Meta

May 19, 2026

Dear Chairman Grassley,

Thank you for your letter and for the opportunity to address these important issues. Child exploitation is a horrific crime that Meta works to fight aggressively on and off its services. Meta has spent more than a decade developing policies and technology, as well as valued partnerships with law enforcement and the National Center for Missing & Exploited Children (NCMEC), in an effort to help keep young people safe. We are proud of our industry-leading investment and leadership in this area and we are committed to continuously improving. Given our leadership and extensive collaboration with NCMEC, we were disappointed to see the characterization of our CyberTip reporting program in NCMEC's March 16, 2026 letter. We welcome the opportunity to provide important context not reflected in that letter.

To be clear at the outset, Meta condemns the predators who target and exploit children. We will continue to strengthen our programs to find these criminals, stop them, and report them—and we support efforts to ensure they are held accountable.

To that end, as part of our ongoing work to make the internet safer for children, we have worked with NCMEC since 2006 in an effort to reduce child sexual abuse material (CSAM) online and help ensure that incidents are reported. We are proud of our work in this space, and continue to report CSAM and other child sexual exploitation to NCMEC's CyberTipline. Thanks to our ongoing investment in detection and reporting, we continue to report more to NCMEC than any of our peers. As NCMEC has said repeatedly, these figures are a reflection of Meta's commitment and investment in robust detection and reporting—not an indication that the problem is worse on Meta apps. Our CyberTipline reporting is just one part of our comprehensive work with NCMEC to improve the child safety ecosystem online. As discussed further below, we also participate in numerous voluntary NCMEC initiatives, including training, capacity-building projects, and technical tool development and support.

We believe the facts reflect a more complete and nuanced picture than the March 16th letter suggests. Maintaining the quality and utility of our reports is of utmost importance to us, and we have invested resources and built tools to that end. We also maintain an open line and regular cadence of communication with NCMEC and seek to address concerns NCMEC may raise, including those noted in your letter. We are committed to constant improvement and appreciate feedback, which has already led us to make improvements, as NCMEC has acknowledged.

With this context in mind, we provide additional information below regarding our child safety work, including our engagement with NCMEC and other organizations to create industry-wide solutions to address these important issues.

Meta's Approach to Child Safety

As part of our longstanding commitment to child safety, we have spent years developing policies and technologies to help keep young people safe and to thwart predators' and criminals' attempts to use our services to abuse children.

We have developed a three-pronged, industry-leading approach to protecting young people online. First, we focus on preventing harm from happening in the first place. We do that by enforcing our comprehensive and aggressive policies and developing cutting-edge, preventative tools. Second, we make it easy to report unwanted interactions and potential harms. And, third, we respond and take action. We also work to provide resources and support to victims. We work with professionals, collaborate with industry experts like NCMEC, and support law enforcement around the world to help fight the online exploitation of children. These efforts are supported by significant and sustained investments in safety. We have spent more than $30 billion overall in the areas of safety and security over the last decade, an investment that reflects our status as an industry leader in this space.

When we become aware of apparent child sexual exploitation, we report it to NCMEC in accordance with applicable law so NCMEC can coordinate with law enforcement authorities from around the world. We also engage law enforcement in a variety of ways, including by directly alerting them when we become aware of someone at imminent risk of harm, and by responding to valid legal requests for information. In 2024, we received over 9,000 emergency requests from U.S. authorities and resolved them within an average of 67 minutes—and even more quickly for cases involving child safety and suicide.

Meta recognizes that, in many countries, CyberTipline reports can outpace law enforcement capacity to assess and act on those reports. To address this challenge, we partnered with NCMEC and the International Justice Mission to create Project Boost, a global training effort to help authorities identify children being sexually exploited online and arrest perpetrators of such abuse. Founded as a capacity-building project, Project Boost enables law enforcement to more effectively act on CyberTipline information and includes training on NCMEC's Case Management Tool. Project Boost has been rolled out in multiple countries and has supported meaningful enforcement outcomes, including cross-border sextortion investigations publicly acknowledged by the U.S. Department of Justice.

In addition, we engage with NCMEC to continuously improve the quality and prioritization of our reports. This engagement has resulted in meaningful changes to our reporting policies, tools, and workflows, including refinements to how we prioritize time-sensitive cases, more context and structure within reports to support law enforcement triage and investigations, and safeguards designed to reduce duplicative or low-signal reporting. Indeed, since May 2024, a

team that includes our dedicated NCMEC Reporting Technical Program Manager has launched or advanced over 100 distinct technical enhancements to our child safety reporting program. Though NCMEC fails to acknowledge these efforts in its letter, our enhancements have improved reporting quality, regulatory compliance, new platform integrations, and industry collaboration.

