EXHIBIT A

to Plaintiff's Reply Memorandum in Support
of its Motion for Partial Summary Judgement for Deceptive
Practices Regarding the Safety of End-to-End Encryption

RESPONSES TO META'S COUNTERSTATEMENT OF UNDISPUTED FACTS ("RCSUF")

1. The State asserts that "Meta knew that E2EE would make its platforms less safe by preventing it from detecting and reporting child sexual exploitation." Mot. 1. This is a disputed issue of fact.

    a. The benefits and drawbacks of adopting E2EE is a "uniquely challenging and divisive issue" that has been long debated among the child safety and privacy and information security communities, and internally at Meta before the rollout of E2EE. Ex. A (Wirth Rep.) at 24; *see also id*. at 25 (concluding that Meta's adoption of E2EE "can't reasonably be viewed as evidence of poor child safety policies or practices").

    DENIED as misleading and incomplete. This "debate" has not concluded that adoption of E2EE makes Meta's platforms safer with respect to detecting and reporting child sexual exploitation, but has in fact resulted in the opposite conclusion, including within Meta. *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe); Ex. 1 (Levine Rep.) at 95-96 ("E2EE prevents the review, detection, prevention [of], and response [to] CSAM/CSEC as well as the provision of information to law enforcement upon request."); *id*. at 115 ("Meta's move to E2EE represents their choice to largely abandon their ability to find CSAM and CSEC in users' content"); *id*. at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end- to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); Exhibit 38 to Austin Decl. in Support of Plaintiffs Opening Brief (March 11, 2025 Testimony of Michelle DeLaune, President and CEO NCMEC, before United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism) at 11.

    The UN High Commissioner for Human Rights has emphasized the importance of E2EE as "essential if people are to feel secure in freely exchanging information with others on a range of experiences." Ex. B (NCOSE Dep. Ex. 46) at 12.

DENIED as misleading and incomplete. The same document warns of the risks of E2EE in hindering the ability "to detect child sexual abuse material" (*see* Ex. 2 - UN HCHR-EN) at ¶23), and notes that the "[UN] Committee on the Rights of the Child has underlined that any measures to detect child sexual exploitation and abuse material in encrypted communications," while they should be narrowly tailored, need not be eliminated. *Id*. at ¶22; *see also* Ex. 1 (Levine Rep.) at 7 n. 10 ("These crimes represent violations of children's fundamental human rights," citing United Nations "Convention on the Rights of the Child."); *id*. at 99 ("In an open response" to letter from top US, UK, Australian, New Zealand, and Canadian government officials opposing E2EE due to consequent inability to detect 'sexually exploitive situations,' 'images and videos of children being raped and sexually abused,' CEO Mark Zuckerberg refused to distinguish the privacy and safety needs of minors from adults. Mr. Zuckerberg instead erroneously claimed that the needs of adults are the same as children's, as if Meta lacked the ability to keep children's accounts unencrypted.").

U.S. government officials have similarly urged messaging services to adopt E2EE. *See* Ex. C (NCMEC Dep. Ex. 50) at 2.

DENIED as misleading and incomplete. The same document notes that "FBI leadership repeatedly argued that it was increasingly unable to wiretap terrorists, organized crime, drug dealers, and child sexual abuse and exploitation cases" and that "[l]aw enforcement in the U.S. and abroad pressed hard to prevent widespread public access to E2EE" which would hinder their efforts with respect to those crimes. *See also*, Ex. 1 (Levine Rep.) at 98-99 ("In October 2020, The US Attorney General, the UK Secretary of State, Australian Minister for Home Affairs, New Zealand Minister of Justice, and the Canadian Minister of Public Safety and Emergency Preparedness co-signed a statement on EE2E" which stated, in part, that "End-to-end encryption will simply close a curtain to what happens online, enabling encrypted platforms to become lawless environments where the lack of oversight and visibility into criminal activity emboldens offenders. We oppose privacy measures that fail to address how the internet is used to entice children into sexually exploitive situations and to traffic images and videos of children being raped and sexually abused."); *id*. fn. 369.

b. Meta publicly recognized that the transition to E2EE would create potential safety issues that would be the subject of mitigation efforts. See Ex. B (NCOSE Dep. Ex. 46) at 14 ("acknowledg[ing] the 'possible risk of use of e2ee to facilitate the trafficking of adults and children, to share CSAM, or to plan terrorist attacks unless these risks are mitigated (in many of the ways we explain in this paper)").

DENIED as misleading and incomplete. The cited document establishes that "the transition to E2EE" would create only "potential" or "possible" risks rather than actual and known "safety issues" (*see* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded,

And Its Platforms Did in Fact Become Less Safe), or that those risks could be mitigated as effectively once E2EE was fully implemented. *Id*; Ex. 1 (Levine Rep.) at 98 ("The adoption of end-to-end encryption would significantly hamper the efficacy of PhotoDNA. This is particularly troubling given that the majority of the millions of yearly Facebook reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world") (quoting Professor Hany Farid, a noted child safety expert and inventor of PhotoDNA); *id*. at 97 ("The use of end-to-end encryption" will "prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.") (quoting NCMEC); *see also* Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals.").

c. Meta put a number of safety measures in place over the course of several years before rolling out E2EE to promote the safety of its platforms and to ensure that Meta would continue to be able to detect and report child sexual exploitation after implementation of E2EE. See Ex. A (Wirth Report) at 23 n.43.

DENIED as misleading and incomplete to the extent that the cited materials establish that "Meta would continue to be able to detect and report child sexual exploitation" to the same extent "after implementation of E2EE." *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe), or that those risks could be mitigated as effectively once E2EE was fully implemented; Ex. 1 (Levine Rep.) at 98 ("The adoption of end-to-end encryption would significantly hamper the efficacy of PhotoDNA. This is particularly troubling given that the majority of the millions of yearly Facebook reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world") (quoting Professor Hany Farid, a noted child safety expert and inventor of PhotoDNA); *id*. at 97 ("The use of end-to-end encryption" will "prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this

solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.") (quoting NCMEC); *see also* Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals.").

Meta's practices are fully in line with industry best practices, and in many cases exceed them. *Id*. at 14-15.

