

Filed Under Seal

Exhibit A

**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

image, eating disorders, and self-harm, as well as structural changes to the brain. Because these platforms have massive user bases, these harms can affect millions (if not tens of millions) of kids every year.

31. These harms are most severe among kids who spend excessive time on Meta’s platforms – something the platforms are designed to encourage. Features like “infinite scroll,” autoplaying of videos, push notifications, ranking algorithms, gamification and ephemeral content all are designed to make the platforms more addictive.⁶

32. Meta’s testimony and internal documents demonstrate this. For example, Meta personnel discussed infinite scroll, autoplay and push notifications as part of its platforms’ “‘addictive’-like design” and “dark pattern.”⁷ (“Dark patterns are user interface elements that can influence a person’s behavior against their intentions or best interests.”⁸)

33. Sean Parker, one of the original developers of Facebook, has described how Meta and other platform developers use the addictive nature of these features to maximize time spent on the platforms (which in turn maximizes ad revenues):

The thought process that went into building these applications . . . was all about how we consume as much of your time and conscious intention as possible. And that means that we need to sort of give you a little dopamine hit every once in a while because someone liked or commented on a photo or a post or whatever. . . . [I]t’s exactly the kind of thing that a hacker like myself would come up with, because you’re exploring vulnerability in human psychology.⁹

34. Children are particularly susceptible to these tactics.¹⁰ Meta, for example, in an internal document about marketing to teens, explains some of the reasons why:

⁶ Surgeon General’s Advisory at 9.

⁷ META3047MDL-044-00108564 at -566; META3047MDL-003-00191207.

⁸ “A Comparative Study of Dark Patterns Across Mobile and Web Modalities” (Oct 2021), https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Gunawan-Pradeep-Choffnes-Hartzog-Wilson-A-Comparative-Study-of-Dark-Patterns-Across-Mobile-and-Web-Modalities.pdf.

⁹ Zuckerberg Dep. at 53:16-54:17 (quoting video recording of Sean Parker).

¹⁰ See, e.g., Surgeon General’s Advisory at 5 (“Because adolescence is a vulnerable period of brain development, social media exposure during this period warrants additional scrutiny.”).

Teen brains are much more sensitive to dopamine, one of the reasons that the risk of drug addiction is higher for adolescents and it's the same thing that keeps them scrolling and scrolling. Due to the immature brain, they have a much harder time stopping even though they want to – our own product foundation research has shown teens are unhappy with the amount of time they spend on our app.¹¹

35. Aside from addiction and mental health issues, the platforms present other significant risks to children as well. For example, they have become hunting grounds for predators seeking to sexually exploit children. Meta's platforms facilitate that in a number of ways, by (for example) recommending predators to children as potential friends, and by recommending children's accounts to adults – particularly adults who show an interest in that type of account – and then allowing those adults to directly message the children's accounts.¹² As a result, children frequently receive unwanted sexual messages from strangers on these platforms.¹³

36. For example, a survey conducted by Meta found that 13% of children aged 13 to 15 on Instagram reported unwanted sexual advances in just the last seven days.¹⁴ “Most teen girls disclosed receiving ‘creepy,’ ‘weird,’ ‘sexual,’ or ‘inappropriate’ comments or messages from unknown adult men.”¹⁵ Meta has estimated that, in English-speaking markets alone, more than 500,000 Instagram underage accounts receive inappropriate interactions from adults on a weekly basis.¹⁶

37. In more extreme cases, children on these platforms have been tricked into sending nude pictures to an adult stranger; nude pictures have been used by adults to blackmail children

¹¹ META3047MDL-003-00191207 at -215 (emphasis in original).

¹² See, e.g., META3047MDL-020-00271442 (“Our existing classifiers do not work great on short form virality that there is no current mitigation for in the Reels product roadmap – namely, predatory DMs from adults sent to minors who are more easily discovered via their Reels content.”); META3047MDL-014-00369785 at 2 (discussing how “bad actors can signal one another and look for and connect with kids and then enter a private messaging thread,” creating “one seamless flow of discovery-->connection--->harm.”).

¹³ See, e.g., META3047MDL-014-00046829 (“On IG there are 32X as many of these (messenger threads with sketchy adults) in the US than on FB”).