Our ongoing work also involves structured, operational meetings with NCMEC and frequent staff contact, technical collaboration, and implementation of reporting enhancements informed by feedback from NCMEC and law enforcement. We have dedicated specialized teams and subject-matter experts, who—among other things—strengthen our CyberTipline reporting systems and processes, reflecting our view that protecting children—both on and offline—from despicable child predators requires ongoing iteration and cross-industry collaboration.

Child Safety: Policies, Prevention, Deletion, and Enforcement

We have strict policies against child nudity, abuse, and exploitation, including CSAM, inappropriate interactions with children, solicitation, exploitative intimate imagery and sextortion. These policies address content or activity that threatens, depicts, praises, supports, provides instructions for, makes statements of intent, admits participation in, or shares links of the sexual exploitation of children. Our policies also prohibit content (including photos, videos, real-world art, digital content and verbal depictions) that sexualizes children and Groups, Pages, and profiles dedicated to sexualizing children. These content policies apply regardless of whether an account is run by a teen or by an adult or whether the content depicts real or non-real children. When we find this type of violating content, we remove it, regardless of the context or the person's motivation for sharing it. We may also disable the account of the person who shared it, unless it appears the intent was not malicious (for example, to spread awareness of child exploitation).

We continue to take aggressive action on accounts that break our rules, including those that violate our child safety policies. We go beyond legal reporting requirements and use sophisticated technology to proactively seek out abusive material. We work constantly to find and remove policy-violating content, including comments that praise or support the sexual exploitation of children; deactivate accounts of predators; and dismantle abusive networks. For example, in early 2025, our specialist teams removed nearly 135,000 Instagram accounts for leaving sexualized comments or requesting sexual images. We also removed an additional 500,000 Facebook and Instagram accounts that were linked to those original accounts. We also let people know that we had removed an account that had interacted inappropriately with their content, encouraging them to be cautious and to block and report.

We also encourage people to report anything on our apps that they think may violate our policies, including and especially as it relates to child sexual exploitation. We have built systems and review processes to prioritize and appropriately address violating content or accounts, and, when appropriate, report it to NCMEC or law enforcement. We have also made our reporting tools easier to find.

In addition to these policies, we design our products to help prevent harmful interactions from occurring in the first place. For example, Teen Accounts have built-in protections that limit who can contact teens under 18 and the content they see. We automatically place teens under 18 into Teen Accounts, which are private and in the strictest message settings by default, and teens under 16 need a parent's permission to change any of these settings to be less strict. In practice, this means that teens in Teen Accounts can only be messaged by people they follow or are already connected to and that only people they approve as followers can see and interact with their content. For years, we have also used technology to prevent potentially suspicious adults from finding, following, or interacting with young people. We deploy machine learning to proactively detect accounts engaged in certain suspicious patterns of behavior by analyzing dozens of combinations of metadata and public signals, such as if a teen blocks or reports an adult, or if someone repeatedly searches for terms that may suggest suspicious behavior. When we identify these accounts, we limit their ability to find, follow, or interact with teens or each other, and we automatically disable them if they exhibit a number of these signals. In 2025, we used these signals to identify more than 265 million Facebook accounts and more than 135 million Instagram accounts that had shown potentially suspicious behavior, and we took additional steps to proactively prevent them from interacting with teens. We have expanded use of this technology to prevent these adult accounts from finding, following, or interacting with one another. On Instagram, potentially suspicious adult accounts are not recommended to each other in places like Explore and Reels, and are not shown comments from one another on public posts, among other things.

Finally, we work regularly with our specialist child safety teams and child safety professionals to help us understand attempts to evade our detection systems and bypass our policies. We recognize that predators may attempt to set up multiple accounts to evade enforcement of our policies and potential reporting to NCMEC. That is why when we disable accounts for these severe violations, we also work to disable explicitly linked accounts (where the individual has linked their Facebook and Instagram profiles), confidently linked accounts (where we have high confidence that the same person is using multiple accounts), and restrict those devices from setting up future accounts. We are working hard to further augment the measures we have in place as predatory behaviors and coded language evolve. We also hire specialists with backgrounds in law enforcement (including former federal child exploitation crimes prosecutors and former FBI investigators) and online child safety to further our efforts. These specialists monitor changing behaviors exhibited by networks engaged in apparent child sexual exploitation-related activity—such as new coded language—not only to remove and, where appropriate, report them, but also to inform the technology we use to find them proactively.

