

Exhibit L

Confidential

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

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

THIS DOCUMENT RELATES TO:

ALL ACTIONS

MDL No. 3047

Case No. 4:22-03047-YGR

Judge: Hon. Yvonne Gonzalez Rogers

Magistrate Judge: Hon. Peter H. Kang

**REBUTTAL EXPERT REPORT OF DR.
NASIR MEMON**

Confidential

users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate.”¹¹

14. Based on information provided by Meta, my own independent analysis and observations, and my expertise in the subject matter, I conclude that Meta’s implementation of measures designed to prevent the use of Facebook and Instagram by children under 13 has been reasonable and has met or exceeded prevailing industry practice throughout the relevant period (2012 through 2024).¹² My opinions are based on the information available to me at the time I drafted this report. In the event that I receive new or conflicting information, I reserve the right to revise or supplement these opinions.

15. **Opinion 1:** Like in the broader field of security, where a strong cybersecurity program depends on a layered approach to safeguard information and systems, no single age verification approach online is sufficient, standing alone. As a result, age verification online necessitates a layered approach. Meta uses such a layered approach, relying on a combination of user reporting, date of birth changes, cross-platform checks, content reviews, checkpointing, and appeals. **Opinion 2:** While Plaintiffs’ experts claim that Meta’s age verification practices are ineffective due to the presence of underage users on Meta’s platforms, Meta’s practices met or exceeded industry practices during the relevant period. **Opinion 3:** Further, Plaintiffs’ experts’ specific criticisms of Meta’s implementation of its neutral age gate and user reporting system are misguided and fail to account for the overall system design, which relies upon layered defenses to prevent, identify, and remove underage users while balancing privacy needs, regulatory limitations, and the technology available for age verification.

¹¹ See <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

¹² The opinions offered in this report relate to Plaintiffs’ School District Complaint, Personal Injury Complaint, and Attorney Generals’ Complaint.

Confidential

IV. BACKGROUND ON AGE VERIFICATION

A. The Challenges of Online Age Verification

16. Age verification is utilized across a wide variety of both online and offline scenarios. While age verification in general presents challenges, age verification online is both notoriously difficult and increasingly complex.

17. Offline and in-person age verification arises in contexts such as purchases of age-restricted products and access control at events or venues. In general, in this context, the individual who purports to be a certain age presents their actual person to the system or employee conducting age verification. In many instances, offline checks rely heavily on human judgment and the ability of an individual to analyze the accuracy of identification documents, compare an individual against prior images, and assess truthfulness. While in-person age verification has its own challenges and is vulnerable to fake IDs or impersonation if staff are not properly trained (*e.g.*, an underage patron who successfully uses a sibling's ID to enter an age-restricted establishment), the presence of a single point of verification, and often a human interface, makes in-person age verification relatively straightforward.

18. Age verification is more challenging in the far broader set of circumstances and platforms where it is needed online. (Scheffler, 2024). These use cases vary widely in risk, regulatory requirements, and user expectations, such that no universal solution exists. Effective approaches must be context-sensitive and proportional to the sensitivity of the access being gated.

19. At the heart of the difficulty with online age verification lie several intersecting challenges: limitations of technology, regulatory compliance, privacy concerns, and critically, scalability. What form age verification should take may vary

Confidential

widely depending on the context, with particular attention to the potential risk posed to a child or teenager by the ability to access a particular platform or resource. (IEEE, 2024).

20. In a low-risk context, such as visiting the website of an alcohol company, simple self-declaration in the form of an attestation that an individual is 21 years or older may be sufficient (because no alcohol can be obtained without further verification). By contrast, high-risk services that necessitate stringent age gates—like online gambling—may require more robust age verification mechanisms, such as government ID verification, because access to the platform itself may expose the individual to age-inappropriate options or content. However, increasing the strength of verification often raises usability barriers and introduces privacy risks, especially when biometric data or sensitive identity information is collected. Complex verification methods may be challenging for less technologically savvy or older individuals to follow, resulting in increased friction and legitimate adult user drop-off. As discussed in more detail below, individuals of all ages (and especially individuals between 13 and 17 years old) may lack access to sufficient documentation, leading to digital accessibility issues, and even if they have such documentation, individuals may not wish to share biometric data, sensitive identity documentation, or financial information online, given growing privacy and cybersecurity concerns.

