

EXHIBIT 79

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, Instagram, LLC,
Meta Payments, Inc., Meta Platforms
Technologies, LLC., 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 PATRICK MCDANIEL
NOVEMBER 21, 2025**

Expert Report – Highly Confidential

79. Another 2024 report by the Federal Trade Commission⁹⁵ similarly concluded that current social media and Video Streaming Services (including Facebook⁹⁶) collects sufficient behavioral and technical data to infer when a user is likely under 13 yet has not consistently used that data to prevent or remove underage accounts. The report concluded in its summary of observations that “SMVSSs⁹⁷ bury their heads in the sand when it comes to Children using their services. Most SMVSSs suggested that, because they were not directed to children and did not allow Children to create accounts, there were no Child users. This is not credible. It is well known that Children are using SMVSSs.”⁹⁸
80. As yet another example, a 2025 national study published in the Journal of Adolescent Health⁹⁹ further confirmed that Instagram is one of the most commonly used platforms among U.S. children under age 13, “Among

⁹⁵ Federal Trade Commission, *A Look Behind the Screens Examining the Data Practices of Social Media and Video Streaming Services*, FTC (Sept. 2024), <https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services>.

⁹⁶ Id. at 9. Facebook was specifically called out as one of the platforms within the scope of the report, “Meta Platforms, Inc., formerly known as Facebook, Inc., operates multiple SMVSSs. In 2023, Meta reported having 3 billion users across its services.”

⁹⁷ Social Media and Video Streaming Services, which is defined as “any product or service that allows users to create and share content with other users (whether a private or group interaction) through an application or website on any device (e.g., personal computer, iOS device, Android device, etc.), or stream video, Including, but not limited to, any social networking service, messaging service, video streaming service, or photo, video, or other content sharing application, whether offered for a fee or for free.” Federal Trade Commission, 6(B) SMVSS STUDY SAMPLE ORDER (2020), Definition II, https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-service-providers/6bs_order_os_final.pdf.

⁹⁸ Federal Trade Commission, *A Look Behind the Screens Examining the Data Practices of Social Media and Video Streaming Services*, FTC (Sept. 2024), <https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services>.

⁹⁹ *Prevalence and Patterns of Social Media Use in Early Adolescents*, Academic Pediatrics (May-June 2024) <https://www.academicpediatricsjournal.net/action/showPdf?pii=S1876-2859%2825%2900009-9>.

Expert Report – Highly Confidential

adolescents under 13 with social media accounts, TikTok (68.2%), YouTube (62.9%), Instagram (57.3%), and Snapchat (55.2%) were the most common.”¹⁰⁰ Participants reported maintaining multiple accounts per person, including “secret” accounts actively concealed from parents or guardians, and described entering a different birthdate when prompted with Meta’s age warning during signup. The study made clear that this pattern of underage access was widespread and easily achieved and not limited to fringe or accidental cases.

81. Studies of underage use of Facebook have been consistent in finding that underage users are on the platform. For example, nationally representative surveys conducted by the nonprofit child-safety organization Thorn show that significant numbers of U.S. children ages 9–12 use Facebook despite being under Meta’s stated minimum age.^{101, 102} Thorn’s 2022 and 2023 Youth Monitoring surveys were based on structured, probability-based samples of U.S. households with children in this age range. Respondents completed anonymous, self-reported questionnaires designed to measure digital platform use among tweens. Across both years, the results were consistent: 53% (2022)

¹⁰⁰ Id. at 5.

¹⁰¹ Neiswnder, C. et. al., Youth Perspectives on Online Safety, 2022: an Annual Report of Youth Attitudes and Experiences, Thorn (Nov. 2023), https://info.thorn.org/hubfs/Research/22_YouthMonitoring_Report.pdf;

¹⁰² Neiswnder, C. et. al., Youth Perspectives on Online Safety, 2023, Thorn (Aug. 2024), https://info.thorn.org/hubfs/Research/Thorn_23_YouthMonitoring_Report.pdf.

