OPPS

TAMARA BEATTY PETERSON, ESQ., Bar No. 5218
tpeterson@petersonbaker.com
DAVID E. ASTUR, ESQ., Bar No. 15008
dastur@petersonbaker.com
PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
Telephone: 702.786.1001
Facsimile: 702.786.1002

Attorneys for Defendant Meta Platforms, Inc.

DISTRICT COURT

CLARK COUNTY, NEVADA

STATE OF NEVADA,

Plaintiff,

vs.

META PLATFORMS, INC. f/k/a FACEBOOK, INC.,

Defendant.

Case No.: A-24-886110-B
Dept. No.: 13

OPPOSITION TO STATE OF NEVADA'S MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION ON ORDER SHORTENING TIME

Date of Hearing: February 26, 2024
Time of Hearing: 9:00 A.M.

COMES NOW, Defendant META PLATFORMS, INC. f/k/a FACEBOOK, INC. ("Meta"), by and through its attorneys of record, PETERSON BAKER, PLLC, hereby submits this Opposition to the State of Nevada's ("the State") Motion for Temporary Restraining Order and Preliminary Injunction on Order Shortening Time.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

This Opposition is based on the attached Memorandum of Points and Authorities, any exhibits attached thereto, the pleadings and papers on file here, and any oral argument that may be presented to the Court.

Dated this 21st day of February, 2024.

PETERSON BAKER, PLLC

By: /s/ Tamara Beatty Peterson

TAMARA BEATTY PETERSON, ESQ., Bar No. 5218
tpeterson@petersonbaker.com
DAVID E. ASTUR, ESQ., Bar No. 15008
dastur@petersonbaker.com
701 S. 7th Street
Las Vegas, NV 89101
Telephone: 702.786.1001
Facsimile: 702.786.1002

Attorneys for Defendant Meta Platforms, Inc.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Meta Platforms, Inc. ("Meta")[1] has offered end-to-end encryption ("E2EE") as an option on its Messenger app since 2016. Compl. ¶ 202. E2EE technology is commonplace and has been hailed as "vital" by privacy advocates for protecting users' communications with each other.[2] The only change Meta made in December 2023 was to announce that the Messenger app would transition all messages to E2EE (rather than an option), *id*.—which is what Apple iMessage, Signal and numerous other messaging services already do.

These facts completely disprove the State's assertion that it is entitled to temporary injunctive relief. E2EE has been available as an option on Meta's Messenger app for eight years, and Meta began rolling out E2EE for all messages on Messenger months ago. The State cannot properly assert that it requires emergency injunctive relief—on two days' notice—blocking Meta's use of E2EE, when that feature has been in use on Messenger for years and began to be rolled out for all messages more than two months ago. The State's delay—for years—to bring any enforcement action related to Meta's use of E2EE (or other providers' use of E2EE) demonstrates why its request for the extraordinary relief of a TRO should be denied.

As addressed in more detail below, the motion for TRO should be denied for multiple reasons, summarized here:

- **It is fundamentally unfair and entirely unnecessary to hear this motion on a highly accelerated timetable that has deprived Meta of the opportunity to develop a full and fair response.**

[1] Meta's appearance does not constitute a waiver of its right to object to a lack of personal jurisdiction, and Meta expressly reserves its right to contest personal jurisdiction at a future date. *See Fritz Hansen A/S v. Eighth Judicial Dist. Court*, 116 Nev. 650, 656-57 (2000) (rejecting the "rigid" and "technical differences between general and special appearances" and holding that personal jurisdiction is not waived as long as it is raised in a defendant's first motion to dismiss); *see also Johnson v. Comm'n on Presidential Debates*, 2014 WL 12597805, at *4 (C.D. Cal. Jan. 6, 2014) (jurisdiction not waived when defendant filed a response to a TRO application four days after complaint was filed and specifically noted that it reserved the right to contest personal jurisdiction, then timely raised the personal jurisdiction issue in its first motion to dismiss).

[2] *See, e.g.*, American Civil Liberties Union, *The Vital Role of End-to-End Encryption*, https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption.

- **The State has not shown, and cannot show, a reasonable likelihood of a statutory violation that could support its requested injunctive relief because (a) its assertions related to E2EE are disconnected from the Complaint and the claims it relies on, (b) Section 230 of the federal Communications Decency Act bars the State's claim and provides Meta with immunity for its choice to publish third-party content using E2EE, and (c) the State cannot succeed on its claims that Meta's use of E2EE is a deceptive practice or is an unconscionable practice.**

LEGAL STANDARD

A preliminary injunction or TRO is "extraordinary relief," not awarded as of right. *Dep't of Conservation & Nat. Res., Div. of Water Res. v. Foley*, 121 Nev. 77, 80 (2005).