21. In terms of security, while online systems can integrate more sophisticated tools like biometric verification,¹³ liveness detection,¹⁴ or database lookups against government-issued IDs (Jain et al., 2011), online age verification mechanisms may

¹³ Biometric verification describes a method to prove identity online by using something unique about the user's body—like their face or voice. For example, the user might take a selfie or speak into their phone, and the system checks if it matches a photo or voice it already has on file. (Jain et al., 2011).

¹⁴ Liveness detection refers to a technology that verifies the authenticity of biometric data by ensuring that it came from a living human, rather than a photograph, or other manipulated media. In doing so, it prevents attacks from malicious actors who intend to misuse biometric data for their own benefit. (Jain et al., 2011).

Confidential

since at least 2012. (META3047MDL-037-00118789). While Instagram has been restricted to users over 13 throughout the relevant period (META3047MDL- 208-00003308), it started to age gate the service in December 2019, when it began collecting user age for the first time. (META3047MDL-012-00000001; META3047MDL- 022-00008803).

66. Since both platforms started age gating, all individuals who create an account on Facebook or Instagram are required to enter their date of birth as part of a multi-step registration flow. (META3047MDL-053-00012657; META3047MDL-190-00000001). The date-of-birth screens are presented neutrally and without a pre-populated date of birth that would meet the minimum age requirement.⁴² One of Plaintiffs' experts, Dr. Gray, claims that the "scrolling date picker" format of the neutral age gate constitutes a dark pattern because it does not contain "contextual warnings or validations."⁴³ This criticism overlooks that the absence of contextual warnings is core to the concept of a neutral age gate, contravening the intent of the design where individuals input a date of birth without any indication of the applicable minimum age threshold for account creation. (META3047MDL-053-00012657).

67. If an individual enters a date of birth reflecting an age under 13, Meta prevents the individual from creating an account. For individuals who attempt to enter an age between 5 and 12, after two consecutive attempts, the individual will be prevented from creating an account and locked out of the registration process for a period of 12 hours. (META3047MDL-053-00012657). Originally, this restriction was session-based only; in 2022, Meta improved the "cooldown" period to persist across mobile application restarts on the same device, making it more difficult for determined underage individuals who

⁴² Note that between 2017 and 2020, the age gate on Facebook displayed, as a default, a birth date reflecting an age of 25. Nonetheless, during this period, the age gate still did not indicate the minimum age required for registration. (META3047MDL-040-00335514; META3047MDL-047-00016158).

⁴³ Gray ¶88.

Confidential

sought to bypass the restriction by closing and reopening the mobile application. (META3047MDL-019-00129336). Gray also takes issue with the fact that Meta gives individuals a second chance to create an account if the individuals at first input a date of birth reflecting an age below 13.⁴⁴ Individuals who attempt to enter an age between 5 and 12 are prevented from creating an account and locked out of the registration process for 12 hours after two consecutive attempts. (META3047MDL-053-00012657). Meta's decision to allow individuals to make a second attempt when they enter a date of birth indicating an age under 13 is reasonable because individuals may input a date of birth in error in light of the design of the neutral age gate (discussed above), for example, by scrolling the "year" selector too quickly or by accidentally submitting the form before they were done selecting the correct date.

68. Critically, individuals who enter a date of birth indicating they are under the age of 13 receive a generic error message informing them that they cannot create an account, without specifying the age threshold that the individual failed to meet, thus avoiding coaching or circumvention. Gray notes that when an individual attempts to create an account with an age below the threshold, the interface presents a generic error message, then allows the individual to subsequently adjust their birthdate.⁴⁵ However, this explanation overlooks that the error message is generic, which prevents the individual from knowing which aspect of their registration caused the account-creation failure, ensuring that the individual is not encouraged to re-attempt with a different date of birth.