Suicidal Ideation and Self-Harm Prevention

One of the topics referenced in NCMEC's letter involves reports of suicidal ideation by a teen. We care deeply about teens' safety and well-being across our apps, and understand that suicide and self-harm are complex mental health issues that can have devastating consequences. We constantly work to develop an informed and thoughtful approach to suicide

and self harm content shared on our apps. For example, in 2017, we built integrated suicide prevention tools to support those who may be struggling, and in 2020, when we saw the need for faster access to support, we developed intelligent ways to share resources with people searching for suicide or self-injury content. We recently announced that Instagram will now notify parents using supervision if their teen repeatedly tries to search for terms related to suicide or self-harm. These alerts are designed to give parents the information they need to support their teen and come with expert resources to help parents approach these sensitive conversations.

Regarding our escalation of this content within CyberTips, Meta seeks to identify and escalate, as appropriate, mentions of suicide. We have worked closely with NCMEC to calibrate how such reports should be identified and reported, after NCMEC specifically requested that we adjust our suicide reporting to focus on the most urgent cases. Accordingly, and consistent with NCMEC's request, our goal is to prioritize urgent cases while maintaining manageable escalation pathways for NCMEC. This includes ongoing alignment on prioritization criteria to help ensure that high-priority reports reflect credible, time-sensitive risks and can be efficiently triaged.

Furthermore, in addition to reporting to NCMEC when appropriate, when we think there is an imminent risk of harm, we alert first responders or emergency services, so they can conduct a wellness check, regardless of whether or not Meta filed a CyberTip to NCMEC.

Our Work to Improve CyberTip Reporting

As noted above, we report apparent instances of child exploitation identified on our apps from anywhere in the world to NCMEC. As part of our ongoing work to provide young people with safe, positive online experiences, we also continue to provide transparency into our efforts to find and report child exploitation to NCMEC. In Q4 2025, Facebook, Instagram, and Threads sent over 2.6 million CyberTip reports for child sexual exploitation. Over 660,000 of those reports involved inappropriate interactions with children, which may include an adult soliciting CSAM directly from a minor, online enticement of a minor, minor sex trafficking, or attempting to meet and cause harm to a child in person. These CyberTips also include cases where a child may be in apparent imminent danger. Over 2 million reports related to shared or re-shared photos and videos that contain CSAM.

We recognize that the quality of our reports, not just the quantity, is important. That is why we work to make our reports as valuable as possible. Working closely with NCMEC, including in response to its feedback, we have streamlined reporting workflows and refined how reports are grouped, annotated, and routed to support more effective triage at scale. For example, we partnered with NCMEC to streamline our reporting process by grouping viral or meme content into a single CyberTip through a process known as "batching." This was an investment in technical mechanisms across our reporting systems to reduce repeat or near-identical submissions. This contributed significantly to the drop in overall CyberTips in 2024, and allowed NCMEC and law enforcement, including Internet Crimes Against Children (ICAC) task forces, to more easily manage and prioritize CyberTips.

Additional efforts are listed in detail below:

- We understand that in mid-2025, NCMEC and law enforcement experienced a temporary influx of duplicative and near-duplicate CyberTip reports from Meta due to our expansion of proactive scanning on Instagram. We treated this with the seriousness it deserved and deployed targeted fixes that reduced duplicative conversation-based reports. This issue is now fully resolved, with monitoring in place.

- We have also prioritized improving the availability and clarity of location-related information in our reports when such data is available and lawful to provide. For example, beginning in April 2025, we began including last-known location coordinates on Instagram reports to help victim safety checks and jurisdictional routing. In January 2025, we began including network source port numbers alongside IP address to improve law enforcement device attribution behind a shared internet connection. In response to feedback from ICACs, we also added device identifiers into standardized structured fields aligned with NCMEC's parsing systems, increasing machine-readability for NCMEC systems and improving cross-referencing for law enforcement. We have expanded the inclusion of other technical metadata and context improvements to aid law enforcement, such as standardized timestamps to Coordinated Universal time across all reports; expanded chat context in WhatsApp reports; expanded reporting to cover audio content; and included victim profile photos after requests from multiple law enforcement jurisdictions.

- NCMEC also provided feedback regarding the classifier we use to predict a person's age, including when we believe minors are lying about their age. Contrary to the assertions in the March 16th letter, this classifier has been in use for years, and makes predictions based on signals like profile information, account activity, and interactions with other profiles and content. When Meta detects a likely age discrepancy during an exploitation-related investigation, it reports to NCMEC even though the user's self-reported age is 18 years old or over. According to feedback from law enforcement, Meta's reports did not adequately explain why Meta believed the user was actually a minor and therefore the information was insufficient to obtain judicial authorization to request records from Meta via subpoenas or search warrants. In addition, given the volumes of reports they receive, law enforcement expressed that they had limited resources to conduct welfare checks based solely on the information provided. Given the complexity of this work, and to improve this reporting in response to feedback from law enforcement, we updated the language we use in reports in March 2025 to help explain the underlying technology. We also began including Facebook and Instagram bios for additional context, to help law enforcement and judges understand why we believe the reports actually involved minors (when they otherwise appeared to involve people 18 years old or over). We also updated the reports to ensure that all text-based reports contain at least 30 messages of conversation to capture potential age confessions by the potential minor.