The State misstates the standard for a TRO. The State relies on *State ex rel. Off. of Att'y Gen., Bureau of Consumer Prot. v. NOS Commc'ns, Inc.*, 120 Nev. 65, 68 (2004), holding that in consumer enforcement actions by the State a ***preliminary injunction*** does not require a showing of irreparable injury, provided the State shows "through competent evidence . . . a reasonable likelihood that the statute was violated." Motion for Preliminary Injunction ("Mot.") 14.

That case did not address the standards for a TRO, and the State cites no law applying this preliminary injunction standard to the more extraordinary remedy of a TRO. The sole case the State cites (Mot. 14) on the standards for a TRO, *Pasaye v. Dzurenda*, 375 F. Supp. 3d 1159, 1164 (D. Nev. 2019), holds that a TRO requires a showing that the plaintiff (1) "is likely to succeed on the merits," (2) "is likely to suffer irreparable harm in the absence of preliminary relief," (3) "that the balance of equities tips in [the plaintiff's] favor," and (4) "that an injunction is in the public interest." If the Court were to bless the State's reading of Nevada law, it would open the floodgates for the Attorney General to seek TROs at the pleadings stage every time it sues, without having to make any showing of an entitlement to emergency relief and instead based solely on its allegations that a statute was violated. That conclusion is supported by neither law nor logic, and the Court should reject it. The purpose of a TRO is to maintain the status quo pending determination of a preliminary injunction, and the State has presented no rationale for requiring one here.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

Further, even if the State meets the standards for a preliminary injunction (*i.e.*, that a statute authorizes it and the State has shown a "reasonable likelihood" of a statutory violation), "[w]hether a preliminary injunction should be granted is a question addressed to the district court's discretion." *NOS Commc'ns, Inc.*, 120 Nev. at 68 (internal quotation marks and citation omitted). Before awarding relief, "the court must consider the totality of the circumstances concerning the alleged violation." *Edwards v. Emperor's Garden Rest.*, 122 Nev. 317, 325 (2006) (citing *NOS Communications*, 120 Nev. at 68). A party seeking an injunction must put forward at least "a prima facie showing through substantial evidence." *Shores v. Glob. Experience Specialists, Inc.*, 134 Nev. 503, 507 (2018).

ARGUMENT

I. It Is Fundamentally Unfair and Unnecessary to Decide the State's TRO Motion on This Highly Accelerated Timetable.

As the State acknowledges, in deciding whether to issue an injunction, the Court must "balance the threat of the injury to the plaintiff against the threat of harm an injunction may cause to the defendant, as well as whether injunctive relief would be contrary to the public interest." Mot. 20 (citing *Ottenheimer v. Real Estate Div.*, 91 Nev. 338, 342, 535 P.2d 1284, 1285 (1975)). The balance of hardships weighs heavily in favor of Meta.

The State admits that E2EE has been available as feature on Messenger for ***eight years***. *See* Mot. 10 ("Since ***2016***, Meta has allowed users the option of employing E2EE for any private messages they send via Messenger." (emphasis added)). On December 6, 2023—***ten weeks ago***—Meta began making E2EE the standard for all messages on Messenger, rather than a setting to which users could opt in.[3] In doing so, Messenger joined other services, including Apple's iMessage, which has deployed E2EE as a standard feature ***since 2011***,[4] and FaceTime, for which

[3] *See* "Launching Default End-to-End Encryption on Messenger," Meta Newsroom (Dec. 6, 2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.
[4] *See* "New Version of iOS Includes Notification Center, iMessage, Newsstand, Twitter Integration Among 200 New Features," Apple Newsroom (June 6, 2011) https://www.apple.com/newsroom/2011/06/06New-Version-of-iOS-Includes-Notification-Center-iMessage-Newsstand-Twitter-Integration-Among-200-New-Features/.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

E2EE has been standard since at least 2013.[5] Yet the State waited until January 20, 2024—six weeks after the new default setting was announced, and eight years after E2EE first became available on Messenger—to file its Complaint. It then inexplicably waited another three weeks to serve Meta with the Complaint.[6] As such, before yesterday, Meta had not even been able to review the full scope of the State's allegations.[7] Mot. 14. Concurrently with its lengthy Complaint, the State served the present motion, along with two supporting declarations that purport to justify enjoining a practice that was announced two months ago (and was available for ***years*** as a non-default setting and as a feature in other services, such as Apple's iMessage).