69. As discussed in Section V, Plaintiffs' experts criticize Meta for not requiring further age verification, such as an ID or credit card check, at account registration

⁴⁴ Gray ¶85.

⁴⁵ Gray ¶85.

Confidential

for Instagram or Facebook.⁴⁶ Specifically, Gray states that Meta’s account registration flow “lacks meaningful friction when verifying a prospective user’s age.”⁴⁷ This criticism fails to consider the many challenges, discussed in detail above, inherent to requiring verification via methods like government ID or biometrics at the point of registration. As discussed above, there is no one-size-fits-all answer to the multidimensional problem posed by online age verification. Effective solutions must navigate the trade-offs between privacy, regulatory compliance, usability, accuracy, and scalability. Balancing the likely efficacy of identification-based and biometric verification against the drawbacks and risks identified above, Meta’s collection of date of birth information as the first step of a layered approach is reasonable in light of the need for low-friction onboarding, the importance of accessibility, and the avoidance of early privacy intrusions, especially across a global, diverse user base, when considered as part of its broader approach to age verification.

E. Identification of Potential U13 Users

70. Building on the foundation of age gating, the next layer of Meta’s age verification process focuses on identifying users who may be under 13 on its services. Meta employs a well-reasoned, multi-channel framework to identify and remove users who may be under 13 who are already on the platform, and Meta is constantly evolving its systems and technology.⁴⁸ The vectors Meta uses to monitor existing accounts for potential underage users include online reporting, internal reviews, user self-reporting, and cross-platform checks. (META3047MDL-012-00000001).

⁴⁶ Estes ¶190.

⁴⁷ Gray ¶84.

⁴⁸ Rothschild Dep. Tr. at 140:15-141:15 (Jan. 21, 2025); *see also* Hartnett Dep. Tr. at 130:15-25 (June 16, 2025).

Confidential

1. Online Reporting

71. Both Facebook and Instagram offer webforms (and related publicly accessible instructions) that allow anyone using a web browser, regardless of whether they use any of Meta's services, to report a potentially underage account to Meta. (META3047MDL-040-00000322; META3047MDL-040-00000323). Plaintiffs' experts take issue with the fact that, during parts of the relevant period, user reporting was not available inside the four corners of the Facebook or Instagram app.⁴⁹ This criticism overlooks that the publicly accessible webforms were nonetheless available, providing the broadest possible set of individuals—anyone with access to the internet—the ability to report potential underage users. This broad access has allowed individuals like parents, guardians, and teachers to make these reports since at least 2013 (for Instagram) or 2012 (for Facebook).⁵⁰ (META3047MDL-012-00000096; META3047MDL-012-00000001; META3047MDL-040-00000327; META3047MDL-208-00003306; META3047MDL-208-00003307). On both Facebook and Instagram, users can also access these reporting forms via an in-app browser, directly from the mobile applications. (META3047MDL-053-00012657).⁵¹

72. Notably, online reporting forms of this kind are vulnerable to abuse and harassment, and a large number of underage reports are false; that is, the user is found to be 13 or older upon checkpoint or appeal.⁵² For example, individuals can report others' accounts as underage or as spam accounts as methods of online harassment or cyberbullying.⁵³ Further, because platforms like Meta want to encourage reporting of problematic or violative content or accounts, these reporting mechanisms often do not

⁴⁹ Gray ¶90; Drumwright ¶340.

⁵⁰ Hartnett Dep. Tr. at 119:19-120:4 (June 16, 2025).

⁵¹ Hartnett Dep. Tr. at 136:1-137:5 (June 16, 2025).

⁵² Hartnett Dep. Tr. at 210:2-19 (June 16, 2025).

⁵³ Hartnett Dep. Tr. at 245:24-246:7 (June 16, 2025).