DENIED as misleading and incomplete. *See* Ex. 4 (Starr Rep.) at ¶ 11 ("there is no universally accepted 'industry standard' governing what specifically a technology company should do to combat online child safety harms"); *compare* Ex. 7 (McCoy Rep.) at 6 ("Extensive internal documentation and correspondence demonstrates that Meta often stalled in fixing known integrity and safety issues until sufficient public and regulatory pressure had accumulated, and only then deploy watered-down or minimal integrity and safety interventions and, even then, often with what appears to be an eye towards forestalling significant impacts to financial metrics or blunting proposed external regulatory measures."); Ex. 1 (Levine Rep.) at 23 ("Meta's policies, statements, and operational practices … merely [follow] widely used practices of tech companies.… In my training and in my field, the security, safety, and privacy of systems that are designed to protect either people or data are not evaluated by the intentions of the owners; what matters is an evaluation of the actual harms observed."); *id*. at 115-116 (noting that "Snap, the owner of Snapchat; and TikTok said their companies took the opposite approach of Meta" on important issues; neither company has enabled E2EE by default for direct messages.); *id*. at 7-8 ("Nothing has changed the nature and prevalence of CSAM- and CSEC-related crimes more than the internet" and "Meta's platforms have played and currently play a key role in that change, as demonstrated by the many tens of millions of CyberTips reported to the National Center for Missing and Exploited Children (NCMEC) and law enforcement, and an untold additional number that have gone unreported or undetected.… [M]eta's platforms are in a distinctly different class of services, as their goal is to 'help people connect,'" meaning "Meta's users are not limited to CSAM file sharing" but "can also connect with others who are interested in CSAM/CSEC"; "Meta has a strong history of proactively recommending content and accounts related to CSAM/CSEC to its users"; and when "communities of adults interested in child sexual exploitation form, they have a unique internet-based opportunity to normalize their interests, train each other on how to groom children to sexual abuse and evade law enforcement, trade CSAM, connect on other venues, and create child sex trafficking markets.")

d. Before Meta rolled out E2EE on Facebook Messenger, it implemented multiple ways to continue to detect violations of its child sexual abuse policies without scanning the content of messages. *See* Ex. A (Wirth Rep.) at 23 n.43; *see also* Ex. D (Zuckerberg Dep.) at 127:15-21 (Q. "Did Meta work to have systems that would maintain the safety of its users as it moved towards end-to-end encryption on Messenger in 2023?" A. "Absolutely. I mean, that's a large part of the reason why it took so long to implement this.").

DENIED as misleading and incomplete to the extent that the cited materials establish that Meta "maintain[ed] the safety of its users" at to the same extent or degree of efficacy after its implementation of E2EE, or that the amount of time that elapsed between announcing E2EE by default, and implementing it, meant Meta "maintain[ed] the safety of its users" at to the same extent after its implementation of E2EE. *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe), or that those risks could be mitigated as effectively once E2EE was fully implemented; Ex. 1 (Levine Rep.) at 98 ("The adoption of end-to-end encryption would significantly hamper the efficacy of PhotoDNA. This is particularly troubling given that the majority of the millions of yearly Facebook reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world") (quoting Professor Hany Farid, a noted child safety expert and inventor of PhotoDNA); *id*. at 97 ("The use of end-to-end encryption" will "prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.") (quoting NCMEC); *see also* Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals.").

e. For example, when Meta announced default E2EE on Messenger, it also announced that it would "use a variety of tools, including artificial intelligence . . . to proactively detect accounts engaged in malicious patterns of behavior instead of scanning private messages." Ex. B (NCOSE Dep. Ex. 46) at 14.

ADMITTED.

Meta implemented "60 different signals to find and label accounts belonging to potentially suspicious adults" that Meta could use to "restrict these accounts from finding, following or interacting with teens," and "from interacting with one another and building abusive networks." *Id*. at 16.

ADMITTED.

These signals can include "blocking, reporting, . . . the content and metadata" Meta can view on its public services, "as well as group names, group photos, and metadata [Meta has] from Messenger and Instagram [direct messages], including those where conversations are end-to-end encrypted." *Id*. at 16.

ADMITTED.

Additionally, Meta made "it much easier to report harm . . . by redesigning [its] reporting feature to be more prominent in Messenger and Instagram" direct messages. *Id*. at 29.

DENIED as incomplete and misleading to the extent that it omits that Meta had, only months before, intentionally reduced users' ability to report harmful content and conduct, including on its direct message surfaces Messenger and Instagram Direct. *See* Ex. 5 METANMAG-059-00001065 at -72 (internal Meta presentation regarding "Messenger, Instagram Direct, and WhatsApp Enforcement Summary" that noted "[r]eactive enforcement depends on review of reports," but that "[c]urrent resource constraints allow for review of just over half of submitted reports," and that "[i]ncreased reporting friction designed to limit inflow" had been designed into Messenger and Instagram Direct: "[w]e have deliberately added steps and difficulty to reporting flow to reduce the overall number" because "[f]rictionless reporting would require 50-100x current review capacity."); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution" and detailing NCMEC's "overall concern that Meta's reporting to the CyberTipline has taken the appearance of a compliance exercise, rather than a crucial child protection mission to ensure children are safe from exploitation on its platforms."); Ex. 1 (Levine Rep.) at 106 ("[A] May 2022 presentation entitled, 'Child Safety on Messenger'" noted that "Over 80% of CSAM reported by FB [Facebook] is from MSGR [Messenger]. [redacted] And with e2ee coming, an enforcement model which relies on finding bad content and bad actors after the harm is done is not enough … Most of what's shared in MSGR are new images for which we have no hash set and it's only after our CEI proactive detection catches it or it's posted somewhere on our public platform and someone reports it that it's possible for us to bank the image, run detection across threads and find that hundreds or thousands of copies have already been distributed via MSGR… High

Level Takeaway: Our current strategy focused on detection and enforcement is not working well today, and will slowly stop working as we move towards E2EE.").

f. These tools permit the detection and prevention of child sexual exploitation following the shift to default E2EE because they focus on the "public-facing surfaces" on Meta's services. *See* Ex. B (NCOSE Dep. Ex. 46) at 14, 16; *see also* Ex. E (Starr Report) ¶¶ 34-35 (explaining that "Meta's rollout of default E2EE has been measured and intentional, prioritizing safety alongside privacy" and that Meta "implement[ed] a suite of detection efforts and interventions specifically designed to work within E2EE environments, including Child Safety – Actor Behavior Framework (CS-ABF), and other advanced classifiers").