The State's delays demonstrate the fundamental unfairness of requiring Meta to prepare this Opposition on one day's notice. There is no emergency that requires this accelerated timetable. *Quiroga v. Chen*, 735 F. Supp. 2d 1226, 1228 (D. Nev. 2010) ("The temporary restraining order should be restricted to serving its underlying purpose of preserving the status quo and preventing irreparable harm just so long as is necessary to hold a hearing, and no longer." (cleaned up)). Meta has not been given sufficient time to identify and prepare responses to the myriad assertions and misstatements in the State's Motion. Moreover, the State apparently seeks to present live testimony from its witnesses. *See* Mot. at 6. In this unfairly accelerated and truncated timetable, Meta has not been given a fair chance to develop responses to the State's witnesses, nor to develop and present its own witnesses and evidence. In short, there is no exigency that warrants this highly accelerated and unfairly compressed timetable for Meta's Opposition to the TRO motion—in contrast to a motion for preliminary injunction that can be noticed, briefed and heard under a reasonable schedule that allows Meta a fair opportunity to be heard.

E2EE ensures that users' communications remain private and secure "from the moment they

[5] *See* "Apple's Commitment to Customer Privacy" (June 16, 2023), https://www.apple.com/apples-commitment-to-customer-privacy.

[6] Meta has still yet to be served by the State in the two simultaneously filed and substantially identical proceedings in the Eighth Judicial District Court but not presently before the Court.

[7] As the Court is aware, the State filed its 116-page Complaint under seal, with significant redactions. Until being served, Meta only had access to the publicly filed, heavily redacted version of the Complaint. Meta has not been afforded sufficient time to review and analyze the unredacted Complaint, further prejudicing Meta in its efforts to respond to the State's motion.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

leave [the users'] device to the moment they reach the receiver's device."[8] The importance and fundamental value of E2EE has been widely recognized. For instance, the American Civil Liberties Union described the critical importance of E2EE in these terms:

> Our lives are increasingly intertwined with technology, and people must be able to communicate privately and securely. End-to-end encryption is the best protection, offering individuals the assurance that their personal data are shielded from prying eyes. As employed in Apple's new iCloud implementation and in messaging apps like WhatsApp and Signal, this technology can ensure that only the sender and the intended recipients can access the content of a message. This level of security not only protects individuals from cyberattacks but also empowers citizens to communicate freely without fear of surveillance, censorship, and warrantless searches — whether by the government, Big Tech, data brokers, or anyone else.[9]

Meta takes seriously the State's allegations that bad actors might use Messenger to do harm and, in conjunction with outside experts, academics, advocates and government agencies, has built into Messenger privacy, safety and control "mitigations to ensure that privacy and safety go hand-in-hand."[10] But the mere switch in Messenger's use of E2EE three months ago—from an opt-in feature to the standard for all messages—does not present an emergency that warrants this unfairly accelerated process, particularly because E2EE has been available on Messenger for ***eight years*** and has been a default feature on other mainstream communication services for over ***a dozen years***.

The consequences of granting a TRO would be immense for the entire industry. Such a TRO would immediately call into question the long-established use of E2EE on other mainstream, widely used messaging services like Apple's iMessage, because the inability to scan messages for harmful content is inherent in E2EE technology itself.[11] Indeed, Nevada law recognizes the value of encryption, requiring data collectors to encrypt personal information. *See* Nev. Rev. Stat.

---

[8] *See* "Launching Default End-to-End Encryption on Messenger," Meta Newsroom (Dec. 6, 2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.

[9] American Civil Liberties Union, *The Vital Role of End-to-End Encryption*, https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption.

[10] "Launching Default End-to-End Encryption on Messenger," Meta Newsroom (Dec. 6, 2023), https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

[11] *See, e.g.*, Tripp Mickle, *In Monitoring Child Sex Abuse, Apple Is Caught Between Safety and Privacy*, N.Y. Times (Sept 1, 2023), *available at* https://www.nytimes.com/2023/09/01/technology/child-sex-abuse-imagery-apple-safety-privacy.html (noting that Apple is "caught between child safety groups, which want it to do more to stop the spread of [child sexual abuse imagery], and privacy experts, who want it to maintain the promise of secure devices").

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

603A.215. A seismic shift that would fundamentally challenge the use of E2EE should not be undertaken with a 24-hour turnaround on briefing that does not afford Meta a fair and reasonable opportunity to develop a full response to the State's arguments.

