Meta

EU Youth Privacy Forum

“Keeping young people safe”

29 JUNE 2022 | BRUSSELS, BELGIUM

The forum was conducted under
the Chatham House Rule.

1. Background

Meta's inaugural EU Youth Privacy Forum took place on 29 June 2022. Attendees including policymakers, industry, youth related service providers, academia and NGOs met in Brussels to discuss key challenges and exchange views on topical privacy policy issues regarding young people online.

The forum has been established to bring together diverse stakeholders that have an interest in youth issues to discuss key challenges and exchange views on topical privacy policy issues regarding the protection of young people online. The forum seeks to facilitate discussion between industry, regulators, trades and NGOs, and fills a gap for engagement in the youth policy landscape. The forum also provides a space for Meta to proactively share its views and positions on youth, harvest feedback and promote best practices as it builds towards the metaverse.

The forum will be running as a series of regional and thematic workshops and events, with the next events planned for Autumn 2022 (see further below). Future sessions will see stakeholders from other disciplines and policy areas invited in order to ensure balanced and representative discussions.

2. Introductory remarks

Meta's David Miles, EMEA Head of Safety, Cecilia Alvarez, EMEA Director of Privacy Policy Engagement and Simon Weidler, Privacy Policy Manager, welcomed attendees to the Meta EU Youth Privacy Forum kick-off event.

David introduced the session, highlighting the important responsibility held by policymakers to strike a careful balance between children's privacy and safety. He shared the example of Meta's own 'best interests of the child framework', explaining how it is underpinned by Meta's approach to children and youth.

The framework covers Meta's product design principles of responsible empowerment, age-appropriate safeguards and the need for constant innovation to deal with existing and emerging harms.

As an example of innovation and cross-industry collaboration, David shared news of Meta's recently announced new ways to verify age on Instagram. This testing, currently underway in the US, allows users to verify their age using a combination of social vouching and selfie video "face-based-age-prediction" through a third party, Yoti. Working with Yoti, Meta are finding innovative solutions to combat challenges faced within the youth sphere. Such collaboration will be key if the industry is to effectively tackle existing and emerging harms.

Cecilia shared with attendees that this event is the first of a series to discuss how to empower and protect youth online. She explained that having joint conversations to develop a holistic approach to reconciling privacy and safety aspects is important, particularly with the development and the increased interest around the Metaverse.

Cecilia spoke about 2022 being the "year of youth", with several EU legislative and regulative initiatives (for example DSA (Digital Services Act) and DMA (Digital Markets Act) being adopted later this year, thanks to which data protection authorities have been giving guidance.

Cecilia highlighted that understanding users' age is one of the most important aspects that Meta is addressing in developing the right experience for the right age. She shared two guiding principles. The first being the best interest of the child framework: children also have rights, and we need to find a way to empower them. And secondly, Cecilia reflected on the importance of having a parent's perspective on these issues and to take decisions on the best way to handle the challenges. Every parent has a role to play, from policymakers to families.

Simon shared the vision for the forum of bringing together diverse stakeholders with an interest in youth issues to have a constructive and structured dialogue on protecting young people online and the regulatory context in a series of workshops and events.

3. Roundtable discussion: "Combatting CSA (child sexual abuse) in light of the CSAM (Child Sexual Abuse Material) Regulation"

INTRODUCTION

The roundtable started with an overview of the European Commission's proposal for new EU legislation to prevent and combat CSA online. This included background to the proposal and an explanation for how the new Regulation might work in practice, aiming to create a long-term instrument built to last a decade or longer. This initiative is complementary to the DSA as it's a sector-specific Act. The initiative includes obligations for service providers.

The roundtable discussion that followed focused on the challenges arising from this, particularly in striking the right balance on childrens' right to privacy and their safety online.

We have a responsibility to protect children. One of the main goals is to create an environment that would be friendly to children and unfriendly to abusers. Reporting sexual abuse online is not a straightforward process currently. National policies could lead to fragmentation, for example in criminal law, but the proposal seeks to make it more straightforward.

Many players are involved in issuing orders, and it has to be strictly targeted before a decision is taken, thanks to the risk assessment that the provider must comply with. Member States will have to designate authorities to enforce the Regulation and this authority can request a detention order to be issued to the Member State. There is a need to support detection, investigation and prevention of abuses. Prevention is one of the key pillars of the regulation for the Commission. The proposal suggests establishing a European Centre to facilitate and support implementation of the Regulation. The European Centre would receive reports from companies and undertake initial filtering to avoid overwork and to ensure that the work done is qualitative. The EU Centre would provide reliable information on what constitutes sexual abuse under EU law. It would have the capacity to help victims remove material online, and signal when some material is shared again. The EU Centre needs to have the capacity to help them.