DENIED as misleading and incomplete because Meta knew it had no choice other than to "focus on the 'public-facing surfaces' [of] Meta's services" following the implementation of default E2EE, despite years-long internal knowledge that it was its direct-message surfaces—which are not public surfaces—served as the conduit for the vast majority of the CSAM on its platform. *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe); Ex. 1 (Levine Rep.) at 29 ("Once [E2EE was] enacted, Meta would no longer be able to detect CSAM, CSEC, or any other type of violating content based on scanning content from users, whether text or images."); *id*. at 10 ("When Meta offers end-to-end encrypted (E2EE) connections that prevent it from viewing its users' contents and reporting abuse, it's because they have decided to do so."); *id*. at 105 ("In 2019, Messenger was responsible for over 80% of all reports of child sexual exploitation made by Facebook… Given the regulatory environment linked to our e2ee announcement... launching products without child safety mitigations plays into accusations that we are abandoning children to black boxes of abuse."); *id*. at 106 ("[A] May 2022 presentation entitled, 'Child Safety on Messenger'" noted that "Over 80% of CSAM reported by FB [Facebook] is from MSGR [Messenger]. [redacted]. And with e2ee coming, an enforcement model which relies on finding bad content and bad actors after the harm is done is not enough … Most of what's shared in MSGR are new images for which we have no hash set and it's only after our CEI proactive detection catches it or it's posted somewhere on our public platform and someone reports it that it's possible for us to bank the image, run detection across threads and find that hundreds or thousands of copies have already been distributed via MSGR… High Level Takeaway: Our current strategy focused on detection and enforcement is not working well today, and will slowly stop working as we move towards E2EE."); *see also, e.g.*, Ex. 6 METANMAG-158-00000001 (showing that Meta made 2,004 NCMEC reports during the roughly seven and a half months between May 12, 2023 and December 31, 2023, prior to the full rollout of E2EE for Messenger. Of those reports, 1,211—or more than 60%—originated from Messenger messages. The filter for the 2,004 figure is Date Sent < 1/1/2024; the

filter for the 1,211 figure is Date Sent < 1/1/2024 and Sharepoint = Messenger_Thread).

These tools allow Meta to identify and stop bad actors by detecting patterns of activities on these same "public-facing surfaces." See Ex. B (NCOSE Dep. Ex. 46) at 14, 16.

DENIED as misleading and incomplete because Meta cannot know whether it has "identif[ied] and stop[ped] bad actors" solely using data from its "public-facing surfaces." *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe); Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals."); Ex. 1 (Levine Rep.) at 98 (NCMEC describing how implementation of E2EE means "a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse"); *id*. at 100 (Canadian Centre for Child Protection's executive director noting that it " is a dereliction of [Meta's] ethical and moral duty of care to society to knowingly bring about changes to their platform, knowing full well that the net effect will be to mask and provide plausible deniability over a problem they have failed to contain over the years.").

g. Meta has invested and continues to invest in these safety features on its platforms, including Instagram. *See* Ex. A (Wirth Report) at 14 ("[A]s of this past year, between 97% and 99% of the CSAM content Meta takes action against is found by Meta's proactive detection systems and removed before any user reports it.").

DENIED as incomplete and misleading because the cited Meta CSER reports regarding the prevalence of CSAM on its platforms are themselves incomplete and misleading. *See* Ex. 7 (McCoy Rep.) at 68-73; Ex. 8 (Lee Dep.) at 457:22–458:1 (former Meta senior safety researcher Dr. Alison Lee: "what they were sharing in their CSER report was an –a deliberately incomplete picture in an underreporting of the rate of harmful content and experiences that were happening on our platform."); *id*. 458:17-22 ("I think by underreporting and diminishing the findings that were leaked, and underreporting the prevalence of that, that they prevented the public from understanding the rate and severity of the risks that are associated with being on the platform, particularly for young people."); Ex. 3 (Levine Dep.) 142:18-143:6 ("If I look at the number of reports to NCMEC from Meta Platforms of known child sexual abuse material, that number is so large that it is not just an accidental click, it is not an accidental upload. It seems to me a lot of people who are motivated to try again and again and again to upload known content, those computational methods, and Meta talks about this, sometimes the items were

published and then they learned they were CSAM and that generated a report. So not all of the reports are due to Meta catching it before it was published.")

h. The State's child safety expert testified that he did not evaluate whether Meta's newly developed methods to moderate content without scanning the content of messages were effective. *See* Ex. F (Levine Dep.) at 223:7-14 ("Q. And did you evaluate whether those enhancements . . . led to positive improvements that didn't require scanning of content? . . . A. I didn't have an opportunity to evaluate that."). The State's expert did not evaluate these changes at all, despite the fact that the summary of these changes, attached hereto as Exhibit B, was public and produced to the State in discovery. *See id*. 230:14-22.

DENIED as incomplete and misleading because NCMEC *itself* evaluated and discounted the purported reasons for the sharp drop in Cybertip reports from Meta after it implemented E2EE by default, and NCMEC *itself* concluded that the "likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)." Exhibit 38 to Austin Decl. in Support of Plaintiffs Opening Brief (March 11, 2025 Testimony of Michelle DeLaune, President and CEO NCMEC, before United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism) at 11; Ex. 1 (Levine Rep.) at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all

companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation."); Ex. 3 (Levine Dep.) 142:18-143:6 ("If I look at the number of reports to NCMEC from Meta Platforms of known child sexual abuse material, that number is so large that it is not just an accidental click, it is not an accidental upload. It seems to me a lot of people who are motivated to try again and again and again to upload known content, those computational methods, and Meta talks about this, sometimes the items were published and then they learned they were CSAM and that generated a report. So not all of the reports are due to Meta catching it before it was published."); *see also, e.g.*, Ex. 6 METANMAG-158-00000001 (showing that Meta made 2,004 NCMEC reports during the roughly seven and a half months between May 12, 2023 and December 31, 2023, prior to the full rollout of E2EE for Messenger. Of those reports, 1,211—or more than 60%—originated from Messenger messages. The filter for the 2,004 figure is Date Sent < 1/1/2024; the filter for the 1,211 figure is Date Sent < 1/1/2024 and Sharepoint = Messenger_Thread).

2. The State asserts that Meta "mispresent[ed] the safety of its platforms with the implementation of" E2EE. Mot. 1. This is a disputed issue of fact. Meta did not misrepresent the safety of its services when rolling out E2EE.

    a. Meta put a number of safety measures in place over the course of several years before rolling out E2EE encryption to ensure it maintained its ability to remove CSAM from its services, which are fully in line with or exceed industry best practices. *See* supra ¶ 1(b)-(e).