Confidential

require verification and can easily be falsified. The underage review flow is particularly vulnerable to abuse because bad actors understand that this flow may result in the reported account being taken down entirely (where reporting specific pieces of content may not). Internal reports at Meta indicate that there are a significant number of underage reports filed that are obvious harassment, such as over 1 million reports of the Israeli Defense Force, as well as inauthentic reports of adult public figures such as Emmanuel Macron and Kim Kardashian, who were reported thousands of times. (META3047MDL-208-00003249).⁵⁴ Accordingly, Meta has implemented evaluation and review processes, described in further detail below, to conduct diligence of accounts reported by third parties to be underage. Meta's choice not to offer "one-touch" in-app reporting is reasonable in light of the history of, and potential for, abuse. This is supported by the fact that a small-scale test of such in-app reporting on Instagram resulted in double the number of false underage reports submitted.⁵⁵

73. Plaintiffs' experts also express concern about the friction involved in the user reporting form, noting that the report involves "7 screens" to complete.⁵⁶ This criticism is also misguided. These screens are designed to guide the reporter through the process, and request information to assist Meta in determining the identity of the user and whether the user may be underage. (META3047MDL-037-00088546; META3047MDL- 037-00088547). This flow is particularly reasonable in light of the impact of the action being requested (*i.e.*, where Meta may checkpoint the user's account, requiring identification to regain access).⁵⁷ Rate-limiting applied to these screens further helps to protect the integrity

⁵⁴ See also Hartnett Dep. Tr. at 210:7-19; 246:11-18 (June 16, 2025).

⁵⁵ Hartnett Dep. Tr. at 145:9-14 (June 16, 2025).

⁵⁶ Gray ¶90; Drumwright ¶340.

⁵⁷ Hartnett Dep. Tr. at 336:1-337:1 (June 17, 2025).

Confidential

of the reporting form against malicious actors who might misuse the reporting form.⁵⁸ Gray also criticizes the specific fields in the form, alleging that the form requests “username, full name, and birthdate” of the individual being reported.⁵⁹ This is not only inaccurate (the form does not require a full birthdate), but fails to consider that requesting this information likewise helps to prevent abuse of the form by substantiating the reporter’s knowledge of the user. (META3047MDL-040-00000321; META3047MDL-040-00000327).⁶⁰

2. Internal Reviews

74. Meta trains thousands of human reviewers to review accounts that are reported by other users for potential violations of the Facebook or Instagram Terms of Service, as well as content guidelines unrelated to age. When reviewing accounts in response to any type of report, reviewers are instructed to proactively monitor for details suggesting that the user may be a child under 13 (for example, photos posted to the account reflecting age or text in the account bio stating an age under 13). (META3047MDL-012-00000001; META3047MDL-040-00000365). In the event that details suggesting the user is under the age of 13 are present, the reviewer will escalate the account for underage review. Meta may also identify potential underage users through other review processes including, for example, where Meta requires users to provide identification to access certain features, *e.g.*, Meta Verified. (META3047MDL-012- 00000001; META3047MDL-040-00000365).

⁵⁸ Hartnett Dep. Tr. at 245:18-246:7 (June 16, 2025) (Confirming that Meta’s underage reporting form has been the subject of scripting attacks and inauthentic reports of child users, by malicious actors).

⁵⁹ Gray ¶89.

⁶⁰ See also Hartnett Dep. Tr. at 120:2-19; 245:18- 246:16 (June 16, 2025).

Confidential

other means, including self-reporting. (FTC Report, 2024). This supports that it was not industry practice to leverage age prediction models for age verification during the relevant period. In the same FTC Report, the FTC underscored how the surveyed companies did not have a full understanding of AI and did not have safeguards in place to provide users with recourse for AI-based decisions, such as account removal, in the event that results were inaccurate, unreliable, or biased. (*Id.* at 60). These issues further explain why the use of such models was not standard industry practice during the relevant period.

VII. ANALYSIS

88. Age verification is a long-standing challenge on the internet. Traditional methods—like self-declared age, credit card checks, and document-based verification—have proven inadequate, standing alone, because they can be easily bypassed, fail to reflect the realities of youth digital behavior, and exclude legitimate users without formal credentials. While methods like third-party verification, facial age estimation and device or IP inference began to emerge during the relevant period, they remain limited in adoption, accuracy, fairness, and reliability when applied in real-world conditions.