- Further, in December 2025, we developed the “Age Assertion Discrepancy” annotation, which is applied to reports where the classifier flags a user as a likely minor but the user self-reports as an adult and there is no age confession anywhere in the conversation or bio. Reports in such circumstances include this annotation to provide additional information to NCMEC and law enforcement, reflecting a response to law enforcement feedback and so that NCMEC can appropriately route these reports. We continue to evaluate further refinements in cooperation with NCMEC and ICACs.

- Regarding gore content in reports, in late-October 2025, NCMEC flagged that certain Meta reports contained gore content with no connection to child exploitation. We identified the root cause—a technical issue with how multiple media files were bundled together—and deployed an initial fix in December 2025. We have continued to address edge cases and deployed additional automated gore classifiers as a further guardrail. This issue is now fully resolved across all workflows.

- Similarly, the volume of Meta’s online enticement reports surged beginning in 2024, driven in part by the U.S. REPORT Act—legislation Meta supported and for which we executed 16 separate compliance workstreams. This surge, while reflecting our expanded detection and compliance efforts, created triaging challenges for law enforcement, which Meta took seriously. In September 2025, we launched updates developed jointly with NCMEC, including a new “Unsolicited Obscene Material Sent to a Child” incident type for sexualized conversations without aggravating factors to help enable NCMEC to route these lower-priority reports informationally rather than directly to ICACs. In January 2026, we discovered that NCMEC had a coding error that was incorrectly routing these reports directly to ICACs, contrary to the agreed-upon approach. Fixing this bug alone reduced the volume of non-CSAM reports reaching ICACs by approximately 45%. As a result of the work we did to solicit feedback from both ICACs and NCMEC, we are also planning a broader recalibration of our reporting approach, which will further reduce lower-priority report volumes reaching ICACs.

We remain committed to leading in the fight against online child exploitation and will continue to devote significant resources and attention to these efforts. In 2026, we have continued advancing these efforts through additional technical safeguards, internal quality-assurance measures, and further expansion of structured data and annotations in our reports. We will continue making refinements to improve our reporting process.

Collaboration with Industry and Child Safety Organizations

Finally, we continue to collaborate with experts and our industry peers to address potential threats and develop educational programs to empower teens and parents to take control of their online experience. This includes:

- Co-hosting with NCMEC in August 2025 a first-of-its-kind roundtable on sadistic online exploitation, bringing in law enforcement, researchers, and private industry from around the world to share best practices on tackling this new and quickly evolving harm type.

- Supporting NCMEC to develop Take It Down, a tool that helps prevent teens' intimate images from being shared online. We provided financial support to NCMEC to develop Take It Down, building on the success of StopNCII.org, a platform we developed that helps adults stop the spread of their intimate images online. We have made both Take It Down and StopNCII easily accessible on our apps when people are reporting potentially violating content.

- Launching awareness campaigns to educate teens and their parents on sextortion, and working with Childhelp on a first-of-its-kind safety curriculum for U.S. middle schoolers. Educators, caregivers, and advocates who use the curriculum report plan to reach more than 1.5 million children within one year. Meta fully funded the curriculum, which was developed with input and resources from a range of world-leading child safety experts, including from NCMEC, Thorn, the Department of Homeland Security, Purdue University and the Crimes against Children Research Center.

- Working with the Tech Coalition as a founding member of the Lantern program, which allows participating companies to share signals about predatory accounts so they can all investigate and take action. Since launching in 2023, Lantern—which operates on Meta's ThreatExchange platform—has surpassed two million signals, with nearly one million signals shared in 2025 alone. According to a recent report, these signals contributed to enforcement actions against 164,575 accounts, 163,112 URLs, and 26,119 pieces of content between 2023 and 2025 across participating platforms, demonstrating the program's growing impact as important industry infrastructure in combating online child sexual exploitation and abuse.

- Working with Mental Health Coalition alongside other industry peers as a founding member of Thrive, which allows tech companies to share signals about violating suicide or self-harm content and stop it spreading across different platforms.

We value our longstanding partnership with NCMEC and will continue to work collaboratively with NCMEC, industry, and law enforcement to improve child safety on and off our platforms.

Thank you again for the opportunity to address this important topic.

Sincerely,

Brian Rice
VP, Public Policy