

EXHIBIT A

**STATE OF NEW MEXICO
COUNTY OF SANTA FE
FIRST JUDICIAL DISTRICT COURT**

STATE OF NEW MEXICO, EX REL.,
RAÚL TORREZ, ATTORNEY GENERAL,

Plaintiff,

v.

NO. D-101-CV-2023-02838

META PLATFORMS, INC.; INSTAGRAM, LLC;
META PAYMENTS, INC.; and META PLATFORMS
TECHNOLOGIES, LLC,

Defendants.

**DECLARATION OF BRENDAN AUSTIN IN SUPPORT OF PLAINTIFF’S
MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR PARTIAL SUMMARY
JUDGMENT FOR DECEPTIVE PRACTICES REGARDING
THE SAFETY OF END-TO-END ENCRYPTION**

I, Brendan Austin, under oath, hereby declare as follows:

I am Counsel for Plaintiff State of New Mexico. My business address is 401 9th Street NW,
Suite 630, Washington, DC 20004.

This declaration is based on my personal knowledge and review of the documents and
information discussed herein.

1. When Meta uses end-to-end encryption (“E2EE”), “messages in the end-to-end encrypted thread—including texts, images, and videos—are end-to-end encrypted, meaning Meta can only view the messages if they are shared with Meta for reporting purposes....” *See* true and correct copy of Defendants’ Objections and Responses to Plaintiff’s Fifth Set of Interrogatories to Defendants, Response to Interrogatory 39 (Sept. 4, 2025), attached as Exhibit 1.

2. Encryption is an “extra layer of security that keeps your messages and calls . . . protected, from the moment they leave your device, to the moment they reach the receiver’s device.

This means that nobody during this delivery, including Meta, can see or listen to what's sent or said." See true and correct copy of <https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/> attached as Exhibit 2.

3. On February 11, 2019, Meta's Safety Policy Manager wrote regarding WhatsApp's E2EE: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] See true and correct copy of METANMAG-079-00111773 at 1774 attached as Exhibit 3.

4. "[E2EE] has been available as an optional setting on Facebook Messenger since 2016, and Messenger started the global rollout of default E2EE for personal chats in December 2023. Meta launched optional E2EE for personal chats on Instagram Direct (IGD) globally starting in the first quarter of 2023." See Ex. 1.

Meta Misrepresented It Would Keep Users Safe While Implementing E2EE

5. On March 6, 2019, Mark Zuckerberg announced that Meta would implement end-E2EE on its Messenger platform. See true and correct copy of <https://www.buzzfeednews.com/article/ryanmac/mark-zuckerberg-facebook-privacy-focused-platform> attached as Exhibit 4. In the announcement Zuckerberg acknowledged: "[T]here are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services. . . We have a responsibility to work with law enforcement and to help prevent [child exploitation] wherever we can. We are working to improve our ability to identify and stop bad actors across our apps by detecting patterns of activity or through other means, even when we can't see the content of the messages." *Id.* at 8. He further promised that E2EE would not be

implemented at the expense of user safety “as long as we take the time to build the appropriate safety systems that stop bad actors as much as we possibly can within the limits of an encrypted service. We’ve started working on these safety systems building on the work we’ve done in WhatsApp, and we’ll discuss them with experts through 2019 and beyond before fully implementing end-to-end encryption.” *Id.* at 9.

6. A March 17, 2021, Instagram blog post titled, “Continuing to Make Instagram Safer for the Youngest Members of Our Community” states: “As we move to end-to-end encryption, we’re investing in features that protect privacy and keep people safe without accessing the content of DMs [direct messages].” *See* true and correct copy of <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community> attached as Exhibit 5.

7. On December 6, 2023, Meta’s vice president for Messenger said: “We worked closely with outside experts, academics, advocates and governments to identify risks and build mitigations to ensure that privacy and safety go hand-in-hand.” *See* true and correct copy of <https://www.theguardian.com/technology/2023/dec/07/meta-facebook-messenger-end-to-end-encryption> attached as Exhibit 6.

8. Each of these statements were available nationally and in New Mexico online via Meta’s website.

9. Meta did not disclose publicly its knowledge, summarized below, that E2EE would eliminate its ability to detect child sexual exploitation on its encrypted spaces.