Indeed, the merits of E2EE are best suited to the deliberative processes of the political branches. The State concedes, as it must, that E2EE has security and privacy benefits. Mot. 19. Advocacy groups nationwide have lauded encryption technology as vital to protecting privacy interests in modern society.[12] And our nation's policymakers are currently evaluating what, if any, rules should be placed on the use of technologies like E2EE to balance competing policy goals and privacy interests.[13] Those policy decisions should not be taken out of the hands of Congress, particularly in such a frenzied fashion.

The Court should also reject the State's proposed TRO because it is vague and infeasible. *First*, it would apply to users "within the State of Nevada." But as Meta has explained in Securities and Exchange Commission filings, "[o]ur data regarding the geographic location of our users is ***estimated*** based on a number of factors, such as the user's IP address and self-disclosed location." Meta Platforms, Inc., SEC Form 10-K, FY December 31, 2023 at 6 (emphasis added). As a result, "[t]hese factors may not always accurately reflect the user's actual location. For example, a user may appear to be accessing Facebook from the location of the proxy server that the user connects to rather than from the user's actual location. The methodologies used to measure our metrics are

[12] *See, e.g.*, "The Vital Role of End-to-End Encryption," American Civil Liberties Union, https://www.aclu.org/news/privacy-technology/the-vital-role-of-end-to-end-encryption; "Encryption: How It Can Protect Journalists and the Free Press," Internet Society & Committee To Protect Journalists (Aug. 2022), https://www.internetsociety.org/wp-content/uploads/2020/03/2022-Encryption-for-Journalists-Factsheet-EN.pdf; "Encryption: A Matter of Human Rights," Amnesty Int'l (Mar. 22, 2016), https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights; "Meta Announces End-to-End Encryption by Default in Messenger," Elec. Frontier Found. (Dec. 7, 2023) ("[W]e applaud this decision. It will bring strong encryption to over one billion people, protecting them from dragnet surveillance of the contents of their [Messenger] messages."), https://www.eff.org/deeplinks/2023/12/meta-announces-end-end-encryption-default-messenger; "U.S. Chamber of Commerce Statement on Encryption Policy and Cybersecurity," U.S. Chamber of Comm. (Oct. 14, 2016) ("Encryption is an integral part of both individuals' and enterprises' cybersecurity."), https://www.uschamber.com/assets/archived/images/documents/files/us_chamber_encryption-cyber_policy_statement_oct_14_2016_final_1_0.pdf.

[13] *See, e.g.*, EARN IT Act of 2023, S.1207, 118th Cong. (2023); STOP CSAM Act of 2023, S.1199, 118th Cong. (2023); Cooper Davis Act, S.1080, 118th Cong. (2023).

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

also susceptible to algorithm or other technical errors." *Id.* Accordingly, Meta would not be able to identify all users within the State of Nevada. Second, the State's TRO would apply to actions by users "who Meta either knows or has reason to know are under the age of 18." But in this context—services with billions of accounts where age is generally provided by users themselves—it is unclear what this knowledge standard entails. To ensure compliance with the TRO, as a result, Meta may have to attempt to disable E2EE on Messenger for all users. Due to the truncated timeline here, Meta has not yet been able to assess the feasibility and burdens of doing so.

II. The State Has Not Shown a "Reasonable Likelihood" of a "Statutory Violation" that Could Support Injunctive Relief.

Even putting aside that it makes no showing of irreparable injury that would support the entry of a TRO, *see Pasaye*, 375 F. Supp. 3d at 1164, the State does not satisfy the standards for entry of preliminary injunctive relief because it has not shown, "through competent evidence, a reasonable likelihood that the statute was violated," *NOS Commc'ns,* 120 Nev. at 68. The only claims pleaded in the State's Complaint and relied on in its Motions are alleged violations of the Nevada Deceptive Trade Practices Act ("NDTPA"). The State's request to enjoin E2EE on the basis of deceptive practices claims is entirely disconnected from its Complaint. The State has also failed to show a statutory violation because its claims are barred by Section 230 of the Communications Decency Act (an issue it fails to address) and it has not shown that its consumer protection claims related to E2EE can succeed.

A. The State's Argument Challenging Meta's Use of E2EE Is Disconnected from Its Complaint, the Claims It Relies on, and Its Purported Evidence.