Expert Report – Highly Confidential

and 59% (2023) of 9–12-year-olds reported having used Facebook at least once, and 29% (2022) and 35% (2023) percent reported daily use. Meta has likewise documented that children were likely on the platform. In September 2020, an internal Meta study stated that 9% of 6-to-9 year olds and 10% of 10-to-13 year olds believed most children their age use Facebook.¹⁰³ An internal Meta study a month later then noted 31% of 6-to-9 year olds and 44% of 10-to-12 year olds reported using Facebook in the last month, and 22% of 6-to-9 year olds and 30% of 10-to-12 year olds reported that most of their friends were on it.¹⁰⁴ In 2021, an internal Meta study stated that in 2018 34% of 8- to 10-year-olds had used Facebook in the past month, along with 22% of 5- to 7-year-olds.¹⁰⁵

82. A similar pattern appears on Instagram. Survey research across 2022–2023 shows that large numbers of U.S. tweens actively use the service: 29% (2022) and 26% (2023) of 9–12-year-olds reported daily use, and 51% (2022) and 50% (2023) reported having used Instagram at least once.¹⁰⁶ Earlier census-style youth-media studies also identified significant tween usage, with 10%

¹⁰³ META3047MDL-003-00031411.

¹⁰⁴ META3047MDL-003-00124191; META3047MDL-003-00124207.

¹⁰⁵ META3047MDL-003-00016725.

¹⁰⁶ Neiswnder, C. et. al., Youth Perspectives on Online Safety, 2022: an Annual Report of Youth Attitudes and Experiences, Thorn (Nov. 2023), https://info.thorn.org/hubfs/Research/22_YouthMonitoring_Report.pdf; Neiswnder, C. et. al., Youth Perspectives on Online Safety, Thorn (Aug. 2024), https://info.thorn.org/hubfs/Research/Thorn_23_YouthMonitoring_Report.pdf.

Expert Report – Highly Confidential

of tweens reporting daily Instagram use in 2021.¹⁰⁷ Meta also documented that children were likely on Instagram. One 2017 Meta survey states that as “age increases [for] (5-to-12-year-olds), so does the self-reported proportion of U13 year olds with FB and IG accounts (~5-30%)”.¹⁰⁸ Another 2017 Meta survey showed that by age 12, roughly 50% of 12-year-olds either use an Instagram account or have asked their parent for one.¹⁰⁹ Later, in 2018, a Meta study stated that assessing users they “predict to be 13 and 14 today” allowed them to estimate that “there were 4M people under 13 in 2015 on IG [which] represents around 30% of all 10-12 years old [sic] in the US.”¹¹⁰ In 2020, a Meta study stated that 22% of 6-to-9-year-olds and 35% of 10-to-12-year-olds reported having used Instagram in the past month, while 14% of 6-to-9-year-olds and 21% of 10-to-12-year-olds reported that most of their friends were on Instagram.¹¹¹ Taken together, studies of the Meta platforms paint a clear and undeniable picture. Across methodologies, sample populations, and survey years, the results converge on the same conclusion: substantial numbers of children under 13 use Facebook and Instagram, and have done so for well over a decade. The exact percentages may vary from

¹⁰⁷ Rideout, V., Peebles, A., Mann, S., & Robb, M. B., Common Sense census: Media use by tweens and teens, 2021. Common Sense Media (2022), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0 at 5.

¹⁰⁸ META3047MDL-003-00135851.

¹⁰⁹ META3047MDL-047-00608197-198.

¹¹⁰ META3047MDL-014-00133666.

¹¹¹ META3047MDL-003-00124191; META3047MDL-003-00124207.