    DENIED as misleading and incomplete. *See* Ex. 4 (Starr Rep.) at ¶ 11 ("there is no universally accepted 'industry standard' governing what specifically a technology company should do to combat online child safety harms"); *compare* Ex. 7 (McCoy Rep.) at 6 ("Extensive internal documentation and correspondence demonstrates that Meta often stalled in fixing known integrity and safety issues until sufficient public and regulatory pressure had accumulated, and only then deploy watered-down or minimal integrity and safety interventions and, even then, often with what appears to be an eye towards forestalling significant impacts to financial metrics or blunting proposed external regulatory measures."); Ex. 1 (Levine Rep.) at 23 ("Meta's policies, statements, and operational practices … merely [follow] widely used practices of tech companies.… In my training and in my field, the security, safety, and privacy of systems that are designed to protect either people or data are not evaluated by the intentions of the owners; what matters is an evaluation of the

actual harms observed."); *id*. at 115-116 (noting that "Snap, the owner of Snapchat; and TikTok said their companies took the opposite approach of Meta" on important issues; neither company has enabled E2EE by default for direct messages.); *id*. at 7-8 ("Nothing has changed the nature and prevalence of CSAM- and CSEC-related crimes more than the internet" and "Meta's platforms have played and currently play a key role in that change, as demonstrated by the many tens of millions of CyberTips reported to the National Center for Missing and Exploited Children (NCMEC) and law enforcement, and an untold additional number that have gone unreported or undetected.… [M]eta's platforms are in a distinctly different class of services, as their goal is to 'help people connect,'" meaning "Meta's users are not limited to CSAM file sharing" but "can also connect with others who are interested in CSAM/CSEC"; "Meta has a strong history of proactively recommending content and accounts related to CSAM/CSEC to its users"; and when "communities of adults interested in child sexual exploitation form, they have a unique internet-based opportunity to normalize their interests, train each other on how to groom children to sexual abuse and evade law enforcement, trade CSAM, connect on other venues, and create child sex trafficking markets.")

b. Meta also provided the public with information about these safety measures. *See*, *e.g.*, Ex. G (Loredana Crisan, Launching Default End-to-End Encryption on Messenger, Meta Newsroom (2023), https://about.fb.com/news/2023/12/default-end-to-end- encryption-on-messenger/t_) ("We've introduced new privacy, safety and control features along the way like delivery controls that let people choose who can message them, as well as app lock, alongside existing safety features like report, block and message requests. 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 also* Ex. B (NCOSE Dep. Ex. 46).

ADMITTED to the extent these quotes were included in documents made publicly available by Meta. **DENIED** as incomplete to the extent that the cited materials establish that these "safety features" would allow Meta to continue to be able to detect and report child sexual exploitation to the same extent after implementation of E2EE. *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe), or that those risks could be mitigated as effectively once E2EE was fully implemented; Ex. 1 (Levine Rep.) at 98 ("The adoption of end-to-end encryption would significantly hamper the efficacy of PhotoDNA. This is particularly troubling given that the majority of the millions of yearly Facebook reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world") (quoting Professor Hany Farid, a noted child safety expert and inventor of PhotoDNA); *id*. at 97 ("The use of end-to-end encryption" will "prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve

online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.") (quoting NCMEC); *see also* Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals.").

c. Meta published a "White Paper" prior to rolling out default E2EE on Facebook Messenger explaining how E2EE would change how Meta detects and removes child sexual abuse material ("CSAM"). Ex. B (NCOSE Dep. Ex. 46); see supra ¶ 1(c).

ADMITTED.

This White Paper also explicitly acknowledged the "possible risk of use of e2ee to facilitate the trafficking of adults and children, to share CSAM, or to plan terrorist attacks unless these risks are mitigated (in many of the ways we explain in this paper)." Ex. B (NCOSE Dep. Ex. 46) at 14 (emphasis added).

ADMITTED to the extent these quoted material is included in the cited document. **DENIED** as misleading and incomplete to the extent that the cited materials establish that the described risks could be "mitigated" to the same extent after implementation of E2EE. *See* Opening Br. § III ("Meta Knew E2EE Would Make its Platforms Less Safe, Its Mitigations Were Inadequate and Underfunded, And Its Platforms Did in Fact Become Less Safe). Ex. 1 (Levine Rep.) at 98 ("The adoption of end-to-end encryption would significantly hamper the efficacy of PhotoDNA. This is particularly troubling given that the majority of the millions of yearly Facebook reports to NCMEC's CyberTipline originate on Facebook's Messaging services. Blindly implementing end-to-end encryption will significantly increase the risk and harm to children around the world") (quoting Professor Hany Farid, a noted child safety expert and inventor of PhotoDNA); *id*. at 97 ("The use of end-to-end encryption" will "prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.") (quoting NCMEC); *see also* Ex. 3 (Levine Dep.) 229:12-18 ("nothing beats a cryptographic match to known CSAM that [was] observable on content" prior to implementation of E2EE, and "given the evasion techniques that are trivial and yet undetected by Meta that we talked about before, they are really

tying a hand behind their back here to go with these really light signals" to detect CSAM that they would be forced to rely on post-implementation of E2EE.); *id*. 231:16-18 ("examining content ... will lend you a much higher accuracy than examining subtle signals.").

3. The State asserts that Meta's reports to NCMEC were "missing a vital piece of data used by law enforcement." Mot. 8. This is a disputed issue of fact.

   a. Meta's reporting systems are designed to include robust information in its reports to NCMEC. Ex. E (Starr Report) ¶ 31 (citation omitted).

   DENIED as misleading because NCMEC itself has for years alerted Meta about widespread deficiencies in Meta's reporting. *See generally* Ex. 1 (Levine Rep.) at 113-118 ("5.1.9 Meta makes it difficult for users to report content and for law enforcement to respond"); *id*. at 118 (2024 report that Meta is "delaying the process of rescuing children by not examining the content of CSAM ahead of sending CyberTips to NCMEC" meaning "law enforcement … cannot view it or open [report] without first serving legal process on the [social media company]'" and that Meta has "slashed jobs from their teams responsible for moderation" resulting in "fewer reports of child abuse material being reviewed by humans at the companies, placing an even more significant burden on law enforcement as the potential number of search warrants needed increases"); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution."); Ex. 9 METANMAG-007-00020093 (2019 NCMEC CyberTipline Report on Facebook and Instagram that notes "submitted reports do not contain enough context or pertinent information to be actioned by law enforcement"; that inactionable reports caused NCMEC "CyberTipline analysts [to] spend a disproportionate amount of time identifying and manually processing these reports" which "takes time away from processing actionable, high valuable reports"and affects law enforcement's "triaging and takes time away from processing actionable reports.").

   Meta continues to work with law enforcement to prevent child exploitation, terrorism, and extortion whenever possible. *See* Ex. A (Wirth Report) at 16 n.23 ("Meta's Law Enforcement Response Team works 24/7 to respond to emergency data requests, including imminent harm cases involving children. . . . The company provides a dedicated portal for law enforcement to submit requests and has trained legal personnel to ensure speedy cooperation in child exploitation cases.").

