CAUSE NO. 26-0393 _____

THE STATE OF TEXAS, Plaintiff, v. META PLATFORMS, INC., and WHATSAPP, LLC, Defendants.	IN THE DISTRICT COURT 71ST JUDICIAL DISTRICT HARRISON COUNTY, TEXAS

PLAINTIFF'S ORIGINAL PETITION

The Attorney General brings this suit on behalf of the State against Meta Platforms, Inc. ("Meta") and WhatsApp, LLC ("WhatsApp") (collectively, "Defendants") for Defendants' violations of the Texas Deceptive Trade Practices—Consumer Protection Act, Tex. Bus. & Com. Code Ann. § 17.41 *et seq.* ("DTPA") and alleges as follows.

INTRODUCTION

1. WhatsApp is the most popular messaging app in the world. It purports to offer its more than ***3 billion*** users in over 180 countries[1] privacy, security, and peace of mind by promising that "[y]our privacy is our priority. With end-to-end encryption on WhatsApp, your personal messages, photos, calls and more stay between you and the people you choose, ***meaning not even WhatsApp can see them***."[2] Mark Zuckerberg, the founder, Chairman, and Chief Executive Officer of Meta (which has owned WhatsApp since 2014), reinforced this claim to the United States Senate

[1] *About*, WhatsApp, https://www.whatsapp.com/about [https://perma.cc/HF26-RFMZ] (last visited May 5, 2026).

[2] *Privacy*, WhatsApp (emphasis added), https://www.whatsapp.com/privacy [https://perma.cc/2TKV-4CC5] (last visited May 5, 2026).

in sworn public testimony, asserting that "we do not see any of the content in WhatsApp, it's fully encrypted . . . . Facebook systems do not see the content of messages being transferred over WhatsApp."[3] And, since at least 2016, every single WhatsApp chat begins with the following statement:

2. WhatsApp's assurances are false. WhatsApp and its parent company, Meta, have access to virtually ***all*** of WhatsApp users' purportedly "private" communications. As concluded by a Commerce Department agent, "[t]here is no limit to the type of WhatsApp message that can be viewed by Meta."[4] On information and belief, to this day, Meta and WhatsApp store, maintain access to, and use WhatsApp's 3 billion users' "encrypted" messages. This lawsuit seeks to prevent the fundamental privacy violations and false, misleading, and deceptive practices Meta is perpetrating against the millions of Texans who have used WhatsApp believing their communications would be private from everyone, even from WhatsApp and Meta.

3. The gravity of Meta's and WhatsApp's violation of users' privacy and trust cannot be overstated. All users were entitled to believe their communications were private when

[3] *Facebook, Social Media Privacy, and the Use and Abuse of Data, Hr'g on S. 115–683 Before the S. Comm. on Com., Sci., & Transp. & the Comm. on the Judiciary*, 115th Cong., 2d Sess. (2018) (testimony of Mark Zuckerberg), https://www.congress.gov/event/115th-congress/senate-event/LC64510/text [https://perma.cc/UCB8-5LBH].

[4] Jake Bleiberg, *US Ends Investigation Into Claims WhatsApp Chats Aren't Private*, Bloomberg (Apr. 28, 2026), https://www.bloomberg.com/news/articles/2026-04-28/us-ends-investigation-into-claims-whatsapp-chats-aren-t-private [https://perma.cc/7TFP-E5DN] (last accessed May 4, 2026).

WhatsApp and Meta unequivocally and repeatedly promised that no one—not even WhatsApp and Meta—can access their messages.

4. Plaintiff brings this action on behalf of Texans and seeks penalties and injunctive relief to prevent WhatsApp and Meta from continuing to willfully deceive them by misrepresenting that their private communications were just that—***private and inaccessible even to WhatsApp and Meta***—when, in fact, WhatsApp and Meta have access to ***all*** WhatsApp users' communications in their entirety.

DISCOVERY CONTROL PLAN

5. The discovery in this case is intended to be conducted under Level 3 pursuant to Texas Rule of Civil Procedure 190.4. This case is not subject to the restrictions of expedited discovery under Texas Rule of Civil Procedure 169 because the State's claims include a claim for non-monetary injunctive relief and claims for monetary relief, including penalties and attorneys' fees and costs, in excess of $250,000, and the claims are within the jurisdictional limits of the Court.