Expert Report – Highly Confidential

breaks the connection between that data and the child’s account by swapping the real user ID with a random, made-up one. The user content and information stays in the system for technical reasons, but Meta no longer knows which user it came from.¹⁷⁸

4.4 META’S UNDERAGE DETECTION AND ENFORCEMENT

101. Meta relies—and has always relied—primarily on user-supplied birthdates collected at sign-up, supplemented by a checkpoint process triggered by user reports, manual reviewer observations, or specific user-created account-change events (e.g., updating age to under 13). Although Meta has narrowly deployed age-assurance mechanisms, its companies’ systems still do not directly classify or infer users under the age of 13 for automated enforcement. Meta has explicitly limited its age-prediction models from detecting or inferring under-13 users, except in narrowly pre-defined and restricted scenarios.

102. At this stage, Meta’s under-13 enforcement posture is characterized by a layered but still largely reactive framework based on self or community reporting: underage reports from users and reviewers, automated dismissal systems optimized primarily to validate adult status, discretionary moderator review, and selective use of third-party verification tools. While the recently

¹⁷⁸ Hartnett Ex. 6 at 15 (“At 90 days, all data is either deleted or de-identified”).

Expert Report – Highly Confidential

introduced heuristic model represents Meta’s first at-scale proactive mechanism for surfacing potential under-13 accounts, this system is rules-based rather than model-based and is sensitive to context and vulnerable to evasion.

103. In practical terms, Meta has implemented incremental improvements in age-assurance controls over the past four years—such as full DOB collection on legacy Instagram accounts and the introduction of cross-platform enforcement, but the reach of those changes is minuscule compared to Meta’s user base. In short, the company still does not operate a comprehensive, purpose-built system to detect and remove under-13 users with reasonable reliability. Instead, Meta’s framework remains reliant on user self-disclosure, and limited and flawed automated heuristics. As explained below, Meta’s historical and current approach to designing and implementing age-assurance controls has not met baseline expectations for secure-age verification mechanisms and is inconsistent with foundational principles of sound security practice.

4.5 META’S DEPLOYED UNDERAGE TECHNOLOGY, PROCESSES AND POLICIES

104. Over its more than twenty-year history, Meta’s efforts to detect and mitigate under-13 use on Facebook and Instagram have been piecemeal, reactive, and largely ineffective. Rather than following a sustained, coherent strategy, the

Expert Report – Highly Confidential

company has introduced isolated technologies, processes, and policies. As detailed below, these mechanisms were deployed, adjusted, or abandoned in an ad hoc manner, with very little measurable progress toward reliably identifying or removing underage users despite two decades of opportunity to do so. This section provides a chronological description of the controls Meta has implemented over time, illustrates how the company’s approach evolved—often slowly and inconsistently—across the platform’s history, and explains why these controls were insufficient to reliably detect or remove under-13 users as highlighted below and expanded in the opinion sections to follow. The initiatives are summarized in Table 1 and described below.

Table 1 - Meta deployed technologies and policies

Date / Period	Initiative (Platform)	Description	Purpose
2004	Facebook launch (<i>FB</i>)	Platform launches self-reporting of age at least by 2009	Established baseline age gate via self-identification
2012	Instagram acquisition (<i>IG</i>)	Meta acquires Instagram; IG users are not asked to report their age	Platform expansion
2013	Underage reporting (<i>IG</i>)	Meta allows reporting of underage IG users via webform	Creates manual enforcement pipeline
2016	Age affinity model development (<i>FB</i>)	Account content was scanned for indicators of age, e.g., “Happy XX Birthday”	Developing ground truth for age inference models
2017–mid-2020	Default age on account creation screen	New accounts default to age 25 unless user changes	
2018	Human under-13 (<i>U13</i>) escalation (<i>FB/IG</i>)	Reviewers instructed to escalate suspected U13 accounts	Creates additional manual enforcement pipeline
Nov 2019–Feb 2020	DOB ¹⁷⁹ change checkpointing (<i>FB</i>)	Accounts changing DOB to <13 are checkpointed	Detect self-identified users “correcting” age to under 13

