

FILED UNDER SEAL

EXHIBIT 43

**HIGHLY CONFIDENTIAL
ATTORNEYS' EYES ONLY**

**EXPERT REPORT OF
Rickey Kitch**

*State of New Mexico, Ex Rel., Raúl Torrez, Attorney General v. Meta Platforms, Inc.;
Instagram, LLC; Meta Payments, Inc.; and Meta Platforms Technologies, LLC*

First Judicial District Court, Santa Fe County

No. D-101-CV-2023-02838

July 11, 2025

images, write reports, prepare discovery, and appear before a grand jury or at a preliminary hearing, and participate in pre-trial interviews, a typical cybertip investigation will take at least 51 hours and sometimes more than 221 hours, or a median of 136 hours. The ICAC unit currently has two investigators/agents. Given the current demand, the NMDOJ would require an additional seven to nine full-time agents and investigators, a certified forensic examiner, and an administrative staff person. Additional agents would be needed to conduct proactive and high-level investigations, including additional chats and dark web investigations.

Opinion Three: Based on my experience and training, there are red flags of child sexual exploitation that can be observed online.

Opinion Four: In my experience, Meta's platforms are frequently used by bad actors to identify, groom, and exploit children.

Since May 2023, when I began working for the NMDOJ, I have worked on more than 400 undercover chats that involved Facebook or Instagram.⁷⁰ Through the course of these chats, I have observed numerous contacts and conduct that indicate that malicious actors have the ability to—and do—operate on Meta's platforms. I base this opinion on my law enforcement training and experience, including investigations involving Meta and other platforms, which have made me familiar with the methods used by bad actors, and on the frequent interactions and posts that I received and observed on Meta's platforms that are consistent with efforts to identify, groom, and sexually exploit children.

Consistent with my observations and experience, the Human Trafficking Institute in 2023 identified Snapchat, Facebook, and Instagram as “The top three platforms identified to recruit victims of sex trafficking.”⁷¹

In the course of my investigations, I also have observed that specific features have facilitated efforts to identify, groom, and sexually exploit children on Meta's platforms. They include the following:

- recommendations of accounts and groups that introduced my undercover accounts to malicious users or groups or suggested these users or groups to me
- public, detailed profiles and account histories that allow bad actors access to detailed information about their targets, enabling them to more effectively target, groom, and solicit minors
- enabling users to search for specific account identifiers

⁷⁰ Because it is end-to-end encrypted, I did not use WhatsApp in my investigations.

⁷¹ Lane, et al., 2023 Federal Human Trafficking Report, Human Trafficking Institute (2024).

<https://traffickinginstitute.org/wp-content/uploads/2024/06/2023-Federal-Human-Trafficking-Report-WEB-Spreads-LR.pdf>.

- permitting ephemeral content, which emboldens bad actors to send sexually explicit images and messages and makes it difficult for users to report sexual exploitation and for law enforcement to document the evidence needed to establish probable cause
- allowing users to tag minors' photos with a photo ID or group ID
- allowing users to anonymously upload CSAM photos and videos into groups
- permitting and/or failing to report the migration of communications between adult strangers and minors to applications that are end-to-end encrypted
- enabling groups to include teen users and to search for and share specific teen accounts

In addition, I observed actions, or inaction, by Meta that also contributed to the conduct I observed:

- permitting users to search for, like, share, and sell large volumes of CSAM, with the sale often carried out on links provided on Meta Platforms
- failing to monitor or investigate complaints and reports of child sexual exploitation
- failing to block and/or delete accounts engaged in inappropriate interactions with children despite red flags
- failing to detect or verify underage users despite red flags
- failing to detect inappropriate interactions with children by considering context that indicated violating conduct, such as chats and videos
- failing to expeditiously remove CSAM from its platform or to remove or effectively block accounts that are involved in generating or selling CSAM
- failing to vet adult users that should not have accounts, such as registered sex offenders

Based on my training and experience, I have identified and observed indicators of efforts to sexually exploit children, including those I describe below. Frequently, my undercover minor personas were solicited for, offered money for, or received sexually explicit photos and sexually explicit communications, including on Meta's platforms. They were encouraged to migrate communications platforms that encrypted messages, including Instagram and WhatsApp, which I understand to be a sign that a bad actor wishes to engage in undetectable communications with a minor.