It was shared that the industry must come up with the means to tackle child sexual abuse online. The proposal takes a technology neutral approach to solutions. There was acknowledgement that this will be a difficult process, especially in striking the balance between the privacy of children and their safety; it is a challenge to find the right balance between different rights.

INDUSTRY VIEWS

The Commission's leadership towards building regulation to better tackle CSAM was acknowledged by attendees. Industry representatives then shared their approaches to tackling CSA online.

Concerns were shared about the proposed Regulation's detection-led approach and the lack of proposal for how to prevent harm happening in the first place. Detecting CSAM after the fact isn't enough. The priority is, and should be, prevention.

Industry shared its commitment to prevention of CSAM, highlighting the protections used by default for young people alongside technology to identify and address potentially malicious activity.

For example:

- Machine learning to identify and analyse behavioural data across platforms.
- Private default experiences for minors, such as preventing unconnected adults from sending friend, message and call requests, limiting how minors can be found in Search, and defaulting minors to private account settings.
- Education through in-app advice and pop-up safety notices for young users. All of the prevention methods mentioned work with end-to-end encryption, allowing individual's private messages to continue to be safe and secure.

From an initial assessment of the CSAM proposal, an industry representative flagged a concern on the topic of end-to-end encryption. CSS (client side scanning) (a system to scan private messages and content against a database of hashes) raises concerns for encryption. In the “Bugs in our pockets”[1] report it flags that CSS would create “serious and security privacy risks for all society”. That report sets out that the software allowing CSS is vulnerable to hacking. Abusers could also evade the database through manipulating the software, or it could be evaded by using dark web or certain devices without CSS software.

It was felt that in the detection versus prevention debate there should be a wider view on combating abuse and stronger focus on prevention. Prevention needs a different set of safeguards and transparency mechanisms. For instance, notifying potential bad actors about restricting the ability to reach out to minors would not be proportionate due to the low impact this has (compared to law enforcement reporting). Such a notification would alert the potential bad actor about what triggered the mechanism. Instead, a more proportionate safeguard would be to have general transparency around prevention measures implemented, and a privacy body reporting to the Commission that ensures safety measures are correctly implemented (instead of individual appeal mechanisms). Industry representatives acknowledged that privacy should be approached in a holistic way. Children’s rights include the right to privacy however the proposal from the Commission so far has focused only on the right to protection from abuse.

One industry representative flagged the importance of industry collaboration. It is commonly accepted that predators move between platforms.

They shared that they report a lot of content however, this is not just because of the number of users but because they actively look for such content. They flagged that it should be borne in mind that a lot of the content itself is self-generated by young people.

Industry is building products which have safety inbuilt from the design stage. They recognise the need for some parental control but acknowledge that as young people grow, they have the right to explore more of the internet unsupervised. There is a role for education here, but education is not enough if the products they are using are intrinsically unsafe.

An area of focus for industry is to improve understanding of whether a user is a minor or not.

Another industry representative shared that they have a team of analysts for whom reviewing reports of CSAM is a top priority. As part of their commitment to their community standards they review reports from both users and hosts. They have a law enforcement request system which makes it easier for law enforcement to intervene at the earliest stage.

As with others in the industry, there were some concerns over whether the right balance is being struck in the proposal. They highlighted feelings that there was a lack of clear risk based approach and not enough differentiation about how interpersonal communication services can present a risk.

[1] . https://arxiv.org/abs/2110.07450

FOLLOW-UP REMARKS

There were industry concerns about scanning personal communications and the implications on this for end-to-end-encryption. Would the proposals set out by the Commission lead to the end of encryption? The Commission wants to find other ways to detect CSAM which do not affect encryption. The goal should be to have less need for detection and more effective prevention. It was discussed that the rule on detection does not mean that detection is the focus of the Regulation. Development should be done to find better solutions rather than relying on detection.

It is important to recognise the differing cultural positions across Member States. An example was given of different approaches to gay rights. Regulation must reflect that some member states are more restrictive than others.

Concerns were flagged about children's rights to participate and explore their sexuality and political affiliation, for example, whilst being totally independent of their parents on social media. It was indicated that whilst a balance is being found, it is possible that seeking to protect children could instead present other conflicts.

The forum discussed how industry can measure the success rate of its preventative measures. It was noted that the growth of CSAM in the global south is unprecedented. It was agreed that content scanning is an old technology. Content scanning drives up the number of reports but doesn't necessarily correlate with quality of reports.