¹⁷⁹ DOB refers to date of birth

Expert Report – Highly Confidential

Dec 2019	DOB required at signup (<i>IG</i>)	DOB required for all new Instagram accounts	Self-identification age gate
Jun 2020– Apr 2024	Underage checkpoint logging (<i>FB/IG</i>)	Centralized logging of U13 checkpoint events	Track enforcement actions
Feb 2021	DOB change checkpointing (<i>IG</i>)	Accounts changing DOB to <13 are checkpointed	Detect self-identified users “correcting” age to under 13
May 2021	Auto-ignore of certain reports (<i>FB/IG</i>)	Reports lacking bios/photos or flagged “adult” by model ignored	Reduce queue backlog
Oct 2021	reCAPTCHA on U13 report form (<i>FB/IG</i>)	Google reCAPTCHA added to report form	Reduce reports from automated “bots”
Dec 2021	Cross-platform account matching (<i>FB ↔ IG</i>)	IG U13 account disabling cascade to FB, in 2021 fixed to flow both ways	Cross-platform enforcement linkage (hard-linking)
May–Jun 2022	DOB collection push (<i>IG</i>)	All IG users without DOB required to add DOB (~60M U.S.)	Collect self-reported user ages
2022–Apr 2023	Disabled account retentions (<i>FB/IG</i>)	Disabled U13 accounts held for 6 months prior to beginning of 90-day deletion process	Post-disable retention policy
Jun 2022	Yoti verification for 18+ DOB changes (<i>IG</i>)	Facial age estimation for DOB change to 18+	Prevention of misreporting of adult status
Dec 2022	Yoti for Facebook Dating (<i>FB</i>)	Yoti deployed for FB Dating (18+ only)	Enforce use of dating service to 18+ users
Oct 2023	Yoti for minor→adult upgrades (<i>FB</i>)	Yoti applied to upgrades from <18 to 18+	Prevent underage age-up fraud
Oct 2024	Under-13 heuristic deployed (<i>FB/IG</i>)	Pattern-based proactive U13 detection system	Automated U13 detection

105. **2004 – Facebook is created (Facebook):** Facebook was founded in 2004 by Mark Zuckerberg along with his Harvard classmates Eduardo Saverin, Dustin Moskovitz and Chris Hughes.¹⁸⁰ Initially called “TheFacebook.com,” it launched as a social network for Harvard students before expanding to other colleges and, by 2006, opened to anyone over the age of 13.¹⁸¹ The company

¹⁸⁰ Mark Hall, Facebook: social network, Britannica Money (2025), <https://www.britannica.com/money/Facebook>.

¹⁸¹ Id.

Expert Report – Highly Confidential

soon became the largest social network service in the world, boasting thousands of schools and millions of users within its first year.

106. Starting in at least 2009 and for many years thereafter, Facebook’s approach to age eligibility relied on self-reported information, specifically the user’s date of birth as entered during signup.¹⁸² In practical terms, this meant that Facebook depended on the user truthfully entering a permitted age rather than on any independent verification or cross-check. This is the principal technique that Meta uses today for age enforcement—self reporting, which can be easily misrepresented.

107. **2012 – Instagram is acquired (Instagram):** In April 2012, Facebook Inc. announced that it would acquire Instagram, the rapidly growing mobile photo-sharing application, for approximately \$1 billion in cash and stock.¹⁸³ Instagram was founded in 2010 and allowed users to capture, edit, and share photos through a mobile-first interface. The app offered simple filters and social sharing at a time when smartphone-based, image-based social networking was expanding rapidly. The acquisition signaled Facebook’s new focus on mobile platforms and required broadening of the services for account management into more visual, mobile-centric services.

¹⁸² Hartnett Dep. Ex. 6 at 25.

¹⁸³ Evelyn Rusli, Facebook Buys Instagram for \$1 Billion, New York Times (Apr. 9, 2012), <https://archive.nytimes.com/dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/>.