The State's Complaint is focused on allegations that Meta's services are "addicting" to users and contribute to mental health issues in teens. The Complaint makes only very brief references to E2EE, which appear entirely in a section about allegedly "hooking" teens. *See* Compl. § II.C.6. While the State's motion seeks to repackage E2EE as part of its deception and unconscionable practices claims, that is simply not what is pleaded. That fundamental mismatch between the Complaint and the injunctive relief sought by the State requires denial of the TRO motion. *See, e.g.*, *Pac. Radiation Oncology, LLC v. Queen's Med. Ctr.*, 810 F.3d 631, 636 (9th Cir. 2015)

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

("[T]here must be a relationship between the injury claimed in the motion for injunctive relief and the conduct asserted in the underlying complaint . . . . The relationship between the preliminary injunction and the underlying complaint is sufficiently strong where the preliminary injunction would grant 'relief of the same character as that which may be granted finally.'" (quoting *De Beers Consol. Mines v. United States*, 325 U.S. 212, 220 (1945)).

The relief the State seeks is also disconnected from the claims it relies on. The State primarily relies on a ***misrepresentation*** consumer protection claim. But the remedy (if any, and after a trial) for a misrepresentation claim is to enjoin the defendant from making the misrepresentation or to correct it. *See* Nev. Rev. Stat. § 598.0979(1) (authorizing Attorney general to bring injunctive relief action only "prohibiting the person from continuing the practices" alleged to be deceptive). The unconscionable practices claim, moreover, likewise focuses only on alleged "addiction" and alleged resulting mental health injuries—allegations and harms untethered from the sweeping relief the State seeks here related to E2EE.

Finally, the relief the State seeks is disconnected from its own evidence. The State has submitted two declarations purporting to show the problems that E2EE causes law enforcement. Those declarations have any number of flaws, and Meta will address them if provided with appropriate time to respond. But, for present purposes, whatever problems the State identifies based on law enforcement's inability to review encrypted messages would not be altered by turning off the setting on a single messaging service that has made this technology available since 2016. The supposed problems that law enforcement faces would remain because many other messaging services use E2EE.

Further, the State's own evidence reflects that law enforcement ***is*** able to review encrypted messages by extracting those messages from mobile devices. *See* State Br. Ex. 1, at ¶¶ 5-9; State Br. Ex. B, at ¶¶ 19-20. In other words, the State's own evidence demonstrates that the requested relief is unnecessary to address the issue the State suggests warrants the relief it requests.

B. Section 230 Bars the State's Claims Regarding E2EE and the Requested Injunction.

The State cannot carry its burden to show that it is likely to succeed on its claims that Meta's

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

use of E2EE violates the NDTPA because federal law—specifically, Section 230 of the Communications Decency Act—precludes imposing liability on Meta for allegedly publishing harmful user-generated content, which the State claims is enabled by Meta's use of E2EE.

"Congress enacted [Section 230] as part of the Communications Decency Act of 1996 for two basic policy reasons: to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material." *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003). To achieve these objectives, Section 230 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). It further provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3).

Because Section 230 "protect[s] websites not merely from ultimate liability, but [also] from having to fight costly and protracted legal battles," *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008) (en banc), courts apply the immunity as early as possible, *e.g.*, *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1101 (9th Cir. 2019) (affirming motion to dismiss). Courts also routinely apply Section 230 to deny requests for injunctive relief. *See, e.g.*, *Hassell v. Bird*, 5 Cal. 5th 522, 546–47 (2018); *Kathleen R. v. City of Livermore*, 87 Cal. App. 4th 684, 698 (Cal. Ct. App. 2001).

In applying Section 230, "what matters is not the name of the cause of action," but "whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content provided by another." *Barnes*, 570 F.3d at 1101–02. Section 230 "is implicated not only by claims that explicitly point to" content created by others, "but also by claims which, though artfully pleaded to avoid direct reference, implicitly require recourse to that content to establish liability or implicate a defendant's role, broadly defined, in publishing" the content. *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140, 156 (E.D.N.Y. 2017). Section 230 thus bars claims where (1) the defendant is a "provider . . . of an interactive computer service," and (2) the claim seeks to hold the defendant liable as a "publisher or speaker" of (3) content provided by someone else. *Barnes*, 570 F.3d at 1099–1100. Each element is satisfied here.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

First, Meta is a provider of an "interactive computer service," as courts routinely hold. *See, e.g., Klayman v. Zuckerberg*, 753 F.3d 1354, 1357 (D.C. Cir. 2014) (Facebook); *Dangaard v. Instagram, LLC*, 2022 WL 17342198, at *4 (N.D. Cal. Nov. 30, 2022) (Facebook and Instagram).