89. Plaintiffs’ experts’ critique that self-reporting of age at registration is “imperfect”⁶⁸ overlooks the profound technical, operational, and privacy challenges associated with alternative approaches. Given these constraints, a layered approach to age verification—beginning with self-declared age during registration, and continuing through the user experience through proactive monitoring, user reporting channels, cross-platform reconciliation, and escalation to stronger verification measures when concerns arise—is not only reasonable, but preferable. It strikes a necessary balance between safeguarding

⁶⁸ See Chandler ¶167.

Confidential

children, respecting user privacy, maintaining platform accessibility, and ensuring operational scalability across a global user base.

90. Within this technological and societal landscape, Meta uses exactly that kind of layered, escalated, and user-transparent enforcement approach—seeking to balance privacy, safety, and fairness to users. While Plaintiffs’ experts criticize certain aspects of Meta’s layered approach to age verification, these criticisms overlook that age verification is a multi-faceted challenge, and effective solutions must balance considerations like privacy, regulatory compliance, usability, accuracy, and scalability.

91. The system begins with lower-friction methods appropriate for a low-stakes context—such as behavioral signals or user-declared information—to prohibit the creation of potential underage accounts without requiring sensitive data from most users. In cases where there are indicia that a user is underage, Meta checkpoints the account and escalates to the next layer of age verification through document-based review. This method of age verification has typically been used in isolation for higher-stakes contexts, such as gambling or adult websites. Importantly, throughout Meta’s age verification process, users are offered choices where possible and are informed about what data is being collected and how it will be used. This structure allows Meta to apply stronger measures only when warranted, aiming to limit unnecessary data collection while addressing safety concerns. Overall, the approach reflects an effort to navigate the trade-offs involved in age verification in a way that is consistent with evolving expectations around transparency and proportionality.

92. Importantly, such an approach was fully consistent with prevailing industry norms during the relevant period (2012-2024), a period of significant technological and societal change. Plaintiffs’ experts contend that Meta could have implemented other means of age verification, such as credit card and payment verification,

Confidential

document-based verification, third-party verification, face-based age prediction, or device or IP inference. However, as discussed above and as acknowledged by Plaintiffs' expert Tim Estes,⁶⁹ these methods each fall short in the context of Meta's diverse global user base. Further, these methods were not standard industry practice for age verification during the relevant period.

93. As confirmed by independent studies (*e.g.*, Pasquale et al., 2020) and regulatory surveys (*e.g.*, FTC SMVSS Report, 2024), major social media platforms overwhelmingly relied on self-declared age during registration and reserved higher-friction verification only for cases of suspected noncompliance. Some social media companies even only contractually prohibited children from creating accounts, such that there was no actual mechanism to identify whether a child was using that website or mechanism to stop a child from creating an account.

94. In contrast, Meta's adoption of layered safeguards and rigorous manual review protocols places it ahead of most peers during the timeframe in question. Meta's implementation of multiple channels used to proactively monitor for and identify potential underage accounts, as well as its scalable automated and manual review processes, go beyond many peer platforms' practices by conducting age verification throughout a user's interaction with the service. Meta's strategy also appropriately reflects technological evolution and social expectations by adopting a risk-based model that recognizes legitimate privacy concerns by minimizing data collection at the earliest point of interaction and ensuring deletion of sensitive data after use.

⁶⁹ Estes ¶¶227, 233, 237, 241, 246.

Confidential

VIII. CONCLUSION

95. In sum, Plaintiffs' experts' opinions are flawed and do not alter my conclusion that Meta's layered, scalable, privacy-respecting approach to age verification is not only reasonable in the context of the technology and regulatory landscape, but also equals or goes beyond that of other global platforms during the relevant period. These conclusions are informed by my technical expertise in biometrics, cybersecurity, and platform security, my current research and publications relevant to age verification issues, and by a comprehensive evaluation of Meta's processes against key industry benchmarks.