   ADMITTED to the extent Meta has worked with law enforcement. **DENIED** as misleading and incomplete because NCMEC itself has for years alerted Meta about widespread deficiencies in Meta's conduct and consequences for law enforcement's ability to effectively thwart child exploitation. *See generally* Ex. 1 (Levine Rep.) at 113-118 ("5.1.9 Meta makes it difficult for users to report content

and for law enforcement to respond"); Ex. 7 (McCoy Rep.) at 6 ("Extensive internal documentation and correspondence demonstrates that Meta often stalled in fixing known integrity and safety issues until sufficient public and regulatory pressure had accumulated, and only then deploy watered-down or minimal integrity and safety interventions and, even then, often with what appears to be an eye towards forestalling significant impacts to financial metrics or blunting proposed external regulatory measures."); Ex. 1 (Levine Rep.) at 118 (2024 report that Meta is "delaying the process of rescuing children by not examining the content of CSAM ahead of sending CyberTips to NCMEC" meaning "law enforcement … cannot view it or open [report] without first serving legal process on the [social media company]'" and that Meta has "slashed jobs from their teams responsible for moderation" resulting in "fewer reports of child abuse material being reviewed by humans at the companies, placing an even more significant burden on law enforcement as the potential number of search warrants needed increases"); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution."); Ex. 9 METANMAG-007-00020093 (2019 NCMEC CyberTipline Report on Facebook and Instagram that notes "submitted reports do not contain enough context or pertinent information to be actioned by law enforcement"; that inactionable reports caused NCMEC "CyberTipline analysts [to] spend a disproportionate amount of time identifying and manually processing these reports" which "takes time away from processing actionable, high valuable reports"and affects law enforcement's "triaging and takes time away from processing actionable reports.").

b. As Meta's child safety expert opines, "Meta maintains an ongoing and productive partnership with NCMEC . . . sharing high-quality, actionable reports. . . . Although, neither NCMEC nor the law specifies precisely which fields must be included in ESP reports, Meta invests in specialized analysts who review reports and compile tags . . . to help NCMEC and law enforcement process and prioritize reports."). Ex. E (Starr Report) ¶ 31 (citation omitted).

ADMITTED to the extent Meta has an ongoing relationship with NCMEC. **DENIED** as misleading because NCMEC itself has for years criticized Meta about widespread deficiencies in Meta's conduct and consequences for law enforcement's ability to effectively thwart child exploitation. *See generally* Ex. 1 (Levine Rep.) at 113-118 ("5.1.9 Meta makes it difficult for users to report content and for law enforcement to respond"); Ex. 7 (McCoy Rep.) at 6 ("Extensive internal documentation and correspondence demonstrates that Meta often stalled in fixing known integrity and safety issues until sufficient public and regulatory pressure had accumulated, and only then deploy watered-down or minimal integrity and safety interventions and, even then, often with what appears to be an eye towards forestalling significant impacts to financial metrics or blunting proposed external regulatory measures."); Ex. 1 (Levine Rep.) at 118 (2024 report that Meta is "delaying the process of rescuing children by not examining the content of CSAM

ahead of sending CyberTips to NCMEC" meaning "law enforcement … cannot view it or open [report] without first serving legal process on the [social media company]'" and that Meta has "slashed jobs from their teams responsible for moderation" resulting in "fewer reports of child abuse material being reviewed by humans at the companies, placing an even more significant burden on law enforcement as the potential number of search warrants needed increases"); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution."); Ex. 9 METANMAG-007-00020093 (2019 NCMEC CyberTipline Report on Facebook and Instagram that notes "submitted reports do not contain enough context or pertinent information to be actioned by law enforcement"; that inactionable reports caused NCMEC "CyberTipline analysts [to] spend a disproportionate amount of time identifying and manually processing these reports" which "takes time away from processing actionable, high valuable reports"and affects law enforcement's "triaging and takes time away from processing actionable reports.").

4. The State asserts that, since moving to E2EE on Facebook Messenger, "NCMEC observed a decline in both the quantity and quality of Meta's CyberTipline reports." Mot. 9. This is a disputed issue of fact.

   a. Meta is the largest contributor of CSAM hashes to NCMEC. *See* Ex. E (Starr Report) ¶ 31.

      DENIED. The cited paragraph of the Starr Report does not assert that "Meta is the largest contributor of CSAM hashes to NCMEC."

      Meta has continued to enhance its reporting systems, which have improved both the volume and quality of reports. *See* supra ¶ 1(f).

      DENIED as misleading because NCMEC itself has for years alerted Meta about widespread deficiencies in Meta's reporting. *See generally* Ex. 1 (Levine Rep.) at 113-118 ("5.1.9 Meta makes it difficult for users to report content and for law enforcement to respond"); *id*. at 118 (2024 report that Meta is "delaying the process of rescuing children by not examining the content of CSAM ahead of sending CyberTips to NCMEC" meaning "law enforcement … cannot view it or open [report] without first serving legal process on the [social media company]'" and that Meta has "slashed jobs from their teams responsible for moderation" resulting in "fewer reports of child abuse material being reviewed by humans at the companies, placing an even more significant burden on law enforcement as the potential number of search warrants needed increases"); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution."); Ex. 9 METANMAG-007-00020093 (2019 NCMEC

CyberTipline Report on Facebook and Instagram that notes "submitted reports do not contain enough context or pertinent information to be actioned by law enforcement"; that inactionable reports caused NCMEC "CyberTipline analysts [to] spend a disproportionate amount of time identifying and manually processing these reports" which "takes time away from processing actionable, high valuable reports"and affects law enforcement's "triaging and takes time away from processing actionable reports.").

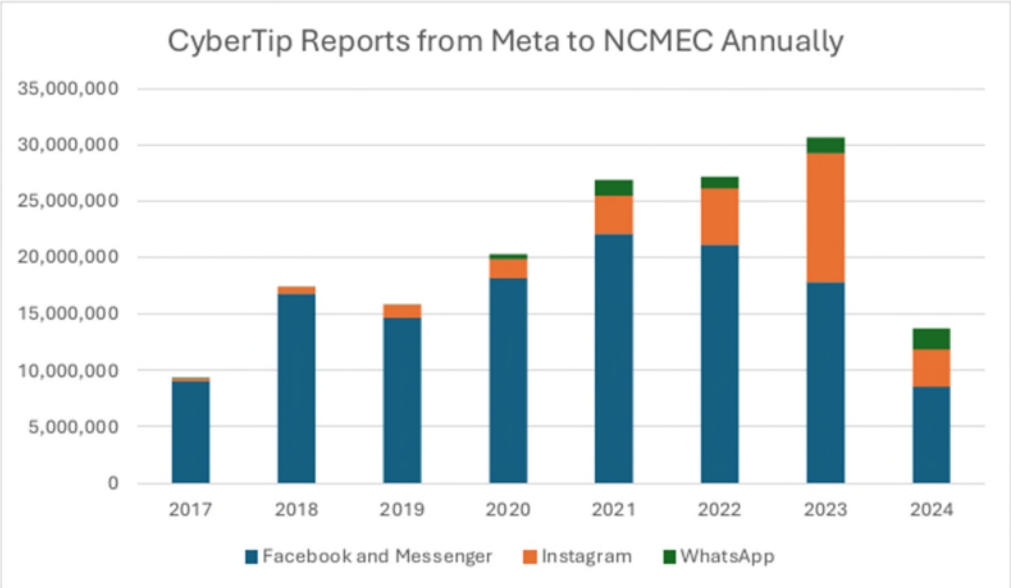
b. The evidence does not support the assertion that E2EE is the reason that Meta's reports to NCMEC declined in 2024. Meta rolled out E2EE on Facebook Messenger in December 2023. Ex. G (Loredana Crisan, Launching Default End-to-End Encryption on Messenger, Meta Newsroom (2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/t_).

