

Filed Under Seal

Exhibit B

**IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF CALIFORNIA**

PEOPLE OF THE STATE OF CALIFORNIA,
et al.,
Plaintiffs,

v.

META PLATFORMS, INC, et al.,
Defendants

IN RE: SOCIAL MEDIA ADOLESCENT
ADDICTION/PERSONAL INJURY
PRODUCTS LIABILITY LITIGATION

THIS DOCUMENT RELATES TO:
4:23-cv-05448

MDL No. 3047

Case No. 4:23-cv-05448-YGR

Judge: Hon. Yvonne Gonzalez Rogers

Magistrate Judge: Hon. Peter H. Kang

TRIAL REPORT OF TIM ESTES
March 20, 2026

I. Summary of Opinions

1. The following opinions detail my conclusions based on my professional training and experience, the relevant standards in the tech industry, the relevant literature, and my extensive review of documents and testimony in this case:

2. As confirmed by the U.S. Surgeon General and my own experience and education on these issues, the Defendants' social media platforms can contribute to a wide range of harms in kids, including anxiety, depression, sleep disruption, negative body image, eating disorders, and self-harm, as well as structural changes to the brain. They have also become hunting grounds for predators seeking to sexually exploit children.

3. Meta could have (and should have) greatly reduced these harms and risks with technological solutions that were readily available to them. As outlined below, these solutions were technically feasible and in many cases had been implemented by other companies in other contexts. But Meta either did not implement them, waited unreasonably long to implement them, or implemented them in ways that were predictably ineffective.

4. **Opinion 1:** Meta should have implemented systems to help parents and guardians protect children from the potential harms of their platforms. One of the most basic ways to protect children from adult-oriented platforms is a system of age verification and Verified Parental Consent (VPC). This ensures that children or minors under a designated age are not able to set up an account without some form of adult consent and supervision. It also allows the platform to exclude the youngest and most vulnerable children altogether. Meta could have, and should have, set up an age verification and VPC system. In public statements, Meta stated that children under 13 are not allowed on their platforms. In practice, however, Meta's age verification systems were either non-existent or broken. Meta allowed millions of pre-teens to use its addictive platforms and collected data from them without obtaining any form of VPC, in violation of industry standards and regulations.

5. **Opinion 2:** Meta claims that age checks and VPC were not feasible or would have created unreasonable privacy risks are incorrect. Effective, privacy-friendly ways to check age and

(sextortion); children have committed suicide following sextortion; and children have been abducted and sexually abused by predators.¹⁷

38. Law enforcement and child safety organizations have repeatedly warned that popular apps are used to lure children into inappropriate contact or worse. In the UK, where such crimes are diligently tracked, over 7,000 instances of online grooming (sexual communication with a child) were recorded in 2023-24 – an 89% increase since 2017.¹⁸ Instagram and Facebook were among the most common platforms used by perpetrators to target children online.¹⁹ The youngest victim was just five years old – meaning a kindergartner ended up on a platform and in contact with a predator.²⁰

39. Many of these harms could be prevented or greatly reduced with technical solutions that were readily available to Meta. For example, Meta could have (and should have):

- combined age verification technology with Verified Parental Consent systems to ensure that minors could not access the platform without their parents’ or guardians’ knowledge and informed consent;

40. As outlined below, these and numerous other options were technically feasible, and in many cases had been implemented by other companies in other contexts. But Meta either did not implement them, waited unreasonably long to implement them, or implemented them in ways that were ineffective.

VI. OPINION 1: META’S AGE VERIFICATION AND PARENTAL CONSENT SYSTEMS WERE BROKEN

A. Overview

41. Having failed to create a safe environment for children, Meta should have implemented systems to help parents protect children from the potential harms of their platforms.

¹⁷ META3047MDL-014-00350154; Rothschild Dep. at 314-18.

¹⁸ Online Grooming Crimes Against Children Increase by 89% in Six Years” (Nov 1, 2024), <https://www.nspcc.org.uk/about-us/news-opinion/2024/online-grooming-crimes-increase/>.

¹⁹ *Id.*

²⁰ *Id.*

One of the most basic ways to protect children from adult-oriented platforms is a system of age verification and Verified Parental Consent (VPC). This ensures that children are not able to set up an account without some form of adult consent and supervision. It also allows the platform to exclude the youngest and most vulnerable children altogether.

42. Meta purports to exclude children under the age of 13 from its social media platforms. The company has gone further and indicated support for U.S. legislation that would require parental consent under the age of 16.

43. As described below, however, Meta failed to implement effective age verifications, and likewise failed to implement Verified Parental Consent. Typically, to determine the age of new users, Meta (at most) simply asked users to input a birthday or check a box confirming they are 13 or older. There was no real-time verification of identity, and no requirement of a parent's involvement. In other words, while they outwardly posted "No Under-13 Allowed" signs on the front door, they left the door unattended.