Second, the State's claims would treat Meta as a publisher. The State contends that Meta's use of E2EE violates the NDTPA because it "enables predators to stalk young users with impunity." Mot. 12 (cleaned up). The State alleges that Nevada minors are injured by the harmful content that they receive from other users, and that E2EE exacerbates that harm by preventing Meta from viewing that user-generated content and by making it more difficult for law enforcement to view it. *Id.* at 10–11. In other words, the State seeks to hold Meta liable for publishing harmful user-generated content on the theory that publishing that content using E2EE hinders "Meta's ability to proactively search[] for harmful content directed towards children." *Id.* at 18.

Courts have repeatedly held that Section 230 bars claims like the State's that would impose liability based on a defendant's failure to monitor communications between users to detect harmful user-generated content. In *Green v. American Online (AOL)*, 318 F.3d 465 (3d Cir. 2003), for example, the Third Circuit held that Section 230 barred failure-to-protect claims brought against an online service because such claims would have imposed liability for failing to monitor and "address certain harmful content on its network." *Id.* at 469. As the court explained, "Section 230 'specifically proscribes liability'" for an online service's "decisions relating to the monitoring, screening, and deletion of content from its network" because such actions are "quintessentially related to a publisher's role." *Id.* (cleaned up). Similarly, in *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008), the Fifth Circuit rejected an argument that minor plaintiffs would not have been assaulted but for MySpace's "failure to implement measures that would have prevented . . . communicat[ion]" between plaintiffs and their abusers. *Id.* at 420. Although those plaintiffs claimed their case was "predicated solely on [the defendant's] failure to implement basic safety measures to protect minors," the court held that was "merely another way of claiming" that MySpace "was liable for publishing the communications" between users and was therefore

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

precluded by Section 230. *Id.* at 420–22.[14]

Courts have likewise held that Section 230 bars claims that would impose liability based on a defendant's publication decisions regarding who can view third-party content—*i.e.*, to whom content should be published. Courts have described communications between users as the "prototypical" content for which a service is protected by Section 230. *Kimzey v. Yelp!, Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016) (cleaned up). That protection applies regardless of the communication's contents. *E.g.*, *Force v. Facebook, Inc.*, 934 F.3d 53, 65 (2d Cir. 2019) (Section 230 barred claims based on messages exchanged between Hamas members); *Bride v. Snap Inc.*, 2023 WL 2016927, at *6 (C.D. Cal. Jan. 10, 2023) (Section 230 barred claims arising from "abusive messaging"). The encryption of messages does not alter this conclusion because Section 230's protections apply to a communication's transmission. Reflecting this point, "a number of courts" have applied Section 230 "to bar claims predicated on a defendant's transmission of nonpublic messages." *Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1128–29 (N.D. Cal. 2016); *see also id.* at 1124 ("[T]he private nature of Direct Messaging does not remove the transmission of such messages from the scope of publishing activity under section 230(c)(1)."); *L.W. v. Snap Inc.*, 2023 WL 3830365, at *4 (S.D. Cal. June 5, 2023) (Section 230 applies to claims involving "disappearing messages"); *Doe v. Snap*, 2022 WL 2528615, at *14 (S.D. Tex. July 7, 2022) (similar), *aff'd*, 2023 WL 4174061 (5th Cir. June 26, 2023). Like private or disappearing messages, encrypted messages fall within publishing's scope because they are "meant to facilitate the communication and content of others." *Dyroff*, 934 F.3d at 1098.

Third, the State's claims wholly depend on content provided by others. The State does not allege that Meta created any harmful content. Instead, the State asserts that such content is generated by third parties. *E.g.*, Compl. ¶ 208 (alleging "malicious actor[s]" are responsible for "improper[] . . . interactions" on Messenger). Encrypting and transmitting that content does not change the fact that it was created by another. *See* 47 U.S.C. § 230(f)(3) (the "information content

[14] Other courts have reached the same result in similar circumstances. *See, e.g.*, *Doe II v. MySpace Inc.*, 175 Cal. App. 4th 561, 569 (2009) (similar); *L.W.*, 2023 WL 3830365, at *4 (Section 230 barred design defect claims because "Defendants' alleged failure to monitor and remove third-party content" would "treat Defendants as publishers").

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

provider" is the "person or entity that is responsible, in whole or in part, for the creation or development of information"); *see also Kimzey*, 836 F.3d at 1270–71 (holding "dissemination of content does not equal creation or development of content" under Section 230). Because the State's alleged harms arise from user-generated content, and because facilitating distribution of such content does not transform it into Meta's own, the State's claims and request for injunctive relief are barred by Section 230.