PARTIES

6. Plaintiff is The State of Texas and brings this suit on behalf of the State by and through the Consumer Protection Division of the Office of the Texas Attorney General, pursuant to its authority under section 17.47 of the DTPA.

7. Defendant Meta Platforms, Inc. is a Delaware corporation, organized and existing under the laws of the State of Delaware, with its principal place of business at 1 Meta Way, Menlo Park, California 94025. With a $1.72 trillion market capitalization (subject to market fluctuations),

Meta is consistently ranked as one of the ten largest corporations in the world.[5] Prior to October 28, 2021, Meta operated as Facebook, Inc. ("Facebook").[6] For simplicity, this Petition may refer to Meta and Facebook, Inc. (the corporate entity) interchangeably as "Meta."

8. Defendant WhatsApp, LLC is a Delaware limited liability company, organized and existing under the laws of the State of Delaware, with its principal place of business at 1 Meta Way, Menlo Park, California, 94025. Since 2014, WhatsApp has been a wholly-owned subsidiary of Meta, acquired by (then-)Facebook for approximately $19 billion in cash and stock.[7]

JURISDICTION AND VENUE

9. This Court has subject-matter jurisdiction over this action. *See* Tex. Const. art. V, § 8.

10. This Court may exercise personal jurisdiction over Defendants because they do business in Texas and the acts complained of relate to that business in Texas. *See* Tex. Civ. Prac. & Rem. Code Ann. § 17.042. Specifically, contractors acting on Meta's behalf in Texas were among the individuals able to access Texas users' supposedly private WhatsApp communications.

11. Venue of this suit is proper in Harrison County under section 17.47(b) of the DTPA because Defendants have done business in Harrison County, and under section 15.002(a)(1) of the Texas Civil Practice and Remedies Code because a substantial part of the events and omissions giving rise to the claims in this Petition occurred in Harrison County.

---

[5] Julie Pinkerton, *The 10 Most Valuable Companies in the World by Market Capitalization*, U.S. News & World Rep. (June 24, 2025), https://money.usnews.com/investing/articles/most-valuable-companies-in-the-world-by-market-cap.

[6] *Introducing Meta: A Social Technology Company*, Meta (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ [https://perma.cc/L75Y-YCVW].

[7] *Facebook to Acquire WhatsApp*, Meta (Feb. 19, 2014), https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/ [https://perma.cc/8EMU-SDXS].

PUBLIC INTEREST

12. The State has reason to believe that Defendants have engaged in, are engaging in, and will continue to engage in, the unlawful practices set forth below; that Defendants have, by means of these unlawful acts and practices, caused damage to and acquired money or property from persons; and that Defendants adversely affected the lawful conduct of trade and commerce, thereby directly and indirectly affecting Texans. Therefore, the Consumer Protection Division of the Office of the Attorney General of the State of Texas believes and is of the opinion that these proceedings are in the public interest.

TRADE AND COMMERCE

13. Defendants have, at all times described below, engaged in conduct that constitutes "trade" and "commerce" as those terms are defined in section 17.45(6) of the DTPA.

ACTS OF AGENTS

14. Whenever in this Petition it is alleged that Defendants did any act, it is meant that Defendants performed or participated in the act, or that their officers, agents, or employees performed or participated in the act on behalf of and under the authority of Defendants.

FACTUAL ALLEGATIONS

I. The WhatsApp Promise: Encryption for Everyone, Accessible to No One

15. Founded in 2009 by Jan Koum and Brian Acton, WhatsApp historically prided itself on being outside the big data economy driven by tech giants like Facebook and an oasis of privacy in a world where Facebook seemingly knew everything about everyone. In a 2009 blog post, Mr. Koum "set the record straight": "We have not, we do not and we will not **ever** sell your

personal information to anyone. Period. End of story."[8] In 2012, WhatsApp's co-founders explained they charged for WhatsApp to keep it ad-free because "[a]t every company that sells ads, a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the servers that hold all the data and making sure it's all being logged and collated and sliced and packaged and shipped out."[9] They cautioned: "Remember, when advertising is involved **you the user** are the product."[10] But at WhatsApp, they stressed, ***"[y]our data isn't even in the picture. We are simply not interested in any of it.***"[11]