Expert Report – Highly Confidential

108. Following the acquisition, Instagram’s existing onboarding and account-creation model remained largely unchanged with respect to age eligibility. Unlike Facebook, which required users to enter a date of birth during signup, Instagram did not require any age disclosure at all. Users could create accounts without providing a birthdate.¹⁸⁴,¹⁸⁵ Aside from third-party reporting (which began on Instagram in mid-2013), no other age verification measures were used until at least 2019 (see below). As with Facebook, self-reporting remains the main (and for most users only) means of age assurance on Instagram.

109. **2013 – Creation of Online Reporting (Facebook and Instagram):** In approximately mid-2013, Meta created a mechanism for individuals to report accounts that appeared to belong to users under the age of 13 on Instagram.¹⁸⁶ A similar mechanism for Facebook had been available since at least 2011.¹⁸⁷ This reporting occurred through a publicly accessible web form that allowed anyone—including Facebook and Instagram users, parents, teachers, and members of the general public—to submit a concern about a potentially underage account. Once submitted, these reports entered Meta’s internal

¹⁸⁴ META3047MDL-047-00809658 at 23; Paolo Zialcita, Instagram Now Requires Users To Provide Their Age, KPBS Public Media (Dec. 04, 2019), <https://www.kpbs.org/news/2019/12/04/instagram-now-requires-users-to-provide-their-age>.

¹⁸⁵ Hartnett Dep. Ex. 6 at 22.

¹⁸⁶ META3047MDL-012-00000096.

¹⁸⁷ See META3047MDL-111-00240578 at -00240581 (55,000 reports of underage users on Facebook from May 2011 through March 2013).

Expert Report – Highly Confidential

attempting to evade enforcement. Because it is available and used widely in other enforcement actions and workflows, extending soft-matching to this use case would require minimal additional computation and would materially increase coverage without meaningfully misidentifying of-age users as being under 13. Indeed, the fact that the soft-matching predictions used data that is already present in Meta’s systems further indicates the integration with the detection of under-13 accounts would be feasible. Meta’s internal documents highlight concerns that the failure to deploy soft-matching for under-13 detection represents an inconsistency. In a senior-level discussion preparing for briefing CEO Mark Zuckerberg⁴⁶⁵, Meta’s employees stated, “It is difficult to defend the use of inferred account links for advertising purposes without also using these links for age management.”⁴⁶⁶

8.3 SUMMARY OPINION

354. Meta’s failure to apply its existing soft-matching capability to the detection and removal of under-13 accounts constitutes a failure to leverage an effective mechanism for under-13 enforcement. Soft-matching is a mature technology relied upon by Meta for a range of sensitive enforcement activities, including identifying evasion by banned users and linking coordinated policy-violating

⁴⁶⁵ Hartnett Dep. 238:15-17

⁴⁶⁶ Hartnett Dep. Ex. 27 at META3047MDL-050-00014485.

Expert Report – Highly Confidential

accounts. The same capability, if applied, would offer an efficient, scalable, and effective method for identifying additional under-13 accounts controlled by the same individual.

9 META RETAINS UNDER-13 USER DATA FOR UNREASONABLY LONG PERIODS AFTER DETECTION

355. I have been asked to evaluate Meta’s processes for disabling and deleting accounts identified as underage, and to assess whether these mechanisms operate in a timely, complete, and reliable manner once an account has been flagged.

9.2 PROCESS FOR UNDERAGE ACCOUNT DATA DELETION

356. In this section I comment directly on Meta’s three-stage process that is applied when an account is checkpointed and may ultimately be deleted. The first stage is a “checkpoint” period which since 2022 has lasted thirty days during which a user may appeal.⁴⁶⁷ No account data deletion, anonymization, or encryption is performed during this stage, and the account remains on the platform. During the checkpoint period, a user’s account is suspended and the user cannot access it and the account.⁴⁶⁸ Prior to May 2020 on Facebook and August 2022 on Instagram, however, when a user was in an age checkpoint, their profile remained visible to other users, though the user could

⁴⁶⁷ Hartnett Dep. at 105:11-106:7, 298:8-25.

⁴⁶⁸ META3047MDL-053-00012720.