C. The State Has Failed to Show That It Will Succeed on Its Deception Claim.

As explained above, a claim about allegedly deceptive statements cannot be used as a vehicle to regulate Meta's practices—because at most, even if an injunction were entered (after a full trial) on the basis of such a claim, it should only extend to barring the making of the deceptive statements. But even setting that fundamental defect aside, the State's deceptiveness claim is deeply flawed.

The State cites only ***one*** statement by Meta about E2EE: "The extra layer of security provided by end-to-end encryption means that the content of your messages and calls with friends and family are protected from the moment they leave your device to the moment they reach the receiver's device. This means that nobody, including Meta, can see what's sent or said, unless you choose to report a message to us." Compl. ¶ 203 (cited by Mot. 18).[15] To start, this statement is not alleged in the Complaint to be deceptive, and the State does not rely on it to support its deception claim. Instead, the statement is used simply to describe E2EE. In any event, this statement is unequivocally true; the State's own brief admits that E2EE prevents messages from being "tampered with by hackers," and the State does not dispute that the statement is accurate. Mot. 10. In fact, this aspect of E2EE is precisely what the State takes issue with.

Aside from this statement, the State's Motion points to no other statements about E2EE, and the Complaint does not allege that any statements about E2EE are deceptive. To the extent the Motion vaguely references broad allegations that Meta represented its service was "safe" for users, that is insufficient to warrant the extraordinary remedy of an injunction. Courts routinely find that

[15] The Complaint contains two paragraphs labeled 203; the relevant paragraph is on page 49.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

such statements about "safety" are not actionable under consumer protection law because they do not create objective, concrete expectations for consumers. *See, e.g.*, *Morris v. Princess Cruises, Inc.*, 236 F.3d 1061, 1068 (9th Cir. 2001) (representation that consumers "would be safely and adequately served" failed to state a claim because the statement "is devoid of any meaningful specificity"). And even if unspecified statements about Facebook and Instagram being safe were somehow misleading (they were not), that provides no basis to issue the sweeping injunction here that targets E2EE in particular.

Perhaps realizing the theories in its Complaint cannot prevail, the State invokes a criminal statute that is nowhere cited in the Complaint and is disconnected from its consumer protection claims. That statute prohibits willfully using encryption to commit crimes, or the aiding and abetting, concealment, or hindrance of crimes. *See* Nev. Rev. Stat. § 205.486. As an initial matter, the State's only hook for citing this criminal statute is the provision of the NDTPA that defines "deceptive trade practices" to include "violating one or more laws relating to the sale or lease of goods or services." Nev. Rev. Stat. § 598.0923(1)(c). But the State has failed to explain how this criminal prohibition on using encryption to commit crimes "relate[s] to the sale or lease of goods or services." It is therefore not an appropriate predicate for a misrepresentation claim. In addition, the State has failed to explain how a communications provider could be held criminally liable for the actions of third parties misusing its services merely by providing those services to the public at large with encryption enabled. *See, e.g.*, *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 506 (2023) (holding that social media services do not "aid and abet" third-party bad actors merely because bad actors post content on their platforms). And the State's single-paragraph argument all but concedes this, providing nothing that even arguably demonstrates that Meta willfully aided, abetted, facilitated, or concealed criminal activity—a finding that would have dramatic consequences for all encrypted messaging services, including services like Apple's iMessage

D. The State Has Failed to Show a Likelihood of Success on Its Unconscionable Practices Claim.

As explained, the State's unconscionable practices claim about "addictive" services, as pled in the Complaint, is divorced from the relief it seeks here because the State does not challenge

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

Meta's default setting for E2EE as an unconscionable practice. That aside, the State has failed to show it is likely to succeed: this claim attempts to transform an ordinary, common and valuable practice—defaulting to encrypting messages—into an unconscionable trade practice. E2EE is widely used, including on the default messaging app for every iPhone used across the nation.[16] As the State admits, E2EE serves the valuable purpose of helping to prevent hackers from reading encrypted messages. Mot. 10. And it has other benefits, including fostering free speech and providing a secure communications service for those in danger of being punished for their expression. In addition, the change to Messenger that the State challenges is solely the update to the default setting for E2EE. For years, users have been able to use E2EE on Messenger by opting in; it will now be applicable to all Messenger messages.[17] E2EE, a feature with unquestionable benefits that has widely been used and widely embraced across the country for years, is not an "unconscionable" practice.