16. When Facebook acquired WhatsApp in 2014, there was widespread concern that WhatsApp's respect for users' data and privacy would be compromised. But Mr. Koum again "set[] the record straight," reminding users of his experience growing up in Ukraine, where KGB monitoring of phone calls was commonplace and part of the reason his family emigrated; at WhatsApp, he stated, ***"[r]espect for your privacy is coded into our DNA."***[12] Complaining that speculation of WhatsApp's partnership with Facebook would change its core principles was "baseless," "unfounded," and "irresponsible," Mr. Koum assured users that WhatsApp's "focus remains on delivering the promise of WhatsApp far and wide, ***so that people around the world have the freedom to speak their mind without fear."***[13] Facebook CEO Mark Zuckerberg also assured the public that "[t]he vision is to keep the [WhatsApp] service exactly the same," noting

---

[8] Jan Koum, *Just Wanted To Say a Few Things*, WhatsApp (Nov. 19, 2009), https://blog.whatsapp.com/just-wanted-to-say-a-few-things [https://perma.cc/3AE4-TYHU].

[9] Jan Koum, *Why We Don't Sell Ads*, WhatsApp (June 18, 2012), https://blog.whatsapp.com/why-we-don-t-sell-ads [https://perma.cc/Z8UJ-U25U].

[10] *Id.*

[11] *Id.* (emphasis added).

[12] Jan Koum, *Setting the Record Straight*, WhatsApp (Mar. 17, 2014) (emphasis added), https://blog.whatsapp.com/setting-the-record-straight [https://perma.cc/9LQV-YQ88].

[13] *Id.* (emphasis added).

WhatsApp does not "use[] or store[] the billions of [messages] exchanged on the app daily."[14] Instead, Zuckerberg promised that WhatsApp content is deleted "almost instantly," which is "what people want," and "[w]e would be pretty silly to get in the way of that."[15]

17. But by 2016, around the same time WhatsApp was achieving end-to-end encryption across its platform, WhatsApp announced it would share user data such as phone numbers, profile photos, status messages and IP addresses with Facebook for purposes ranging from fighting abuse to ad targeting.[16] Although WhatsApp would still not have access to communications (at least according to their policies and public statements), the Facebookization of WhatsApp was underway.[17] As one author stated at the time: "Your individual messages on WhatsApp are still safe; that end-to-end encryption isn't going anywhere. But this change introduces a more insidious kind of privacy erosion, of the very sort people flocked to WhatsApp to escape."[18]

18. Since abandoning its hands-off approach to user data with its 2016 privacy policy changes and completing the rollout of end-to-end encryption across its platform, WhatsApp has made end-to-end encryption for everyone that prevents anyone—even WhatsApp and Meta—from accessing private communications one of its most ubiquitous and emphatic promises to its users. It is clear WhatsApp and Meta marketed WhatsApp in this way because they (correctly)

---

[14] Bianca Bosker, *Zuckerberg Promises Facebook Won't Read Your WhatsApp Chats*, Huffington Post (Feb. 24, 2014), https://www.huffpost.com/entry/zuckerberg-facebook-whatsapp_n_4848205#:~:text=top%20stories%20here.-,Zuckerberg%20Promises%20Facebook%20Won't%20Read%20Your%20WhatsApp%20Chats,of%20that%2C%22%20he%20added [https://perma.cc/E3NT-5TZK].