¹⁴ META3047MDL-004-00015029 at -033, -049.

¹⁵ META3047MDL-074-00164587 at 30-31.

¹⁶ META3047MDL-003-00028214 at -218.

(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.

verification fee, or a third party handles it for pennies). Even where the platform might pay a service fee, it's on the order of cents per user.

103. To put this in perspective, consider a credit card verification. As discussed, Nintendo and others charged \$0.50; Google charges \$0.30 for a parent verification on Family Link (to cover the payment processor fee) and then immediately refunds it.⁸⁵ In other words, Google spends a few dimes per new child user to ensure a parent is involved – and it still offers the Family Link service “completely free.” For a social platform, even if performing millions of verifications, this would only amount to a few million dollars in one-time processing costs. As noted above, Meta (Facebook/Instagram) had revenues of roughly \$117 billion in 2022. Even if verifying every single one of its ~3 billion users with a \$0.50 transaction were needed, that would be \$1.5 billion – about 1.3% of one year's revenue. In reality, the percentage would be far smaller, because not all users need credit card verification, and cheaper methods like AI age scans could be used for the majority.

104. Third-party verification services like IDWise advertise enterprise pricing of about \$1 per verification for robust ID checks. Volume discounts and simpler checks (like just age, not full identity) could drive this much lower. AI age estimation is even cheaper.

105. In summary, the direct costs of implementing real age checks is economically feasible for even the largest user bases. The costs per user range from a few cents to a few dollars at most, and those are one-time costs, not recurring. Against the backdrop of multi-billion-dollar revenues, this is a drop in the bucket.

106. The true cost to these platforms is the potential loss of revenue they earn from advertising to the millions of young children's accounts on their platforms.⁸⁶ Unlike direct costs

⁸⁵ Why Am I Prompted to Enter a Credit Card to Create a Nintendo Account for My Child?, https://en-americas-support.nintendo.com/app/answers/detail/a_id/1334/~/why-am-i-prompted-to-enter-a-credit-card-to-create-a-nintendo-account-for-my; <https://www.lifewire.com/how-to-use-google-family-link-4174557>.

⁸⁶ See, e.g., Social Media Platforms Generate Billions in Annual Ad Revenue From U.S. Youth, Harvard School of Public Health, (December 27, 2023) <https://hsph.harvard.edu/news/social-media-platforms-generate-billions-in-annual-ad-revenue-from-u-s-youth/>.

of verification, the loss of that revenue could significantly impact the companies' bottom lines. That, however, does not justify the unlawful and irresponsible targeting of young children with platforms known to be harmful to them.

C. Early Adopters: Age Verification in Gaming and Mobile Device Platforms

107. One of the strongest responses to the notion that “robust age verification wasn’t possible” is the fact that related industries already did it. From video game consoles to mobile operating systems, there are real-world case studies showing these methods in action – in some cases deployed by the same tech giants who failed to use them on their social media platforms. The following are some examples:

1. Video Games and Consoles - A Decade of Parental Gates

108. The gaming industry had to confront online child safety early, largely due to COPPA and the presence of voice/chat features in games. Microsoft, Nintendo, and Sony each implemented parental consent and age gates as they expanded their online services. Already mentioned above is Nintendo’s \$0.50 verification fee for child accounts on the Wii U in 2012. That system was straightforward and effective – no child under 13 could create an account without a parent’s involvement. Once the parent unlocked the first account with a credit card, additional child profiles could be managed with a PIN (recognizing that the adult had been verified already).

109. Microsoft’s Xbox Live similarly required that children (under 13) be added to an adult’s Microsoft Account family. As far back as the Xbox 360 era (late 2000s), Microsoft distinguished between “child accounts” and “parent accounts.” If a child tried to sign up, the system would prompt for an adult to sign in and approve. By 2012, Microsoft had an online mechanism where the adult would verify via a small credit card charge to confirm they were 18+. ⁸⁷ In June 2023, the FTC settled a case with Microsoft for failing in some aspects of COPPA

⁸⁷ See, e.g., Networking Your Xbox, Informit, (May 3, 2012) <https://www.informit.com/articles/article.aspx?p=1834696&seqNum=2>.

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