Meta Knew E2EE Would Make Its Platforms Less Safe, and that Meta’s Safety Mitigations Were Inadequate

10. On November 29, 2018, a former Data Scientist and Integrity Engineer sent an internal PowerPoint to several Meta employees admitting: “A significant portion of our high

intensity content violations are from Messenger. . . . Referrals to law enforcement heavily depend on Messenger evidence.” *See* true and correct copy of METANMAG-002-00385884 & METANMAG-002-00385885 at pgs. 1, 5, collectively attached as Exhibit 7.

11. On February 12, 2019, Antigone Davis, Director, Global Head of Safety, told Meta’s Director of Policy Communications: “The quality and value of our reports to NCMEC [National Center for Missing and Exploited Children] will drop dramatically, rendering them close to useless. . . . FB allows pedophiles to find eachother [*sic*] and kids via social graph [the network among users] with easy transition to Messenger. WA [WhatsApp] does not make it easy to make social connections, meaning making Messenger e2ee will be far, far worse than anything we have seen/gotten a glimpse of on WA.” *See* true and correct copy of METANMAG-002-00392940 attached as Exhibit 8.

12. On February 25, 2019, a senior staffer in Meta Global Affairs provided a note “analyzing the impact of E2EE in messenger on safety.” *See* true and correct copy of MT-IG-AG-NM-000054789 attached as Exhibit 9. The note states: “Without robust mitigations, E2EE on Messenger will mean we are significantly less able to prevent harm against children.” *Id.* at 4790-95. The note states: “Without mitigations on e2ee that enable us to credibly identify images of child sexual exploitation within Messenger, total reporting to NCMEC will drop (at least) from 18.4 million to 6 million (a 65% drop).” *Id.* The analysis continued: “E2EE will severely impact our proactive and reactive work with law enforcement, including terrorism, child sexual exploitation, suicide and school shootings emergencies.” *Id.* The note warns: “Implementing E2EE will also potentially create additional harms given the connection between FBM [Facebook Messenger] and Facebook. Given that perpetrators can identify and befriend victims on Facebook, before taking them easily into the secret world of E2EE.” *Id.* The note also warned: “We currently

scan messenger content for images of child sexual exploitation, using a hashing system is used by all major companies (this compiles a digital signature or fingerprint of images (known as a “hash”), which can be matched against a database of known child pornography images) . . . In annual year 2018, we reported 12.4 million cases of messenger users exchanging CSE [child sexual exploitation] imagery to NCMEC. 12 million of these were detected by us using hashes, the rest were reported by users. Total NCMEC reporting for 2018 was 18.4 million. Without our ability to scan for hashes, NEMEC reporting would have been 6.4 million.” *Id.* The note also admitted that “behavioral analysis of metadata for child grooming is only 1% successful and throws up thousands of false positives.” *Id.*

13. On February 26, 2019, the staffer provided an updated note with a more specific breakdown of E2EE’s impact. Based on 2018 data, Meta “would be unable to provide data proactively [to law enforcement] in: 600 child exploitation cases[,] 1,454 sextortion cases[,] 152 terrorist cases[,] and 9 threatened school shootings. *See* true and correct copy of METANMAG-007-00339102 attached as Exhibit 10.

14. On March 3, 2019, responding to a draft of Mark Zuckerberg’s E2EE announcement, Antigone Davis told Monika Bickert, Head of Global Policy Management: “[I]f we reconcile for [REDACTED] [REDACTED], Meta’s Executive Communications Director]/Mark we don’t give Mark an opportunity to think through the tension.” *See* true and correct copy of METANMAG-002-02430615 at 0615 attached as Exhibit 11. Bickert responded: “I agree. He is doing bad stuff and should get the blowback for it.” *Id.*

15. On March 2, 2019, [REDACTED], Director and Global Head of Security Policy and Counter-Fraud, and Bickert discussed Zuckerberg’s planned E2EE announcement. *See* true and correct copy of METANMAG-005-01153310 attached as Exhibit 12. Bickert said: “We are

about to do a bad thing as a company . . . This is so irresponsible.” *Id.* at 3310. ██████ said: “The section on safety seems pretty problematic . . . Feels like we are committing to stuff we absolutely can’t deliver on.” *Id.* Bickert responded: “Absolutely. . . . There is no way to find the terror attack planning or child exploitation . . . The stuff we do the proactive referrals on . . . Period.” *Id.* ██████ also said: “I specifically meant the E2EE section – and the gross misstatements of our ability to conduct safety operations w/ E2EE. . . . doing it while telling ourselves and the world that it won’t have any impact on safety seems both bad business . . . and deeply irresponsible.” *Id.* at 3311.

