

Exhibit K

Expert Report – Highly Confidential

**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, and Instagram,
LLC,
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 RYAN SHEATSLEY
MARCH 20, 2026**

Expert Report – Highly Confidential

TABLE OF CONTENTS

1 SUMMARY OF OPINIONS1

1.1 Opinion 1 – Meta’s Underage Reporting and Enforcement Data Show Hundreds of Thousands of Reports About Underage US Users and Checkpointing Over a Million Such Users; State-Level Geographic Information Is Missing for Most of These Users1

1.2 Opinion 2 – Expanding Meta’s Shortened Underage Reporting Flow Will Likely Lead To an Increase In The Number Of Detected Underage Users.....1

1.3 Opinion 3 – Meta’s Automations Ignore Many Underage Reports2

1.4 Opinion 4 – Meta’s Instruction To Ignore Reports Where Less Than 50% of Photos On The User’s Profile Were Of Children Had a Large Impact.....3

1.5 Opinion 5 –Many Reports Were Not Reviewed For Months And Reviewers Spent Less Than 30 Seconds Reviewing Most Reports3

1.6 Opinion 6 – Meta’s Underage Detection System Most Often Disables Users Who Admit They Are Underage; Third-Party Verification Services And Internal Review Result In Fewer Checkpoints.....4

1.7 Opinion 7 – Users Who Are Checkpointed For Being Underage Can Remain In Checkpoints For Over a Year.....4

1.8 Opinion 8 – Many Underage Users Could Have Been Removed From Meta’s Platforms Via Hard-Linking and Soft-Matching5

2 INTRODUCTION6

2.1 Qualifications and Experience6

2.2 Statement of Compensation8

2.3 Assignment.....9

3 TECHNICAL BACKGROUND.....10

3.2 Online Platforms.....10

3.3 Account Management.....11

3.4 Computer Security Fundamentals12

3.5 Understanding Under-13 Use of Meta Platforms.....14

4 META’S DETECTION AND MANAGEMENT OF UNDERAGE ACCOUNTS19

4.2 Age Detection on Meta’s Platforms19

Expert Report – Highly Confidential

4.3 An Overview of Meta’s Under 13 Reporting Tool and Flow.....24

5 ANALYSIS OF META LOG DATA.....41

5.2 Meta’s Logging Data Productions.....42

5.3 Field Descriptions.....44

5.4 Analysis Overview47

5.5 Analysis Methodology48

APPENDIX A. CURRICULUM VITAE AND PRIOR TESTIMONY
WITHIN FOUR YEARS

APPENDIX B. MATERIALS CONSIDERED

Expert Report – Highly Confidential

1 SUMMARY OF OPINIONS

1.1 OPINION 1 – META’S UNDERAGE REPORTING AND ENFORCEMENT DATA SHOW HUNDREDS OF THOUSANDS OF REPORTS ABOUT UNDERAGE US USERS AND CHECKPOINTING OVER A MILLION SUCH USERS; STATE-LEVEL GEOGRAPHIC INFORMATION IS MISSING FOR MOST OF THESE USERS

1. My analysis of Meta’s underage reporting and enforcement data shows that Meta has received hundreds of thousands of reports about underage users in the US and has checkpointed and ultimately disabled the accounts of more than a million users in the US for being underage over the time periods covered by Meta’s data productions. However, Meta’s data productions lack state-level geographic information for the majority these users. For example, as detailed below, Meta’s data productions contain roughly 700,000-2,300,000 reports about underage US users. Of these reports, roughly 200,000 of them contain state-level geographic information about the users.

1.2 OPINION 2 – EXPANDING META’S SHORTENED UNDERAGE REPORTING FLOW WILL LIKELY LEAD TO AN INCREASE IN THE NUMBER OF DETECTED UNDERAGE USERS

2. Meta’s data productions showed many reports that are sourced by the Shortened Underage Reporting Flow (“SURF”) result in checkpointed users. Despite SURF being rolled out to a small percentage of users, the number of reports from SURF are roughly the same from the underage contact form, indicating SURF creates a much higher reporting rate than the contact form. My analyses show comparable checkpointing rates for reports submitted via

Expert Report – Highly Confidential

SURF versus contact forms, and therefore increasing the SURF deployment from the currently small percentage of users will likely increase the number of detected underage users.

1.3 OPINION 3 – META’S AUTOMATIONS IGNORE MANY UNDERAGE REPORTS

3. Meta’s underage automations, which are mechanisms designed to automatically filter reports, ignore many underage reports. One of these automations ignores reports of underage users not because Meta has any indication that the user is not under 13, but because the reported account does not have the two pieces of information that are used by Meta’s human reviewers to determine whether or not to checkpoint the reported accounts (an account bio or photos). My analyses showed that roughly 40,000 reports about underage users were ignored because the profile did not have a bio or photos. Another automation ignores reports about accounts predicted by Meta’s machine learning model to belong to users 18 or older. Using this classifier to ignore underage reports is not reliable; among other issues, the classifier was trained to predict users in one of two categories (ages 13-17 or 18+), but was not designed or intended to detect users under the age of 13. My analysis showed that Meta ignored approximately 164,000 reports about underage users because the user was predicted to be 18 or older via Meta’s machine learning models.

Expert Report – Highly Confidential

1.4 OPINION 4 – META’S INSTRUCTION TO IGNORE REPORTS WHERE LESS THAN 50% OF PHOTOS ON THE USER’S PROFILE WERE OF CHILDREN HAD A LARGE IMPACT

4. Meta’s human review process contains a decision tree that instructs reviewers to analyze the pictures of a user’s profile. As part of that instruction, reviewers were instructed to ignore reports where less than 50% of the photos on the user’s profile were of the same child. My analysis of Meta’s data productions shows that there were roughly 13,000 reports where the reviewer found photographs of children but still ignored a report because of this instruction. Moreover, I found up to 2,000 of the users in these reports were eventually checkpointed for being underage through other means.