44. The results were predictable. Preteens swarmed these platforms en masse. Children lied about their birth dates, clicked a self-attestation box, and instantly joined the digital crowd. A 2021 survey of found that 38% of U.S. children aged 8 to 12 had used social media, and that 18% used it "every day," despite the platforms' rules prohibiting children under 13.²¹

45. In this section, I discuss how and why Meta's age verification and parental consent systems became a broken facade, chronicling each platform's failures to keep young children out.

B. The Need for Age Gating and Parental Consent is Well-Recognized

46. Based on my experience, including my work setting up AngelQ, an online platform that provides a safer search and exploration experience to children, I have become intimately familiar with the legal requirements and best practices for providing online platforms to children.

²¹ The Common Sense Census: Media use by Tweens and Teens, Common Sense Media, (2021) https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf at p.33.

CONFIDENTIAL

have to do anything about it.” Meta’s response to reports of underage users reflects this: in 2020, Meta had to create an underage enforcement war room to attempt to clear a backlog of more than 1.16 million reports. Considering how difficult it is to report, this is likely a small window into the true scope of the problem.

59. Even after Instagram began asking users for their age in 2019, it did not require any verification (such as an ID or credit card check). Meta’s former Product Leader for Site Integrity, Arturo Bejar, acknowledged that it is “well-known in the industry” that kids can simply “lie [about their age] when they sign up for an Instagram or other social media account.” Bejar testified that, during his time at Meta (through 2021), he “was not aware of any efforts to detect or remove under-13 accounts.” That was despite Mr. Bejar stating that Instagram “was not a safe place” for kids younger than 13.

60. According to Mr. Bejar, Meta had “the ability to build effective tools to try to prohibit kids younger than 13 from being on Instagram,” but chose not to do so. This is confirmed by Meta’s own admissions in this case. In sworn responses, Meta acknowledged that, “[p]rior to December 2019, Meta relied on a user’s stated age from either their Facebook or Instagram account(s) (if available) to determine whether a user fell within an age group for age-based targeting; and if no such age information was available, Meta relied on a predictive age model to determine whether a user fell within a particular age group for ad targeting.” If Meta had a predictive age model sufficient for purposes of ad targeting, surely it could have deployed that model to identify and kick off children under the age of 13 consistent with its stated policy.

61. Far from attempting to remove such accounts, Instagram “made it almost impossible to report underage accounts” and implemented “features that were designed to appeal to those kids.” In a video I have reviewed from 2023, Mr. Bejar conducted an experiment where he set up a brand new account and watched Reels served by the Instagram algorithm. When a video of a child that appeared to be under 13 was shown, he would watch the video in full; for other videos, he would swipe quickly, without watching the full video. In less than a day, his feed was full of underage children, including many who were announcing their age on video as part of a

methods recently: in iOS 16, they added the ability to use a digital ID in Apple Wallet to verify age.⁹² This further reduces friction while keeping the age gating requirement intact.

112. On the Android/Google side, Family Link (officially launched 2017 after a pilot) allowed creation of Google Accounts for kids under 13, managed by the parent. The signup flow forces the parent to authenticate and then verify with a small credit card charge (typically \$0.30 in the U.S.).⁹³ Google explains this is required to comply with COPPA. After that, the child's account is marked as under 13 and has various protections (no targeted ads, SafeSearch on, Play Store restrictions, etc.).

113. In summary, mobile platform operators have for more than a decade treated age verification as a standard feature. They leveraged the same techniques available to everyone: credit cards, IDs, and trusted login flows. The fact that Apple and Google – two of the world's largest tech companies – implemented these measures demonstrates that these systems could have been deployed at scale by Meta, which is similarly large and technologically sophisticated. Unlike Meta, mobile platform operators prioritized building frameworks to differentiate adults and children and enforce appropriate policies. Social media platforms could have, and should have, done the same.

D. Summary

114. For over a decade, the social media industry's approach to age verification was a textbook example of too little, too late – and in truth, often nothing at all. Meta built digital playgrounds and invited the world, put up a token age limit sign, and then shrugged as elementary and middle-school children flooded in. It was a broken system that put the onus on kids to self-regulate and on parents to play catch-up, while the platforms themselves sat back and watched their user numbers climb.

⁹² This is mentioned in their support: you may use a driver's license in Wallet where available instead of a credit card. See <https://support.apple.com/en-us/111803>.

⁹³ Access Age-Restricted Content and Features, <https://support.google.com/accounts/answer/10071085>.

The undersigned hereby certifies their understanding that they owe a primary and overriding duty of candor and professional integrity to help the Court on matters within their expertise and in all submissions to, or testimony before, the Court. The undersigned further certifies that their report and opinions are not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation.

Dated: March 20, 2026



Timothy W. Estes