16. In April 2019, Meta began a “proactive risk investigation into inappropriate interactions with children [IIC] with a focus on preparing for end to end encryption.” *See* true and correct copy of METANMAG-002-02373893 attached as Exhibit 13. The executive summary for the risk investigation explained: “IIC enforcement currently focuses heavily on detecting real world harm (such grooming . . .) and online harm (CEI [child exploitation images] and sexual conversations). These abuses largely occur in messenger.” *See* true and correct copy of METANMAG-021-00151987 at 1987 attached as Exhibit 14. The risk investigation found “IG recommended a minor . . . to an account engaged in groomer-esque behavior[,] 3 accounts engaged in IIC remained live on the platform even after FB received signal that they were engaging in child exploitation[,] [m]inors reported adults interacting inappropriately in IGDM [Instagram direct messages] and we left the accounts up[,] [m]inors have a limited ability to prevent receiving violating unsolicited messages from adults[, and] [a]dults interacted with minors inappropriately in comments.” *Id.* at 1987-88. “Currently, in order to identify something as IIC we have to know the relative age of the two parties (adult and minor) and the two must be engaged in sexualized conversation. This has been historically challenging to enforce on IG both because we do not collect age of users and the detection of sexualized conversation usually occurs in messages which

receive limited review and will no longer be accessible going forward (unless user reported).” *Id.* at 1988-89. Making encrypted messages even more dangerous, the investigation warned: “[w]e are facilitating adults finding minors and minor-focused content through recommendations and explore. . . . Adults are easily able to find minors to inappropriately interact with on IG. . . . IG algorithm does not take in to [sic] account violations when serving content. . . . We don’t take age into account when deciding what to recommend to someone.” *Id.* at 1990.

17. On April 4, 2019, a Meta Data Science Manager acknowledged: “I believe everyone knows that I’m an advisor at an anti-human trafficking non-profit. The moment Backpage¹ was taken down, all of their data showed that IG had become the leading two-sided marketplace for human trafficking. This is something I have brought up, and it’s a challenging situation, which will be made untenable (more) with e2e [end-to-end encryption].” *See* true and correct copy of METANMAG-002-00559617 at 9617 attached as Exhibit 15.

18. A June 2019 document, titled “On Encryption: law Enforcement / Child Safety Messaging,” internally admitted: “We will never find all of the potential harm we do today on Messenger when our security systems can see the messages themselves”; “[Zuckerberg] already committed to e2e without knowing what safety you can build.” *See* true and correct copy of MT-IG-AG-NM-000067909 & MT-IG-AG-NM-000067918 at 7919, collectively attached as Exhibit 16. The document asks Zuckerberg: “[I]f we don’t think you can build true safety into this platform will you abandon e2e messaging?” *Id.* at 7920. To which Zuckerberg responded: “We will do

¹ “Backpage.com, a now-shuttered internet forum for prostitution ads that included ads depicting sex work of children” *See* <https://www.justice.gov/usao-cdca/pr/justice-department-agrees-215-million-settlement-agreement-related-assets-internet>.

everything we can to keep them safe on our services within the limits of what's possible in an encrypted service.” *Id.*

19. An internal document from the second half of 2019, titled “Child Sexual Exploitation, Abuse, and Nudity Top Risks Identified by CRA [Community Risk Assessment]” states: “As the problem team is well-aware of, one of the most significant challenges with regards to Child Nudity and Sexual Exploitation on the platform is the shift to E2EE. We have seen in countless investigations that individuals and networks . . . use messenger to share images of children, as well as to pursue inappropriate relationships with them. . . . Efforts to proactively combat this content and behavior will be significantly limited in an encrypted world.” *See* true and correct copy of METANMAG-122-00017648 at 7648 attached as Exhibit 17.

