

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

obtain VPC have been feasible since at least 2010. Methods like credit card checks, secure login systems, and AI-based age estimation were available and proven. Companies in other industries, including video game platform developers and mobile device platform developers, have utilized age verification and parental consent for more than a decade.

6. In my expert report, I laid out numerous approaches that could have mitigated harms on Meta's platforms and that were feasible—in some cases for over a decade. Meta's experts do not meaningfully dispute that these approaches were available. Their criticisms, instead, boil down to three basic arguments: the approaches that I propose are not perfect; they would represent an inconvenience for Meta to deploy; and their social networking peers were not doing any better. Meta's experts imply that it is acceptable to create a considerable amount of harm to kids (measured in a population of tens of millions) to deliver a so called "better" and "more engaging" experience. In my opinion this collateral damage is both unnecessary and preventable.

7. In my opinion, Dr. Memon's claims regarding the infeasibility of age verification are incorrect and undermined by a decade of industry precedent. The factual record shows Meta's failure to implement robust age verification was not a technical limitation but a business and legal strategy to avoid "actual knowledge" of millions of underage users and thereby evade its COPPA obligations, a strategy that reached the highest levels of the company.¹ Furthermore, Dr. Memon's dismissal of AI-based facial age estimation as being in its "infancy" is directly contradicted by his own commercial enterprise.

II. Introduction

1. My name is Tim Estes. For over twenty years, I have developed and built critical software systems for high-stakes environments using cutting-edge technologies. I have applied these skills in a variety of contexts including, most pertinently, designing and building an online platform intended for children. I was asked by the Plaintiffs in this case to evaluate whether the Meta's social media platforms, as designed, were or are reasonably safe for children; to evaluate

¹ Davis Dep. Ex. 28A.

137. Dr. Memon's central defense of Meta's conduct is that it employed a reasonable "layered approach" to age verification, which he likens to the cybersecurity principle of "defense in depth".¹²¹ This analogy is fundamentally misapplied. A true defense-in-depth strategy relies on multiple, independently effective layers. Meta's system, by contrast, was a series of independently ineffective and permeable barriers, a fact confirmed by its own internal documentation.

i. A System Designed for Permeability Does Not Protect

138. An analysis of each of Meta's "layers," as described by Dr. Memon, reveals their inherent weaknesses when contrasted with the factual record described in my report and Meta's own documents:

139. **Layer 1: The Age Gate.** Dr. Memon presents the age gate at registration as the first layer of defense.¹²² However, as I state in my report, this is not a defense at all because it is trivially bypassed by any child willing to enter a false birthdate.¹²³ Meta's own registration flow documents show that if a user enters an underage birthdate, they receive a generic error and can simply go back and enter a different date.¹²⁴ This is not a controversial point; it is a self-attested failure. By 2011, it was documented that over 7 million children under 13 were on.¹²⁵ This initial failure, renders subsequent layers reactive rather than preventative.

140. **Layer 2: User Reporting.** Dr. Memon presents online reporting as a key vector for identifying underage users.¹²⁶ What he fails to mention is that, according to my review of the evidence, Meta's reporting system was designed with "friction" to "discourage reporting" in the first place.¹²⁷ Furthermore, Meta's own reporting forms from 2014 and 2015 state that if a "child's age can't reasonably be verified as under 13, then we may not be able to take action on the

¹²¹ Memon Report at pp. 26-29.

¹²² *Id.*

¹²³ Zuckerberg Dep. Ex. 65.

¹²⁴ META3047MDL-044-00108564.

¹²⁵ *Id.*

¹²⁶ Memon Report at pp. 32-33.

¹²⁷ Béjar Dep. 45:1-23.

account,” placing a high burden of proof on the reporter.¹²⁸ A system that is unreliable, intentionally difficult to use, and sets a high bar for action cannot be considered an effective security layer.

141. ***Layer 3: Manual and Automated Review.*** Dr. Memon describes Meta’s internal review processes as the next layer.¹²⁹ This final layer, however, is in effect a cleanup operation for a problem that should have been prevented proactively. Meta’s own “Age Misrepresentation Wiki” confirms this: “Currently we only reactively enroll underage users in our underage pipelines, this means that we do no proactive detection currently.”¹³⁰ The same document reveals that the automated systems ignore reports based on criteria like the account’s age or the output of an “adult classifier,” and that manual review for Facebook date-of-birth changes “does not currently use IDs to validate the age” but instead relies on looking at photos.¹³¹ These are not the hallmarks of a robust review system.

142. In sum, Meta’s “layered defense” was not a robust security architecture but a porous facade. The failure of the first layer was comprehensive, and the subsequent layers were inadequate and designed to be permeable. This structure allows the platform to benefit from the engagement of underage users, a practice consistent with Meta’s growth-at-all-costs business model and “don’t ask don’t tell” policy.

ii. Applying the Wrong “Industry Standard”

143. Dr. Memon repeatedly concludes that Meta’s practices “met or exceeded prevailing industry practice”.¹³² He arrives at this conclusion by narrowly defining the “industry” as only other social media platforms, many of which were similarly lax in their approach to child safety. This is a self-serving and inappropriate benchmark. In my opinion the relevant “industry” practices

¹²⁸ Jimenez Dep. Ex. 14.

¹²⁹ Memon Report at pp. 37-42.

¹³⁰ META3047MDL-146-00072824 at 25.

¹³¹ *Id.*

¹³² Memon Report at p. 7.