New and innovative technologies will help measure success and improve quality of reports, for example use of artificial intelligence and machine learning. The industry agreed that prevention should come first. This would help avoid some abusive behaviours and give young people the tools to avoid abuses, while being more aware of the risks. The proposed Regulation would benefit from more clarity on how grooming could be tackled, particularly on leveraging communications metadata.

SUMMARY OF INDUSTRY REMARKS

In general the industry welcomes the Commission's initiative.

Roundtable discussions highlighted some concerns across the industry about the proposed Regulation in its current form, particularly about some of the proposed processes in addition to implementation and enforcement. The key challenges raised were:

- Lack of clear risk-based approach.
- Definitions used i.e. significant risk.
- Lack of legal basis.
- Technology neutral approach – detection is important, but it should be secondary – the first goal should be to have no CSA in the first place, and focus on prevention. This aspect is not present enough in the proposal.
- Taking a more holistic approach when looking at privacy and safety.

4. Conclusions from the interactive discussion: Key policy challenges in the youth space - “What are the building blocks for age-appropriate design”

Rachael Gallagher, Privacy Policy Manager EMEA at Meta, presented a keynote providing an overview of the youth policy landscape. The forum split into break-out groups to facilitate discussion on two areas of focus for youth: parental supervision and age assurance.

PARENTAL SUPERVISION

The group considered the tools that could be used under the banner of parental supervision and discussed parental consent versus parental control.

It was agreed that parental consent was not the best tool and doesn’t leave autonomy to the child. Parental consent is not very transferable and parents should have the option, depending on the technology, to activate or restrict features depending on the age of their children. There are a number of challenges for implementing parental consent for example verifying parental responsibility, whilst respecting data minimisation, and acknowledging different family structures.

Parental control was the preferred approach and provided for a more positive outlook given certain risks. The group acknowledged that children have rights to privacy and should be made aware when they were being supervised. The group considered the risks involved with children using technology, for example grooming and addiction. There was a consensus that there is a need to identify different tools for different risks and that one may be more suitable for a particular risk than another.

The group considered the approach taken by some companies whereby they are seeking to avoid problems occurring from the outset. It was however agreed that teenagers should be enabled to make mistakes and experiment on their own. This contrasts with the position for younger children where it was agreed different measures would be more appropriate.

AGE ASSURANCE

The group considered the purpose of age assurance. It was generally felt that age assurance was not about locking children out of experiences or identifying age for the sake of it, but to ensure services and user experiences were safe.
It was acknowledged that this is a complex space and that there is no silver bullet.

The group highlighted key principles that must be considered for age assurance systems, namely:

- Data minimisation
- Transparency
- Importance of trust
- Privacy
- Proportionality

The group discussed what criteria for success looked like in age assurance. It was recognised that no technology is 100% accurate. Greater accuracy can be given for identifying users who are 18+ and that the purpose of the data collection would depend on how important accuracy is. The group questioned how systems could be certified and quality assured. A distinction was made between age assurance for content regulation and data processing regulation.

At present, there are a number of challenges for industry surrounding age assurance. There are concerns around exclusion and the wider cultural attitude towards age assurance processes.

Generally, services need to obtain further information from a user to determine whether someone is a child or not. The group also flagged a question about what happens with content wrongly removed online.

It was agreed that age assurance does not exclude parental control.

There is a need for age assurance to be neutral. The group felt there was benefit to using a sandbox in order to share best practices and to develop greater clarity over standards, including those for interoperability. Safety by design is crucial.

5. Meta Quest 2 demo

Forum attendees had the opportunity to network and experience VR in between discussion sessions. Attendees were able to experience Meta Quest 2, in particular Rebuilding Notre Dame, First Steps and National Geographic.

6. Closing remarks and next steps

Cecilia and David brought the event to a close. They shared that the forum was a historical moment for this kind of conversation, with all the legislative and regulatory initiatives happening between all key players (EU institutions, industry, associations).

The main conclusion and agreement among attendees was that there is real hope to have more useful and constructive debates soon, to ensure the safety of young people vonline while guaranteeing their rights to privacy and their personal development.

Meta is excited to announce that following the success of our first event, we will be holding two events this autumn. The first event will be held in Brussels in the afternoon of **26 October 2022** building on discussions from our June event and taking a deep dive on preventing child sexual abuse online. Our second event will be held later this year, and will focus on age appropriate design. Invitations to follow.

Meta

EU Youth Privacy Forum

29 JUNE 2022 | BRUSSELS, BELGIUM