20. In a presentation dated May 28, 2020, titled “Child Safety Risks in Rooms & RTC 101,” a Safety Policy Director and Safety Policy Manager acknowledged: “User Reporting is important but it’s not enough: Minors rarely report their own abuse. Tech savvy offenders engage in extensive vetting of one another when sharing CSAM [child sexual abuse material] or exchanging tips. Bystanders will have limited access or visibility into what’s really happening.” *See* true and correct copy of METANMAG-005-00508073 at p. 47 attached as Exhibit 18.

21. An internal PowerPoint, dated February 4, 2021, titled “IG Teen Safety Check In” admitted: “Almost all IIC happens in private spaces and over 90% of CEI sharing. Limited access to message data post E2EE means it’s harder for us to confirm that a child has been harmed.” *See* true and correct copy of METANMAG-002-00741159 at p.11 attached as Exhibit 19.

22. On May 7, 2021, an employee wrote: “I came across this a while back and it’s more about Messenger than IGD [Instagram Direct], but it’s research on why people are hesitant to report abuse in their private messages (which is the only way we’d be able to act on such content

in an e2ee environment).” *See* true and correct copy of METANMAG-002-01824224 attached as Exhibit 20.

23. On May 8, 2021, a former Vice President at Facebook said: “[c]ontext here - there was decision made to encrypt all private messages for u13. This has severe impact on safety as we know. I am trying to argue, perhaps foolishly, that its [*sic*] not the best decision for our users. Decision was made a while ago.” *See* true and correct copy of METANMAG-002-00032490 at 2490 attached as Exhibit 21.

24. In his deposition, Mark Zuckerberg testified that, in implementing E2EE, he weighed user privacy versus safety and said: “In general, yeah, once we decide that we’re going to do something, unless there’s a good reason to change it, we’re not going to change.” *See* true and correct copy of excerpt of Mark Zuckerberg Dep. Tr. (July 14, 2025) at 74:16-19 attached as Exhibit 22.

25. An internal document with a metadata date of January 5, 2022, reported: “With E2EE, we lose the ability to identify and remove the ~600k shares of CSAM and NCII per day.” *See* true and correct copy of METANMAG-010-00249146 at 9152 attached as Exhibit 23. The document further states: “With E2EE the MMS system will no longer be able to run on content. Meaning the content that would be removed today will continue to exist in the messaging ecosystem and likely to be propagated even further.” *Id.* at 9154. The document further states: “With the launch of E2EE, we will lose our ability to enforce on a significant amount of . . . CSAM.” *Id.* at 9155.

26. On August 22, 2022, employees considered: “how valuable is this [child safety] signal post e2ee?” An employee replied: “It’s not :) This is one of the signals that will decay.” *See* true and correct copy of METANMAG-011-00058374 at 8375 attached as Exhibit 24.

27. On August 24, 2022, an employee wrote: “Violations in child safety are some of the most egregious on our platform and for the larger society. However, with end-to-end encryption (e2ee) across private surfaces, the child safety team will lose most of the signals used to detect actual violations.” *See* true and correct copy of METANMAG-079-00067274 at 7275 attached as Exhibit 25.

28. On March 13, 2023, Meta employees discussed a new “Child Safety Account Score (powered by MaCSA).” *See* true and correct copy of METANMAG-039-00014006 attached as Exhibit 26. One of the employees advised: “E2EE resilient detection when they say this, it means they are just not looking into messages[.] it’s not like a big thing imo, they are just trying to sell it as E2EE resilient.” *Id.* at 4006.

29. On April 26, 2023, an employee warned: “1. The vast majority of cybertips are not from user reports. [W]e will almost certainly lose >90% of csam cybertips after e2ee. 2. [W]e have greatly improved the number of user reports we now get through upselling and other tactics. It’s moving in the right direction. But this will never replace our proactive scans. Not ever.” *See* true and correct copy of METANMAG-130-00047617 at 7618 attached as Exhibit 27.