1.5 OPINION 5 –MANY REPORTS WERE NOT REVIEWED FOR MONTHS AND REVIEWERS SPENT LESS THAN 30 SECONDS REVIEWING MOST REPORTS

5. My analysis of Meta’s data productions shows tens of thousands of reports that took over a month for human reviewers to review. Specifically, 710,050 reports were reviewed within 2 days, 64,855 reports were reviewed within 3 days to 1 week, 69,577 reports were reviewed within 1 week to a month, and 51,160 reports took longer than 1 month to be reviewed. Moreover, my analysis shows that approximately 44% of all human-reviewed underage reports are processed in under 10 seconds, and roughly 67% are completed in under 30 seconds.

Expert Report – Highly Confidential

1.6 OPINION 6 – META’S UNDERAGE DETECTION SYSTEM MOST OFTEN DISABLES USERS WHO ADMIT THEY ARE UNDERAGE; THIRD-PARTY VERIFICATION SERVICES AND INTERNAL REVIEW RESULT IN FEWER CHECKPOINTS

6. My analysis of Meta’s data productions shows that the majority of accounts that are checkpointed or enforced against are due to users who admit they are under 13 by changing their date of birth on their account—the top five reasons why users are checkpointed all describe such scenarios (whose collective frequency constituted 1.7 million underage checkpoints). Further analysis shows that 80% of these users who are checkpointed for these reasons end up having their accounts disabled (corresponding to 800,000 users). Correspondingly, third-party age verification services such as Yoti rarely result in checkpointing users for being underage (as only 3,100 checkpoints were due to age verification services), reflecting that Yoti is only used in narrow contexts rather than as part of Meta’s core under-13 detection workflow. Moreover, the data productions show around 13,000 checkpoints come from Meta’s internal review program, which is comparable with the number of third-party reports that result in checkpoints.

1.7 OPINION 7 – USERS WHO ARE CHECKPOINTED FOR BEING UNDERAGE CAN REMAIN IN CHECKPOINTS FOR OVER A YEAR

7. My analysis of Meta’s data productions shows that users who have been checkpointed for being underage can remain in the checkpointing process for

Expert Report – Highly Confidential

various periods of time. Eighty percent (1,180,858) of checkpoints reach a decision within 45 days, 16% within 46 days to 6 months, 0.5% within 6 months to a year, and 3% (44,289) take longer than 1 year. During this time, the data corresponding to these users can be used by Meta for business purposes, such as improving its AI models. Moreover, my analysis shows the impact of various retention policies Meta has used, where Meta held the data of hundreds of thousands of accounts that were disabled for being underage for six months to a year before the deletion process was initiated.

1.8 OPINION 8 – MANY UNDERAGE USERS COULD HAVE BEEN REMOVED FROM META’S PLATFORMS VIA HARD-LINKING AND SOFT-MATCHING

8. Analysis of Meta’s data productions show that greater than 300,000 enforcements are due to hard-linking (where users explicitly link their accounts through Account Centre). Within the periods covered by data provided, I estimate that up to 100,000 additional accounts would have been removed due to propagation of enforcements via hard-linking if Meta’s hard-link propagation system would have been implemented/fixed in the past. Moreover, my analysis of Meta’s soft-match data (which describes the likelihood that two accounts are owned by the same user) provides estimates that Meta could have disabled tens of thousands of additional underage accounts on Facebook and Instagram that were soft-matched to accounts that were disabled for being underage. Over a 90-day period, I found tens of

Expert Report – Highly Confidential

thousands of accounts that were soft-matched to accounts that were disabled for being underage. While Meta does not use soft-matching to disable underage accounts, Meta has been using soft-matching for disabling accounts for other types of policy violations, as well as using soft-matching for other commercial purposes, for years.

2 INTRODUCTION

2.1 QUALIFICATIONS AND EXPERIENCE

9. My relevant qualifications are summarized here and provided in more detail in my curriculum vitae, which is attached as **Appendix A** to this report. This appendix also includes a list of my publications in the past ten years.
10. I earned a Ph.D. in Computer Sciences from the Department of Computer Sciences at the University of Wisconsin, Madison in 2024. I earned a Master of Science degree in Computer Science and Engineering and a Bachelor of Science degree in Computer Engineering from the Pennsylvania State University in 2018 and 2015, respectively.
11. From 2014-2018, I spent my summers as a research scientist for the United States Army Research Laboratory (ARL) in the Tactical Network Assurance Branch. My responsibilities at ARL included performing fundamental research on the security of computer networks and serving as team lead on associated projects.

Expert Report – Highly Confidential

20. This report presents the same data analyses and conclusions set forth in the portions of the reports originally prepared by Dr. Patrick McDaniel in which I was directly involved. Specifically, this report addresses the data analytics material contained in Section 5. I conducted the data analysis reflected in those sections, participated in developing the analytical approach, and implemented the methodology in code. I also assisted in drafting Sections 3 and 4. The data analyses and results are replicated without modification (except as otherwise noted), and the opinions expressed in this report reflect my own knowledge, work, and independent review of those analyses.

3 TECHNICAL BACKGROUND

21. This section outlines the technical foundation for my findings, emphasizing what online platforms are, how accounts are managed at scale, and computer security fundamentals. I define and explain how large-scale digital platforms have evolved over time; security mechanisms for account management; and threat modeling in the context of underage users on Meta's platforms.

3.2 ONLINE PLATFORMS

22. Online platforms (often referred to as digital platforms), are large-scale digital services that provide account-based access to, for example, social, communication, commercial, or content-driven functionality over the Internet. These include platforms such as social networks, messaging