of all users (e.g. privacy of communications)?
Response:
The European Data Protection Supervisor's (EDPS) Opinion on the Commission proposal concluded that the legislative should not be adopted in its original form as it did not meet the criteria of necessity and proportionality, and in particular because of the lack of a

specific legal basis and lack of clear and precise rules governing the scope and application of the measures in question, as well as the lack of adequate safeguards.

Equally, the European Parliamentary Research Service (EPRS) has just issued a report on this topic saying that "instead of using these techniques to monitor all private messages, their use should be limited to private messages of persons already under suspicion of soliciting child abuse or distributing CSAM" (page 47) and that current practices may be sending data to countries with an inadequate level of protection (p. 44 of the report).

Last but not least, UNICEF is not particularly satisfied by these mass scanning practices either. A toolkit on Children's Online Privacy and Freedom of Expression published by UNICEF on scanning tools said that improving privacy and data protection for children is essential for their development and for their future as adults. The toolkit highlights that any monitoring tools should "bear in mind children's growing autonomy to exercise their expression and information rights".

Finally, the UN Committee on the Rights of the Child has adopted the General comment No. 25 (2021) on children's rights in relation to the digital environment (https://undocs.org/CRC/C/GC/25) has made clear that "**children's participation [in the digital environment] does not result in undue monitoring or data collection that violates their right to privacy, freedom of thought and opinion**" (para. 18), that "**[c]ontent moderation and content controls should be balanced with the right to protection against violations of children's other rights, notably their rights to freedom of expression and privacy.**" (para. 56), that "**[a]ny restrictions on children's right to freedom of expression** in the digital environment,**such as filters,** including safety measures, should be lawful, **necessary and proportionate.**" (para. 59), and that "States parties should ensure that uses of automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment." (para. 61). Regarding encryption, the General comment states that "[w]here encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. **Such measures must be strictly limited according to the principles of legality, necessity and proportionality.**" (para. 70). Finally, the paragraph 75 needs to be quoted in full:

"75. **Any digital surveillance of children,** together with any associated automated processing of personal data, **should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge** or, in the case of very young children, that of their parent or caregiver; **nor should it take place without the right to object to such surveillance**, in commercial settings and educational and care settings, and consideration s**hould always be given to the least privacy-intrusive means available to fulfil the desired purpose.**"

Question: Do you have any other comments in relation to the current situation and challenges in your actions to fight against child sexual abuse online?
Response: We have 3 additional comments:

1 - Normalisation of scanning of communications and the slippery slope of surveillance
Despite arguments saying that the debates on the interim Regulation were not about attacking encryption and confidentiality of communications, these proposals to allow the scanning of private communications align with the broader narrative to prevent encryption from being deployed widely.

The rhetoric pushed forward by the EU legislator leading to the imposition of upload filters in the Copyright Directive and in the Terrorist Content Online Regulation (aka TERREG) is worrisome. As with other types of content scanning (whether on platforms like YouTube or in private communications) scanning everything from everyone all the time creates huge risks of leading to mass surveillance by failing the necessity and proportionality test. Furthermore, it creates a slippery slope. The implementation of monitoring measures is justified by less harmful infringements (copyright) first, facilitating the political support of identical measures for more serious issues (child sexual abuse, terrorism). What it leads to is the normalisation of communications scanning and snooping, where everyone is considered suspect by default: This infringes the basic human rights to privacy and freedom of expression and does not meet the requirements of a democratic society.

2 – Increasing pressure on services providers to decrease the level of protection that encryption provides.

Despite arguments stating that the debates on the interim Regulation were not about attacking encryption and confidentiality of communications, these proposals to allow the scanning of private communications align with the broader narrative to prevent encryption from being deployed widely. As far as we understand, the scope of the proposal would be limited to services that are able to monitor the communications between end-users. **Once this has been normalized, it can be reasonably foreseen, that there will be pressure to monitor other forms of communication, such as those protected with end-to-end encryption**. Another likely consequence is that there will be **increased public pressure on large service providers such as Facebook to refrain from introducing encryption in their electronic communications services** (like Facebook Messenger). This will expose the users, including many children, to additional risks that their communications content will be processed unlawfully for marketing purposes or other profiling of user behaviour. Even though EU data protection and privacy laws apply irrespective of whether the communications content is encrypted or not, **services with end-to-end encryption offer users a technical guarantee against unlawful processing**, besides the legal protection. In practice, encryption provides stronger and more credible privacy guarantees for users who do not have to speculate about what the service provider might do with their communications content, possibly in violation of EU data protection and privacy laws. The adverse consequences of lacking DPA enforcement, something that seems to be a chronic problem for Big Tech operating in the EU, will simply be less severe when encryption is part of the package.

3- Empowerment of Big Tech companies

We cannot allow Big Tech to become even more powerful. Allowing and encouraging Facebook and other private companies to continue scanning private communications would put private companies in charge of surveillance and censorship mechanisms that, because of their impact on fundamental rights, are illegal. Any wiretapping of communications should be the responsibility of public authorities which abide by strict legal standards in full respect of fundamental rights. While the EU is on one hand trying to rein in the power of Big Tech via the adoption of the Digital Services Act (DSA), Digital Markets Act (DMA),the General Data Protection Regulation (GDPR), and the ePrivacy Regulation these initiatives that allow Big Tech to police private communications only reinforce their power as gatekeepers and as key allies of governments for the surveillance of the population.