Although the State's E2EE theory for why using E2EE is unconscionable is far from clear, it appears to boil down to the contention that E2EE makes law enforcement more difficult because encrypted messages cannot be as easily read. Mot. 18–20. As explained above, this theory is not pled in the State's Complaint; instead, the Motion relies on two untested, insufficient declarations discussing this issue in an attempt to find shoehorn E2EE into the rubric of an unfair trade practice.[18] And those declarations, on their face, specifically acknowledge that law enforcement officials ***are*** able to review encrypted messages by extracting those messages from mobile devices. *See* State Br. Ex. 1, at ¶¶ 5-9; State Br. Ex. B, at ¶¶ 19-20. In other words, the State's own evidence demonstrates that encrypted messages are not the impediment to law enforcement that the State suggests—which further demonstrates why the use of E2EE, with all of its benefits, cannot be an unfair trade practice. That is basis enough to reject the State's argument.

---

[16] Apple, Messages & Privacy, https://www.apple.com/legal/privacy/data/en/messages/#:~:text=We%20designed%20iMessage%20to%20use,(s)%20can%20access%20them.

[17] *See* Meta, *Launching Default End-to-End Encryption on Messenger*, https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.

[18] The State's motion also quotes extensively from the allegations of the Complaint, but those of course are not "competent evidence" that can support injunctive relief. *NOS Communications*, 120 Nev. at 68.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

In any event, the State conspicuously relies only on one subsection of Nevada law to demonstrate unconscionability, *id.*, but that section relates to unequal bargaining power, *see* Nev. Rev. Stat. § 598.0923(2)(b)(1). But the basis of the State's motion – its assertion that E2EE hampers law enforcement – has nothing to do with differential bargaining power between companies and customers, so this provision has no application here.

CONCLUSION

For the reasons set forth above, the Court should deny the State's motion for a TRO or preliminary injunction or, at the very least, set an appropriate briefing schedule to allow Meta a fair opportunity to respond to the motion.

Dated this 21st day of February, 2024.

PETERSON BAKER, PLLC

By: /s/ Tamara Beatty Peterson

TAMARA BEATTY PETERSON, ESQ., Bar No. 5218
tpeterson@petersonbaker.com
DAVID E. ASTUR, ESQ., Bar No. 15008
dastur@petersonbaker.com
701 S. 7th Street
Las Vegas, NV 89101
Telephone: 702.786.1001
Facsimile: 702.786.1002
Attorneys for Defendant Meta Platforms, Inc.

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

PETERSON BAKER, PLLC
701 S. 7th Street
Las Vegas, NV 89101
702.786.1001

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that pursuant to NRCP 5(b), EDCR 8.05, Administrative Order 14-2, and NEFCR 9, I caused a true and correct copy of the foregoing **OPPOSITION TO STATE OF NEVADA'S MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION ON ORDER SHORTENING TIME** to be submitted electronically for filing and service with the Eighth Judicial District Court via the Court's Electronic Filing System on the 21st day of February, 2024, to the following:

AARON D. FORD, ESQ.
Attorney General
ERNEST FIGUEROA, ESQ.
Consumer Advocate
MARK J. KRUEGER, ESQ. (#7410)
Chief Deputy Attorney General
State of Nevada, Office of the Attorney General, Bureau of Consumer Protection
100 North Carson St.
Carson City, NV 89701-1108
mkrueger@ag.nv.gov

Attorneys for Plaintiff

MICHAEL J. GAYAN, ESQ. (#11135)
m.gayan@kempjones.com
J. RANDALL JONES, ESQ. (#1927)
r.jones@kempjones.com
DON SPRINGMEYER, ESQ. (#1021)
d.springmeyer@kempjones.com
KEMP JONES, LLP
3800 Howard Hughes Parkway, 17th Floor
Las Vegas, Nevada 89169

Attorneys for Plaintiff

N. MAJED NACHAWATI, ESQ.
mn@ntrial.com
BRIAN E. MCMATH, ESQ.
bmcmath@ntrial.com
PHILIP D. CARLSON, ESQ.
pcarlson@ntrial.com
NACHAWATI LAW GROUP
5489 Blair Road
Dallas, Texas 75231

Attorneys for Plaintiff

DAVID F. SLADE, ESQ
slade@whlaw.com
WH LAW
1 Riverfront Place, Suite 745
North Little Rock, Arkansas 72114

Attorneys for Plaintiff

/s/ Julia Melnar
On behalf of Peterson Baker, PLLC