mlex®
a LexisNexis® company

Platforms' encryption protected in EU Parliament's revision of child-abuse content rules, lead lawmaker says

19 Apr 2023 | 16:15 GMT | **Insight**
By Lucy Valeski

End-to-end encrypted platforms, such as WhatsApp and Signal, would not be undermined by the European Parliament's draft amendments to rules aimed at detection and removal of child sexual abuse material online, says Spanish lawmaker Javier Zarzalejos, who is steering the draft law through the legislature.

End-to-end encrypted platforms, such as WhatsApp and Signal, would not be undermined by the European Parliament's draft amendments to rules aimed at detection and removal of child sexual abuse material online, says the lawmaker steering the draft law through the legislature.

“The important thing is that we are not going to say anything weakening the encryption, but there are some technical developments already ongoing, so [detecting abuse material] is possible without having access to the content,” said Javier Zarzalejos in an interview with MLex.

Zarzalejos, a Spanish conservative, is responsible for drafting the first round of parliamentary amendments to the controversial Regulation to Prevent and Combat Child Sexual Abuse.

The draft regulation will make it mandatory for providers of messaging and cloud storage services, such as Meta Platforms and Google, to perform a risk assessment and develop mitigation strategies to reduce the spread of child sexual abuse material, known as CSAM, on their servers.

If a court or other administrative authority determines a “significant risk” of a company’s services being abused by predators, they will issue a detection order. These orders could force platforms to scan user communications with technology determined by the authority. Zarzalejos said that detection orders would be a “last resort.”

— Opposition —

The European Commission's draft regulation has garnered significant opposition since it was presented last May.

A joint statement from EU privacy watchdogs, the European Data Protection Board and the European Data Protection Supervisor, said it was not a proportionate or effective measure (see here).

In a joint letter last June, 124 digital privacy NGOs, including Access Now and European Digital Rights wrote that the proposal should be withdrawn because it threatened free speech and privacy.

An impact assessment requested by the parliament also found that the proposal was “highly problematic” due to potential privacy harms and the immaturity of necessary technology (see here).

These concerns focus on balancing the need to protect children from online abuse and preserving free speech and privacy rights (see here).

“We are definitely very aware of the importance of respecting fundamental rights, and at the same time we really want to include within those fundamental rights of the children which have been assaulted and abused,” Zarzalejos said.

He said his draft amendments emphasize the importance of maintaining the integrity of end-to-end encryption, creating a “future-proof” framework that allows for technological innovation and establishing “preventive” measures such as digital literacy education for children.

The regulation is on lawmakers’ desks in time to replace a temporary measure that allows companies to scan for CSAM voluntarily but that expires in August 2024 (see here). If lawmakers cannot pass this new regulation in time, companies may not be allowed to scan user communications for CSAM.

Zarzalejos said that even if discussions on the new law take time, however, something will be worked out before that happens. He said there was a “clear political consensus” to continue allowing platforms to scan for CSAM.

— End-to-end encryption —

End-to-end encryption, or communication that only the sender and receiver can decrypt, is protected in the report, Zarzalejos said. Services offering end-to-end encryption, such as Meta’s WhatsApp or Signal, will not be forced to break their encryption under detection orders, he argued.

But messaging and cloud storage service providers may have to use other technologies to find CSAM on their platforms.

“The principle of integrity of encryption is upheld,” Zarzalejos said. “Well, does that mean that we have to make it just a black box in order to prevent any effort to find the case, and try to fix it from abuse? I don't think so.”

Zarzalejos said the use of metadata is mentioned as an effective detection method in his report. Scanning metadata would allow companies to look for suspicious behavior or usernames on their servers without having access to contents of communication.

Client-side scanning, a controversial method for scanning the contents of encrypted messaging without technically breaking the encryption, is not specifically mentioned in the report, according to Zarzalejos. It is unclear if courts will deem the technology as upholding the integrity of encrypted environments, but privacy advocates, including European Digital Rights, have said client-side scanning breaks encryption in practice.

End-to-end encrypted messaging will be included in the EU’s CSAM prevention regime, but Zarzalejos says lawmakers will leave decisions up to judicial and independent authorities on what technology companies use to find the illegal material.

“It should not be the focus of our debates because it is not for us to decide what kind of technologies are used,” Zarzalejos said.

— Scope —

The commission’s original proposal said platforms would need to detect three types of CSAM: known, unknown and grooming. The initial draft report from the parliament’s leading committee maintains this scope, Zarzalejos said.

Known CSAM is that previously reported and included in databases that companies can use to find replications. The automated detection of this type of abuse material is largely uncontroversial.

But unknown CSAM or grooming content requires scanning technology that is more error-prone and too “immature” for preventing it, according to the parliament-requested impact assessment.

But Zarzalejos has kept these categories of CSAM in his proposal. He says the possibility of false positives will be counteracted by safeguards of human reviewers, who will see all material flagged by AI systems as potential CSAM.

“Human review has never been put into question,” Zarzalejos said. “We have never thought that detecting or responding to unknown material should be an automatic process.”

— Prevention —

Zarzalejos said there is a new focus on the prevention of abuse in the parliament’s proposal. While scanning content for CSAM may discourage perpetrators, the commission’s proposal did not include measures that would specifically prevent online abuse from happening in the first place.

One prevention method would have platforms implement self-reporting channels in a “child-friendly manner.” Another would require age recommendation labels on platforms.

He says the draft also gives education responsibilities to the EU Center. The center would provide educational materials for parents, guardians and teachers to teach children more about digital safety so they can more safely interact with others online.

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):
Regulation - Proposed legislation to combat child sexual abuse online (EU)

Areas of Interest: Data Privacy & Security, Sector Regulation

Industries: Communication Services, Information Technology, Interactive Media & Services, Media & Entertainment, Software and Services

Geographies: EFTA, Europe, EU