Expert Report – Highly Confidential

not access their account unless they provided documentary proof they were over 13.⁴⁶⁹

357. When an account enters the suspended “disabled” state,⁴⁷⁰ it is flagged as being disabled,⁴⁷¹ indicating that it is no longer designated for operational purposes and Meta’s systems are supposed to ignore the account.⁴⁷² The data for the account, however, stays in the same database as it was before.⁴⁷³ There is also a period of time before an account is deleted, during which such an account’s data continues to appear in and be used by Meta’s systems that train its machine learning models.⁴⁷⁴ Lastly, the account enters a “scheduled for deletion” state,⁴⁷⁵ after which the account is physically or virtually deleted, which can take 90 days.⁴⁷⁶

358. In summary, underage personal information identified before April 2024 could remain in Meta’s systems for over one year after Meta determined it likely belonged to an underage user before Meta began deleting it (a process that could take an additional 90 days, or three months, and may not result in the data actually being deleted off of Meta’s systems).⁴⁷⁷ Following the April

⁴⁶⁹ META3047MDL-053-00012720.

⁴⁷⁰ Harnett Dep. at 349:18-351:22.

⁴⁷¹ Hartnett Dep., Ex.6, at 14.

⁴⁷² Harnett Dep. at 339:9-339:15, Ex. 6 at 14.

⁴⁷³ Hartnett Dep. at 299:3-301, Ex. 6 at 14.

⁴⁷⁴ Backstrom Dep. at 28:24-31:3, 41:12-23 and related errata.

⁴⁷⁵ Hartnett Dep. at 106:3-17, Ex. 6 at 14.

⁴⁷⁶ Hartnett Dep. at 301:15-19.

⁴⁷⁷ Hartnett Dep. at 297-301, 349-351, Ex. 6 at 13-15.

Expert Report – Highly Confidential

2024 change, the combined duration of all three stages is approximately four-and-a half-to-five months.⁴⁷⁸

9.3 PROCESS-DRIVEN DELAYS IN DELETION

359. In my opinion, Meta’s timeline for deleting underage user data is overly protracted and leads to unnecessary retention of sensitive data on the platform, in violation of well-accepted industry norms and standards.⁴⁷⁹
360. As an initial matter, modern cloud platforms are capable of deleting user data quickly and reliably, often within seconds.^{480,481,482} Major providers such as Amazon Web Services, Microsoft Azure, and Google Cloud implement deletion operations that update object state immediately and propagate the change across replicated storage systems within seconds to a few minutes, depending on the service tier and durability model. This behavior is standard in large-scale distributed storage architectures: rapid, consistent deletion is required both for normal operation (e.g., freeing space, updating indexes) and for meeting industry expectations around data governance and lifecycle management. Meta operates storage and data-infrastructure systems of

⁴⁷⁸ Id.

⁴⁷⁹ International Organization for Standards, ISO 27001:2022: A.8.10; National Institute of Standards & Technology NIST Pub. 800-53 ch. 3 SI-12.

⁴⁸⁰ Delete and restore a blob with .NET, Microsoft Azure, <https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-delete>.

⁴⁸¹ Deleting a general purpose bucket, AWS, <https://docs.aws.amazon.com/AmazonS3/latest/userguide/delete-bucket.html>.

⁴⁸² Data deletion in Google Cloud, Google, <https://cloud.google.com/docs/security/deletion>.

Expert Report – Highly Confidential

comparable sophistication, including globally distributed object stores, replicated databases, and large-scale indexing systems. Nothing in publicly available information or in the internal Meta materials I reviewed suggests any technical limitation that would prevent Meta from deleting underage user data on similarly rapid timescales.