Grooming activity follows certain patterns: offering flattery ("you are so beautiful"); asking the minor persona to confirm her age ("are you really 13?"), offering the bad actor's (false) age ("I'm 14"), asking the minor about the minor's sexual experience or volunteering the user's sexual interests (e.g., "are you a virgin?" or "I have friends who have done [sexual act]"). Sometimes, the personas are sent photos of cash with a message like "can I be your daddy?" Not uncommon, too, are "hero" or "guardian" interactions, in which the bad actor pretends to offer to help the persona out of a difficult circumstance and then turns to grooming or soliciting the persona.

Meta also has identified red flags of sexual exploitation that are consistent with those described above. I reviewed an internal Meta presentation, “Understand Grooming Violator Strategies: Co-designing with Experts” given at the Crimes Against Children Conference in 2022, which identified tactics used by bad actors to exploit children based on an analysis of internal data from 100 child sexual exploitation cases on Facebook and Instagram.⁷⁹ The presentation noted that many violators “provided or offered some tangible benefit (e.g., cash, phone credits, etc.) in exchange for sexual activity or explicit material.”⁸⁰ 34% of CSAM exchanges were during “unsociable hours,” most frequently around midnight.⁸¹ Meta also found references to other platforms were “often used to direct victims to more ephemeral or encrypted services.” In addition, “[m]any violators or victim wanted to know each other’s age, not a behavior usually seen between adults.” “Past messages were often referenced (40%), a powerful manipulation tool used coercively.”⁸²

Opinion Five: Based on my training and experience, Meta and other social media platforms have expanded child sexual exploitation by introducing predators to a wide universe of children to whom they previously did not have access.

While predators have always had access to children, Meta’s platforms have enabled predators to identify, groom, and exploit children at an unprecedented scale. New Mexico receives hundreds to thousands of cybertips related to child exploitation every year.⁸³ Based on my experience when I started in law enforcement and my interactions with other law enforcement personnel, it used to be the case that a predator had to find a child in the real world and befriend or abduct that child. Now, Meta delivers a universe of kids—a virtual marketplace of minors—directly to predators’ living rooms on their phones and computers. As noted above, Meta, in particular, designs its platforms to present profiles and photographic histories of children, allowing predators not only to find them, but providing details that allow the predator to groom them.

Predators can use search terms—a list of which is attached as Exhibit C, which allow them to identify a virtual menu of potential victims. For example, CSAM sellers and buyers have used cheese pizza, which shares an acronym with child pornography, or its shortened form of pizza links, to indicate interest in or availability of child pornography since at least 2016. In my experience, searching for accounts or characteristics of children on Meta will prompt the recommendation of other similar accounts, multiplying the opportunities for a predator to find additional victims. Bad actors that interacted with my undercover accounts reported that my account was recommended, connected through groups my personals were invited to unsolicited or where my profile IDs and photos were added, or that they are a friend of a friend. In addition, bad actors can signal to each other to seek out particular children by sharing and searching for specific

⁷⁹ METANMAG-005-01333676; *See also*, METANMAG-010-00126613.

⁸⁰ METANMAG-005-01333676.

⁸¹ METANMAG-005-01333676.

⁸² METANMAG-005-01333676.

⁸³ *See e.g.*, NMAG-SM-0187369; NMAG-SM-0187370; NMAG-SM-0187371; NMAG-SM-0187372; NMAG-SM-0187373; NMAG-SM-0187374; NMAG-SM-0199119; and NMAG-SM-0187798.