DENIED as incomplete and misleading because NCMEC *itself* evaluated and discounted the purported reasons for the sharp drop in Cybertip reports from Meta after it implemented E2EE by default, and NCMEC *itself* concluded that the "likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)." Exhibit 38 to Austin Decl. in Support of Plaintiffs Opening Brief (March 11, 2025 Testimony of Michelle DeLaune, President and CEO NCMEC, before United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism) at 11; Ex. 1 (Levine Rep.) at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse

will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation."); Ex. 38 to the B. Austin Declaration (March 2022 letter to Meta from NCMEC's General Counsel about "Widespread Flaws in Meta's Reporting to the CyberTipline," asserting that "Meta's poor reporting practices have become a hindrance to child safety, rather than a solution.")

But from 2021 to 2023—before Meta rolled out E2EE—Meta's NCMEC reports also dropped consistently year-over-year. See Ex. H (Levine Report) at 97.

DENIED as false because neither the cited page of Dr. Levine's report nor the underlying NCMEC data show that "Meta's NCMEC reports also dropped consistently" "from 2021 to 2023." Ex. 1 (Levine Rep.) at 97 (graph reproduced below, showing increase both in number of NCMEC reports from Instagram and Meta overall between 2021-2023):



See also Ex. 10 (Wirth Report Ex. A) at "2021 CyberTipline Reports by Electronic Service Providers (ESP)" showing **26,885,302** reports by Meta in 2021 (Facebook: 22,118,952 + Instagram 3,393,654 + WhatsApp 1,372,696); *id*. at "2022 CyberTipline Reports by Electronic Service Providers (ESP)" showing **27,190,665**

reports by Meta in 2022 (Facebook: 21,165,208 + Instagram 5,007,902 + WhatsApp 1,017,555); and *id*. at "2023 CyberTipline Reports by Electronic Service Providers (ESP)" showing **30,658,047** reports by Meta in 2023 (Facebook: 17,838,422 + Instagram 11,430,007 + WhatsApp 1,389,618).

The State's expert, who opines that Meta's reporting to NCMEC dropped because of its implementation of E2EE on Facebook Messenger, testified that he did not know what caused the consistent drops in NCMEC reports. Ex. 3 (Levine Dep.) at 244:2-8 (Q. "You did not evaluate the reasons for the decline in NCMEC reports on Facebook Messenger between 2021 and 2023? A. I think you are right that I didn't have the opportunity to evaluate that precisely.").

DENIED as incomplete and misleading because NCMEC *itself* evaluated and discounted the purported reasons for the sharp drop in Cybertip reports from Meta after it implemented E2EE by default, and NCMEC *itself* concluded that the "likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)." *See* Exhibit 38 to Austin Decl. in Support of Plaintiffs Opening Brief (March 11, 2025 Testimony of Michelle DeLaune, President and CEO NCMEC, before United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism) at 11; Ex. 1 (Levine Rep.) at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all

companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation."); *see also, e.g.*, Ex. 6 METANMAG-158-00000001 (showing that Meta made 2,004 NCMEC reports during the roughly seven and a half months between May 12, 2023 and December 31, 2023, prior to the full rollout of E2EE for Messenger. Of those reports, 1,211—or more than 60%—originated from Messenger messages. The filter for the 2,004 figure is Date Sent < 1/1/2024; the filter for the 1,211 figure is Date Sent < 1/1/2024 and Sharepoint = Messenger_Thread).

He also acknowledged that reports to NCMEC by Instagram in 2024 declined by a larger percentage than Facebook's reports, even though Instagram had not implemented E2EE, *id*. at 256:3-9, and that overall reporting to NCMEC by the entire industry declined in 2024. *Id*. at 247:10-21.

DENIED as incomplete and misleading because while Meta had not "not implemented E2EE" *by default* as of 2024, E2EE was nevertheless available on Instagram during this time period. *See* Austin Decl. ¶ 4 ("Meta launched optional E2EE for personal chats on Instagram Direct (IGD) globally starting in the first quarter of 2023."); Ex. 1 (Levine Rep.) at 18-19 ("In 2023, Meta deployed end-to-end encryption for Messenger by default and has stated that it is committed to deploying E2EE for Instagram Direct by default. (E2EE communications is available on both apps, but in Instagram, the user has to enable it before it is active, thus it is not "by default".); *id*. fn. 63 ("Direct messages on Instagram also will shift to such encryption by default somewhat later, likely in the new year, according to people familiar with the matter"; "Meta refreshes promise to roll out default end-to-end encryption in Messenger this year. Protection for Instagram will come shortly after"; "We remain committed to rolling our default end-to-end encryption for private conversations on Messenger in 2023, and shortly afterwards for Instagram,'[Meta's deputy privacy officer, Rob] Sherman wrote.").

He also recognized that Meta had adopted bundled reporting to NCMEC in 2024, which necessarily reduced its total reports to NCMEC. *Id*. at 253:16-22.

DENIED as incomplete and misleading because NCMEC itself accounted for the "bundled reporting" and nevertheless concluded that "the likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)," (Ex. 1 (Levine

Rep.) at 98), which Dr. Levine noted at his deposition. Ex. 3 (Levine Dep.) 254:1-24.

These factors all contradict the suggestion that E2EE caused the decline in Meta's NCMEC reports for Facebook.

DENIED as incomplete and misleading because NCMEC *itself* evaluated and discounted the purported reasons for the sharp drop in Cybertip reports from Meta after it implemented E2EE by default, and NCMEC *itself* concluded that the "likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)." See Exhibit 38 to Austin Decl. in Support of Plaintiffs Opening Brief (March 11, 2025 Testimony of Michelle DeLaune, President and CEO NCMEC, before United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism) at 11; Ex. 1 (Levine Rep.) at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified

multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation.").

c. NCMEC reporting declined industry-wide during the period of E2EE roll out.

ADMITTED.

NCMEC began batching reports in this same period and reports declined on both Meta's encrypted and unencrypted surfaces. *See* Ex. E (Starr Report) ¶ 36.