361. Note that Meta suggests that the extended periods holding in a disabled state is due to legal reasons: "[t]he reason Meta does that is for the possibility of needing to do legal discovery that would involve sharing the data on those disabled accounts. That's why the disablement period exists."⁴⁸³ And "The reason we have a disabled period is so that further reviews can be done and we can determine if we need to extend the retention of those accounts. The disablement timelines above are minimum times; there are certain instances where extensions for those periods are implemented, for example for legal hold."⁴⁸⁴ Even in situations where temporary retention might be justified, best practice (described below) dictates that such data should be immediately segregated from the active operational environment.⁴⁸⁵ Common strategies

⁴⁸³ Hartnett Dep. 300:9-13.

⁴⁸⁴ Hartnett Dep. Ex. 6 at 14.

⁴⁸⁵ Technical Approaches to Uncovering and Remediating Malicious, CISA (Sept. 24, 2020), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a>; Duke Information Security Office, Compromised Account Quarantining Practices, Duke University, <https://security.duke.edu/policies-procedures-and-standards/access-security/compromised-account-quarantining-practices/>.

Expert Report – Highly Confidential

for incident response⁴⁸⁶ (such as identification of suspected underage users and content) include the immediate transfer of the data to a dedicated, quarantined storage zone or the application of encryption-at-rest with the keys for decryption isolated in a secure key management service.⁴⁸⁷ In both scenarios, the data remains available for administrative or compliance purposes, and again, to train Meta's machine learning models, but is inaccessible to some other business processes.⁴⁸⁸ Here, in opposition to best practices relating to data isolation, Meta continued to expose data of users its systems had determined were likely under-13 to internal systems during the disabled period, leaving the data available for training Meta's machine learning and generative AI models powering Meta's content and ad recommendation systems and features.⁴⁸⁹

362. Regardless of the rationale Meta offers for maintaining a disabled period, the additional 90-day window required to complete deletion⁴⁹⁰ is difficult to justify. As described below, modern storage systems used by large platforms routinely support timely data removal or cryptographic erasure, and nothing

⁴⁸⁶ In cyber-security, incident response is the coordinated set of technical and operational procedures a platform uses to detect, analyze, contain, remediate, and recover from security events or system abnormalities. The detection of an underage account would be deemed an incident. See for example, Duke University, Compromised Account Quarantining Practices, <https://security.duke.edu/policies-procedures-and-standards/access-security/compromised-account-quarantining-practices/>; Rice University Office of Information Technology, Quarantining Process used by IT Staff Members, Rice University, <https://oit.rice.edu/quarantining-process-used-it-staff-members-introduction>.

⁴⁸⁷ Id.

⁴⁸⁸ Hartnett Dep., Ex.6 at 14; Backstrom Dep. 28:24-31:3, 41:12-23 and related errata.

⁴⁸⁹ Backstrom Dep. 29:23-30:22, 41:12-23 and related errata.

⁴⁹⁰ Hartnett Dep. 301:6-301:19, Ex. 6 at 14.

Expert Report – Highly Confidential

in Meta’s architecture prevents the company from deleting underage user data on significantly shorter

9.4 META’S DATA-RETENTION DELAYS FALL OUTSIDE ACCEPTED SECURITY PRACTICE

363. Failure to delete known sensitive data for long periods (such as 90 days) is counter to security practice. The management of sensitive, high-risk data (e.g., underage social media data, including personal information) is not simply a matter of efficiency; it is a foundational requirement of sound data governance. Effective programs minimize data retention, restrict access to the smallest possible set of individuals or systems, and ensure that sensitive data cannot be misused while it remains in storage. These principles are reinforced in widely recognized standards. For example, NIST guidance recognizes that one of the fastest and most secure ways to “delete” data is simply to destroy the encryption keys that protect it. Without the key, the remaining data becomes unreadable instantly, even though the encrypted bits may still sit on a server for a short period.⁴⁹¹ This method, called cryptographic erasure, allows organizations to make data immediately inaccessible.⁴⁹² ISO/IEC

⁴⁹¹ Computer Security Resource Center, cryptographic erase, National Institute of Standards & Technology, https://csrc.nist.gov/glossary/term/cryptographic_erase.