30. On June 14, 2023, a Content Policy Manager said: “I recall one of the MaCsa signals being ‘user has searched for a designated CSAM search term in X timeframe.’” *See* true and correct copy of METANMAG-051-00257846 at 7846 attached as Exhibit 28. With respect to the list of CSAM search terms, an employee responded “██████████ organized it and for a while we had a queue to add to it. We couldn’t maintain funding for this over time and adding to the list didn’t make the cut. . . . the recall is likely inadequate.” *Id.*

31. An internal document with a metadata date of September 13, 2023, admitted: “Is [Messenger] E-2-E Encryption a concern for CEI? Yes. Messenger is the platform where the large

majority of CEI is shared . . . When E2E encryption is instated, we lose the ability to enforce on content from Messenger. This means an estimated decrease of 86% of bad actors we are disabling and 77% of CEI profiles referred to NCMEC.” *See* true and correct copy of METANMAG-002-02104658 at 4679-80 attached as Exhibit 29.

32. In December 2023, Meta began to implement default E2EE in Messenger and completed the process in the summer of 2024. *See* Ex. 2.

33. On December 14, 2023, a Meta employee observed: “there goes our CSER [Community Standards Enforcement Report] numbers next year . . . this is the big report that Meta discloses on enforcement . . . the 7.5 million CSAM reports . . . we’ll lose a ton of recall due to E2EE . . . you know how [REDACTED] tells you to stop looking under rocks, the entire company just put a big rug down to cover the rocks.” *See* true and correct copy of METANMAG-051-00251525 at 1525 attached as Exhibit 30. Another employee responded: “easy as anything to view CSAM on Instagram.” *Id.* at 1526.

34. On March 20, 2024, another employee wrote: “We previously confirmed that Upload IP is not available on WA (and consequently for E2EE Messenger bc we use the same infra[structure]) because of privacy decisions that WA has taken in the past. . . . The bigger picture risk, on that basis, is that in the context of fewer reports going to LE [law enforcement] post E2EE, the ones that we do send are set to miss a vital piece of data which LE uses to convince judges to sign search warrants.” *See* true and correct copy of METANMAG-084-00160745 at 0745-46 attached as Exhibit 31.

Governments And Child Safety Advocates Urged Meta to Abandon E2EE Without an Exception For Child Exploitation

35. On October 4, 2019, Rt Hon Priti Patel MP, United Kingdom Secretary of State for the Home Department, William P. Barr, United States Attorney General, Kevin K. McAleenan,

United States Secretary for Homeland Security, and Hon Peter Dutton MP, Australian Minister for Home Affairs, wrote a letter to Mark Zuckerberg “to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction in user safety and without including a means for lawful access to content of communications to protect our citizens.” *See* true and correct copy of Open Letter: Facebook’s “Privacy First” Proposals, found at https://assets.publishing.service.gov.uk/media/5d95fae040f0b6174e96e6f1/Open_letter_from_the_Home_Secretary_-_alongside_US_Attorney_General_Barr_Secretary_of_Homeland_Security_Acting_McAleenan_and_Australian_Minister_for_Home_Affairs_Dutton_-_to_Mark_Zuckerberg.pdf attached as Exhibit 32. The letter also said: “NCMEC estimates that 70% of Facebook’s reporting – 12 million reports globally – would be lost. This would significantly increase the risk of child exploitation or other serious harms.” *Id.* at 2.

36. A briefing titled “MZ Briefing E2E Meeting w/Co-Founder of Thorn Ashton Kutcher” states: “Thorn . . . would like us to find a way to make a special carve out for child exploitation . . . they have made clear they will push us and policymakers to find a way to carve out child sexual exploitation.” *See* true and correct copy of MT-IG-AG-NM-000067910 at 7910 attached as Exhibit 33.

37. A briefing titled “MZ Briefing NCMEC” reported: NCMEC had “received calls from the UK Home Office, the European Commission, Interpol, the Child Exploitation and Obscenity Section and the DoJ, [*sic*] and others expressing concern about our decision and plans.” *See* true and correct copy of MT-IG-AG-NM-000067914 at 7915 attached as Exhibit 34.