DENIED as incomplete and misleading because NCMEC *itself* accounted for the "bundled reporting" and other factors noted in Starr Report ¶ 36 and nevertheless concluded that "the likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)," (Ex. 1 (Levine Rep.) at 98) ("Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023… While [these] factors likely contributed to the decrease, the likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end- to-end encryption (E2EE)"), which Dr. Levine noted at his deposition. Ex. 3 (Levine Dep.) 254:1-24.

d. Any perceived decline of Meta's reports may be due to changes in platform usage or volume of violative content, not a reduction in Meta's reporting. *See* Ex. E (Starr Report) ¶ 36 ("While NMAG's experts speculate that default E2EE reduced Meta's reports to NCMEC, their analysis is unable to demonstrate a clear causal link. NMAG experts oversimplify and ignore several variables that led to the decline in NCMEC reporting, including NCMEC's implementation — and Meta's adoption of — bundling, the removal of meme content that was previously reported as CSAM, and general declines in reporting across several platforms, as well as declines in reports from the public.") (citations omitted).

DENIED as incomplete and misleading because NCMEC *itself* accounted for the "bundled reporting" other factors noted in Starr Report ¶ 36 and nevertheless concluded that "the likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE)," (Ex. 1 (Levine Rep.) at 98) ("Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023… While [these] factors likely contributed to the decrease, the likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end- to-end encryption (E2EE)"), which Dr. Levine noted at his deposition. Ex. 3 (Levine Dep.) 254:1-24.

5. The State asserts that "NCMEC testified . . . that Meta was failing to detect and report child sexual exploitation." Mot. 9. This is a disputed issue of fact.

   a. It is incorrect that NCMEC said Meta "was failing to detect and report child sexual exploitation." Mot. 9 (emphasis added). Instead, NCMEC merely agreed that it believed Meta left certain unspecified and unidentified "cases of child exploitation undetected and unreported." State Ex. 35 at 159:6-9.

      DENIED as incomplete and misleading. NCMEC's deposition excerpt is only one of many instances where NCMEC has made statements indicating Meta's deficient detection and reporting. *See, e.g.*, Ex. 1 (Levine Rep.) at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation."); *id*. at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024.366 Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); Ex. 3

(Levine Dep.) 142:18-143:6 ("If I look at the number of reports to NCMEC from Meta Platforms of known child sexual abuse material, that number is so large that it is not just an accidental click, it is not an accidental upload. It seems to me a lot of people who are motivated to try again and again and again to upload known content, those computational methods, and Meta talks about this, sometimes the items were published and then they learned they were CSAM and that generated a report. So not all of the reports are due to Meta catching it before it was published."); *see also, e.g.*, Ex. 6 METANMAG-158-00000001 (showing that Meta made 2,004 NCMEC reports during the roughly seven and a half months between May 12, 2023 and December 31, 2023, prior to the full rollout of E2EE for Messenger. Of those reports, 1,211—or more than 60%—originated from Messenger messages. The filter for the 2,004 figure is Date Sent < 1/1/2024; the filter for the 1,211 figure is Date Sent < 1/1/2024 and Sharepoint = Messenger_Thread).

b. Despite NCMEC testimony, Meta has and continues to be the highest per volume NCMEC reporter out of all electronic service providers. See Ex. E (Starr Report) ¶ 31. Once potentially violative content is detected, Meta reports to NCMEC and law enforcement in accordance with law. Ex. B (NCOSE Dep. Ex. 46) at 29.

DENIED as incomplete and misleading. Although Meta "has and continues to be the highest per volume NCMEC reporter," that does not also mean that Meta is not also "failing to detect and report child sexual exploitation." Ex. 1 (Levine Rep.) at 9 ("The large number of CyberTips that Meta has reported to NCMEC is an indication that CSAM- and CSEC-related content and activity is attracting users to the platform."); *id*. at 90 ("At this time [July 2021], CyberTips to NCMEC from Meta were at an all-time high, indicating that the platforms are as popular as ever with persons who sexually exploit children."); *id*. 76-82 ("Meta's CSAM and CSEC Detection Efforts are Inadequate and Mismanaged."); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further

implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE without an exception for detecting child sexual exploitation."); *id*. at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end-to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); Ex. 3 (Levine Dep.) 142:18-143:6 ("If I look at the number of reports to NCMEC from Meta Platforms of known child sexual abuse material, that number is so large that it is not just an accidental click, it is not an accidental upload. It seems to me a lot of people who are motivated to try again and again and again to upload known content, those computational methods, and Meta talks about this, sometimes the items were published and then they learned they were CSAM and that generated a report. So not all of the reports are due to Meta catching it before it was published."); *id*. at 261:9-17 ("If there is a lot of CyberTips, it might mean the company is active. But it also means that so are perpetrators on the platform. If there are no CyberTips filed, or very few, you cannot necessarily, without other information, argue there are no perpetrators on the platform or that they are -- or whether it is the case they are ignoring content on their platform.); *id*. at 261:24-262:16 ("It may mean that they have employed algorithmic methods, but it doesn't mean that they -- for example, in this particular sentence, I said Facebook reported 15.8 million reports to NCMEC. I don't know whether that is 95 percent of the content of Facebook's platform or 1 percent of the content. All I know is just that they made that many reports. So it tells me that perpetrators are active, and it tells me that they have something in place, but I don't know whether they are doing a job good. Nor do I know, similarly, whether companies that don't report or have very few reports have done a good job preventing perpetrators or whether they are just not looking."); *id*. at 263:9-15 ("What it doesn't tell me, I just can't evaluate, is whether they are detecting 1 percent of the activity on their platform or 99 percent of it. We just don't have the information. It also tells me that perpetrators come again and again to attempt it. And that is a strong signal.")

c. Following implementation of E2EE, Meta is still able to report child sexual exploitation to NCMEC. *See supra* ¶¶ 2(b)-(f).

ADMITTED.

d. Meta's expert Mary Wirth explained that she "disagree[d] with NCMEC's position" regarding Meta's implementation of E2EE. Ex. I (Wirth Dep.) at 178-80.

ADMITTED.

Wirth explained in her report that as a result of Meta's ongoing investment in its detection capabilities, it proactively detects and reports more CSAM and files more cyber tips each year than all other ESPs combined. Ex. A (Wirth Report) at 13. In fact, "[i]n every single year from 2020 to 2024, Meta filed more CyberTips with NCMEC than all other service providers combined." *Id*. at 14.

