WhatsApp, Signal could use behavioral data to comply with EU lawmakers' rules on child abuse material

20 Apr 2023 | 11:26 GMT | **Insight**
By Lucy Valeski

Encrypted messaging services, such as WhatsApp or Signal, may be able to use behavioral data instead of accessing the content of user communications to detect child sexual abuse material, to comply with an EU draft regulation trying to catch perpetrators online. Providers of messaging and cloud storage services will also be required to participate in prevention measures, such as age assessments and parental controls, under new rules from conservative Spanish lawmaker Javier Zarzalejos.

Encrypted messaging services will be required to process users' metadata — such as usernames, locations and behaviors — under the European Parliament's initial amendments on a draft regulation attempting to stamp out child sexual abuse material online (see here).

This would allow the end-to-end encrypted messaging platforms, such as Meta Platforms' WhatsApp or Signal, to maintain the "integrity" of their service by not exposing the content users' communications. WhatsApp already uses metadata to detect potential abusers voluntarily.

The parliament's draft, which hasn't been published but has been made available to journalists, says encrypted platforms will be allowed "to process metadata that can detect suspicious patterns of behavior without having access to the content of the encrypted communication."

But this protection does not go far enough for some privacy advocates, for example German Pirate Party member Patrick Breyer. He is concerned that this wording does not explicitly prohibit client-side scanning, a controversial technology that scans content before it is encrypted.

"The wording is not yet sufficient to exclude mandatory client-side scanning with certainty. Some argue client-side scanning wouldn't interfere with the encryption process as such," Breyer said in a statement today.

The draft Regulation to Prevent and Combat Child Sexual Abuse would make it mandatory for providers of messaging and cloud storage services to perform a risk assessment and develop mitigation strategies to reduce the spread of child sexual abuse material, known as CSAM, on their services.

If there is still a "significant risk" of a company's services being abused by predators, it could be compelled by a court to scan user communications with technology determined by the judicial or independent authority.

Conservative Spanish lawmaker Javier Zarzalejos is responsible for steering the regulation through the parliament's civil liberties committee. His amendments on end-to-end encryption will be debated over the next few months as lawmakers try to determine the best way to protect both children's and users' privacy.

Lawmakers have a committee vote planned for September, and a full parliament vote is scheduled in October. At that point, EU lawmakers will begin negotiating with EU governments, which are working on their version of the text, to reach a final agreement.

— Prevention —

Providers of messaging and cloud storage services will also have responsibilities to promote prevention under the draft amendments from the parliament.

Companies will be required to provide "clearly visible and identifiable" age ratings on their services. They will also have to try and keep children off risky platforms through age assessment.

The new draft amendments also call for self-reporting channels on messaging services that would allow users to flag illegal material to the service provider.

Finally, service providers will be required to “reinforce awareness-raising measures” on their platforms.
In addition to overseeing the implementation of the regulation, the EU Center on Child Sexual Abuse will have responsibilities in creating educational materials about digital literacy for children.

— Voluntary detection orders —

The parliament’s draft regulation will allow service providers to voluntarily scan for CSAM on their platforms through voluntary detection orders.

The judicial and independent authorities that are responsible for issuing detection orders can also authorize platforms to use specific technologies to combat CSAM. The provider could request authorization prior to scanning communications or metadata.

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