38. NCMEC raised concerns regarding E2EE with Meta: “There would have been numerous meetings and conversations at different operational levels, at a leadership level, when NCMEC was first made aware of Meta’s plans to implement end-to-end encryption, the impact that would have both in the quality of reports and the volume of reports that Meta was able to make.” *See* true and correct copy of excerpts of NCMEC Rule 1-030(b)(6) Dep. Tr. (July 3, 2025) at 131:10-17 attached as Exhibit 35.

Meta’s Platforms Became Less Safe in New Mexico After Meta Implemented E2EE

39. On May 8, 2024, three suspected online predators were arrested in New Mexico following a months-long undercover investigation of child predators on Meta’s platforms called “Operation Metaphile.” *See* true and correct copy of <https://nmdoj.gov/press-release/new-mexico-attorney-general-raul-torrez-announces-arrests-of-suspected-online-predators-following-operation-metaphile/> attached as Exhibit 36. The suspects, Fernando Clyde, Marlon Kellywood, and Christopher Reynolds, contacted and solicited sex with underage age decoy accounts created by the New Mexico Department of Justice. *Id.* Prior to the arrests, Meta had “detected multiple instances of potential inappropriate activity by accounts believed to be operated” by each of these suspects, *see* Ex. 1, Response to Interrogatory No. 38, yet each of these suspects remained active on Meta’s platforms. Meta did not report any of the suspects to NCMEC until *after* their arrests. *Id.* Meta also admitted that two of the three suspects had message threads that were encrypted. *Id.*

40. Since Meta’s implementation of E2EE, NCMEC has observed a decrease in both the volume and quality of the contents of Facebook’s reports, which NCMEC’s analysis demonstrates stems from E2EE. *See* Ex. 35 at 125:15-126:25; 235:4-20.

41. According to NCMEC, user reports are not an adequate substitute for scanning messages and images that are encrypted: “They are only one facet of child safety for a platform,

but it can't be the only thing that a platform relies on." *See* Ex. 35 at 142:4-19. "[T]he majority of the time children are choosing not to report." *Id.* at 142:21-143:1. The chat information provided with Meta user reports has also become more limited in the wake of E2EE. "Having that limited information can make it extremely difficult to understand what exactly is occurring" and "law enforcement may have difficulty in following up on those reports." *Id.* at 125:15-126:25.

42. In its Rule 1-030(b)(6) deposition, NCMEC testified that, with the implementation of E2EE, cases of child exploitation on Meta's platforms have gone undetected and unreported. *Id.* at 159:6-10.

43. On March 11, 2025, NCMEC submitted written testimony to the US Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism acknowledging that "CyberTipline reports submitted in 2024 did drop from 36.2 million in 2023 to 20.5 million in 2024." *See* true and correct copy of https://www.judiciary.senate.gov/imo/media/doc/2025-03-11_testimony_delaune.pdf at 10, attached as Exhibit 37. The testimony states: "The decrease in overall CyberTipline reports in 2024 does not mean fewer crimes are occurring; it simply means online platforms are not reporting as they should." *Id.* The testimony further states: "Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023." *Id.* at 11. "The most significant factor when comparing volume from 2023 to 2024 was a decline in the number of reports that we received from Facebook." *See* Ex. 35 at 161:2-5.

44. Meta requires users to agree to Facebook's Terms of Service and Instagram's Terms of Use in order to use those platforms. *See* true and correct copy of https://mbasic.facebook.com/legal/terms/plain_text_terms/ attached as Exhibit 38; *see* true and correct copy of <https://help.instagram.com/termsfuse> attached as Exhibit 39

45. The Terms of Service for Facebook states: “How our services are funded . . . we use your personal data...to show you personalized ads.” *See* Ex. 38.

46. The Terms of Use for Instagram states: “How Our Service Is funded . . . We use your personal data . . . to show you ads that are more relevant to you.” *See* Ex. 39.

47. Meta admitted in a blog post, dated September 17, 2024: “We know parents want to feel confident that their teens can use social media to connect with their friends and explore their interests, without having to worry about unsafe or inappropriate experiences.” *See* true and correct copy of <https://about.fb.com/news/2024/09/instagram-teen-accounts/> attached as Exhibit 40.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed this 5th day of November 2025.

/s/Brendan Austin
Brendan Austin