DENIED as incomplete and misleading to the extent that it suggests a higher volume of reporting to NCMEC indicates Meta was not nevertheless failing to detect and report child sexual exploitation or that the volume of its reports serve as any indication of the actual prevalence of child sexual abuse material or Meta's ability to identify any proportion of that material. Despite Ms. Wirth's testimony, the NCMEC documents she cites state that "[h]igher numbers of reports can be indicative of a variety of things," not merely "how robust an ESP's efforts are to identify and remove abusive content," Ex. 10 (Wirth Report Ex. A) at 1; *see also, e.g.*, Ex. 1 (Levine Rep.) at 9 ("The large number of CyberTips that Meta has reported to NCMEC is an indication that CSAM- and CSEC-related content and activity is attracting users to the platform."); *id*. at 90 ("At this time [July 2021], CyberTips to NCMEC from Meta were at an all-time high, indicating that the platforms are as popular as ever with persons who sexually exploit children."); *id*. at 76-82 ("Meta's CSAM and CSEC Detection Efforts are Inadequate and Mismanaged."); *id*. at 97 ("NCMEC's position on E2EE is and has been that '[t]he use of end-to-end encryption would prevent the companies or any third-party from detecting illegal activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children. We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes.'"); *id*. at 97-98 ("In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation [total from all companies]. While this is a significant number, the overall number of reports declined from 36.2 million reports received in 2023.This decline is especially concerning because the REPORT Act, which was enacted in 2024, mandates companies to report two additional forms of child sexual exploitation for the first time –child sex trafficking and online enticement. With additional mandatory reporting, we would have expected increased reporting, but our analysis identified multiple contributing factors to the decline, including a decrease in reports from certain platforms and a decline caused by further implementation of end-to-end encryption (E2EE). NCMEC has long raised concerns about implementing E2EE

without an exception for detecting child sexual exploitation."); *id*. at 98 ("NCMEC has commented on Meta's drop in CyberTip reports in a statement to Congress: '[T]he likeliest factor contributing to the overall drop in reported incidents in 2024, is a result of Facebook's implementation of end- to-end encryption (E2EE). Meta began to implement default E2EE in Facebook Messenger in December 2023 and completed that process in the summer of 2024. Even when NCMEC adjusts for Facebook's bundling and realignment of content it reports to the CyberTipline, the numbers demonstrate that Facebook reported approximately 6.9 million less reports in 2024 than it did in 2023. For years NCMEC has anticipated a negative impact on CyberTipline reporting as more online platforms adopted default E2EE on their platforms without adequate safeguards for child protection. When a platform voluntarily chooses to blind itself to child sexual exploitation by disabling its ability to detect and report abuse, it is not just losing a report –it is potentially losing a child. Every lost report can represent a child who may never be identified, rescued, or safeguarded. It means the child's ongoing abuse and repeated revictimization will continue unchecked, while offenders remain free to exploit more victims in the shadows.'"); Ex. 3 (Levine Dep.) 142:18-143:6 ("If I look at the number of reports to NCMEC from Meta Platforms of known child sexual abuse material, that number is so large that it is not just an accidental click, it is not an accidental upload. It seems to me a lot of people who are motivated to try again and again and again to upload known content, those computational methods, and Meta talks about this, sometimes the items were published and then they learned they were CSAM and that generated a report. So not all of the reports are due to Meta catching it before it was published."); *id*. at 261:9-17 ("If there is a lot of CyberTips, it might mean the company is active. But it also means that so are perpetrators on the platform. If there are no CyberTips filed, or very few, you cannot necessarily, without other information, argue there are no perpetrators on the platform or that they are -- or whether it is the case they are ignoring content on their platform.); *id*. at 261:24-262:16 ("It may mean that they have employed algorithmic methods, but it doesn't mean that they -- for example, in this particular sentence, I said Facebook reported 15.8 million reports to NCMEC. I don't know whether that is 95 percent of the content of Facebook's platform or 1 percent of the content. All I know is just that they made that many reports. So it tells me that perpetrators are active, and it tells me that they have something in place, but I don't know whether they are doing a job good. Nor do I know, similarly, whether companies that don't report or have very few reports have done a good job preventing perpetrators or whether they are just not looking.") *id*. at 263:9-15 ("What it doesn't tell me, I just can't evaluate, is whether they are detecting 1 percent of the activity on their platform or 99 percent of it. We just don't have the information. It also tells me that perpetrators come again and again to attempt it. And that is a strong signal.")

6. The State asserts that "Meta knowingly made false and misleading statements that have the tendency to deceive or mislead New Mexico consumers into the false belief that, to ensure the safety of its platforms, Meta implemented sufficient safety mitigations to address the risks posed by E2EE." Mot. 3 (emphasis added). This is a disputed issue of fact.

a. As Meta's consumer behavior expert has explained, with respect to Meta's alleged misrepresentations, New Mexico has not produced any evidence showing (1) whether Meta's statements on the safety of its platforms reached any citizens of New Mexico and, if so, how many; (2) whether any citizens of New Mexico (and, if so, how many) attended to the alleged misrepresentations; and/or (3) to the extent that any New Mexico citizens received and attended to the alleged misrepresentations, how they interpreted Meta's statements on the safety of its platforms. *See* Ex. J (Novemsky Report).

DENIED as incorrect, misleading and contradicted by record evidence. None of the "facts" in this paragraph are required to establish a "tendency to deceive" as proof of actual reliance is not required to establish the State's claims under the UPA and New Mexico law includes a presumption of materiality for statements regarding safety. *See* Reply at 1, 8-9. Further, Novemsky offers these opinions without having interviewed any residents or advertisers in New Mexico (Ex. 11 (Novemsky Dep.) at 87:19-88:1), without having reviewed any consumer complaints submitted to Meta (*id*. 88:16-89:4), and without performing any analysis as to the number of New Mexico users on its platform (*id*. 89:11-22). Novemsky expressly admitted at his deposition that he could not claim there were no New Mexico residents misled by the at-issue statements (*id*. 97:10-17).

7. The State asserts that "New Mexico consumers engage in an exchange of value with Meta in order to access Meta's platforms." Mot. 9. This is a disputed issue of fact.

a. Meta does not charge users to access its social media apps. See Defendants' Motion for Summary Judgment No. 6 or, in the Alternative, for Partial Summary Judgment for Lack of an Actionable Transaction on the State's Unfair Practices Act Claims (Counts I, II, III).

DENIED as incomplete. Upon signing up for the service, Facebook users enter into an "agreement between [the user] and Meta Platforms, Inc. regarding [the user's] use of [Meta's] Products," pursuant to which Meta "use[s the user's] personal data to help determine which personalized ads to show" the user and "businesses and organizations, and other persons pay [Meta] to show [the user] ads for their products and services." *See* Facebook Terms of Service (Ex. 37 to the B. Austin Declaration). Similarly, Instagram users make roughly the same agreement, pursuant to which the user "acknowledge[s] that Meta can show [the user] ads that businesses and organizations pay [Meta] to promote" and Meta "use[s the user's] personal data, such as information about [the user's] activity and interests" to display targeted advertisements. *See* Instagram Terms of Service (Ex. 39 to the B. Austin Declaration).