⁴⁹² NIST SP 800-88 Rev. 2: Guidelines for Media Sanitization, NIST, 2025, <https://csrc.nist.gov/pubs/sp/800/88/r2/final>

Expert Report – Highly Confidential

27040 (Storage Security)⁴⁹³ and ISO/IEC 27001 (Annex A.8.10)⁴⁹⁴ stress that sensitive data should be retained for no longer than strictly necessary, protected through segregation from production systems, and subject to secure sanitization as soon as its retention is no longer justified.

364. The prolonged retention of confirmed underage user data — for periods that historically stretched beyond half a year and to this day extend close to five months (even after policy changes in April 2024) — exposes the highly sensitive personal information of underage users to ongoing risk. Such processes are a failure to meet basic data governance standards for security.

9.5 SUMMARY OPINION

365. Meta’s handling of data associated with identified under-13 users does not conform to sound security or data-protection practice. Once an account is confirmed or strongly suspected to belong to a minor, Meta continues to retain that user’s data for extended periods—often weeks or months—through multiple internal processing stages.⁴⁹⁵ These protracted processes for executing the deletion are counter to appropriate security practice.

⁴⁹³ International Standards Organization, ISO/IEC 27040:2024 (Information technology - Security techniques - Storage security) (2024).

<https://www.iso.org/standard/80194.html>

⁴⁹⁴ International Standards Organization, ISO 27001 Annex A 8.10 – Information Deletion.

⁴⁹⁵ Hartnett Dep. 297:17-301:19, Ex. 6 at 14.

Expert Report – Highly Confidential

366. From a technical and risk-management perspective, Meta creates unnecessary exposure and contradicts the basic principle of minimizing retention of known ineligible user data. Established industry and government standards emphasize prompt, verifiable deletion once data is no longer required for lawful or operational purposes.⁴⁹⁶ Meta’s multi-stage pipeline—spanning checkpointing, review queues, and scheduled deletion windows—introduces risks of error, loss of control, and potential misuse while providing no corresponding security benefit.
367. In sum, Meta’s deletion practices for under-13 accounts reflect a protracted and fragmented process that leaves children’s data stored longer than necessary and exposes it to avoidable operational risk. These delays run counter to well-established industry expectations for handling sensitive or ineligible user data.

⁴⁹⁶ International Organization for Standards, ISO 27001:2022: A.8.10; National Institute of Standards & Technology NIST Pub. 800-53 ch. 3 SI-12.

Expert Report – Highly Confidential

10 META’S CLAIM THAT SCRIPTED ATTACKS SUBSTANTIALLY IMPACTED THE REPORTING SYSTEM IS NOT SUPPORTED BY THE DATA

368. I have been asked to evaluate the claim that Meta’s reporting system has been under attack from automated software, called “scripted attacks” or “bots”⁴⁹⁷, and, to the degree that such attacks exist, whether they have had a large and/or lasting impact.

369. Meta stated that they have “experienced scripting attacks that increased the number of reports made through these [reporting] forms. The Company has taken steps to reduce the number of these types of attacks, but the data reflects these attacks in addition to legitimate reports to underage users.”^{498, 499} Here Meta has produced documents⁵⁰⁰ (internal communications among employees) discussing seeing very large numbers of reports peaking at 2.3M reports in one and showing graphs of the observed loads:

⁴⁹⁷ Throughout I will use the term scripted attack and bot interchangeably. Further, consistent with its use in cyber-security, I will refer to the coordinated collection of bots as a botnet.

⁴⁹⁸ META3047MDL-012-00000522 at -00000523; META3047MDL-053-00012709 at -00012722.

⁴⁹⁹ See Hartnett Dep., Ex. 28 at 1.

⁵⁰⁰ See META3047MDL-065-00000902 at -00000905; META3047MDL-111-00006892; META3047MDL-190-00034496.

Expert Report – Highly Confidential

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.

A handwritten signature in black ink, appearing to read "Patrick McDaniel", written in a cursive style.

Patrick McDaniel