[15] *Id.*

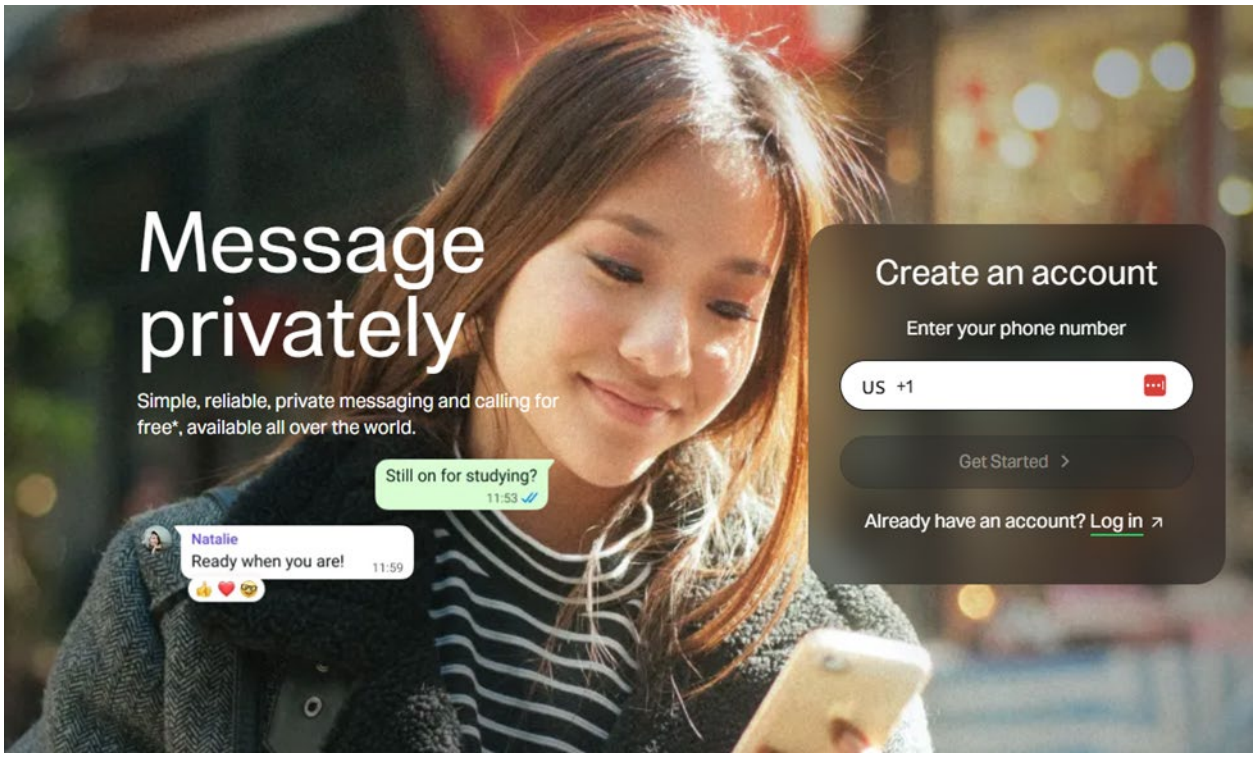
[16] *See, e.g.*, Brian Barrett, *WhatsApp's Privacy Cred Just Took a Big Hit*, Wired (Aug. 25, 2016), https://www.wired.com/2016/08/whatsapp-privacy-facebook/ [https://perma.cc/7TFP-E5DN].

[17] *See, e.g.*, Daniel Chandler & Rod Munday, "Facebookization," *Dictionary of Social Media* (2016).

[18] Brian Barrett, *supra* note 16.

determined that this promise would maintain and grow WhatsApp's user base, despite users' obvious and well-founded concerns about Meta's broader privacy problems.

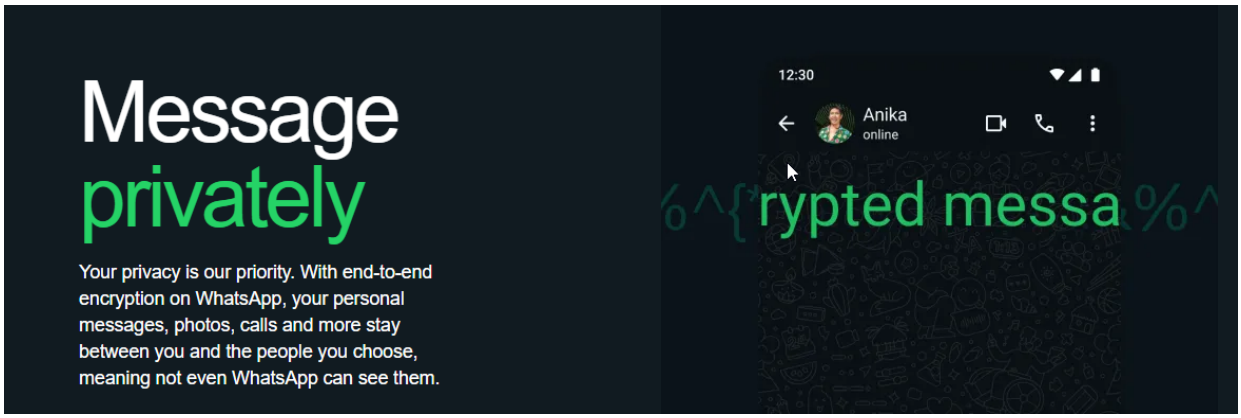
19. For example, the first image that greets users upon visiting WhatsApp's website touts WhatsApp is "private messaging and calling . . . available all over the world":[19]



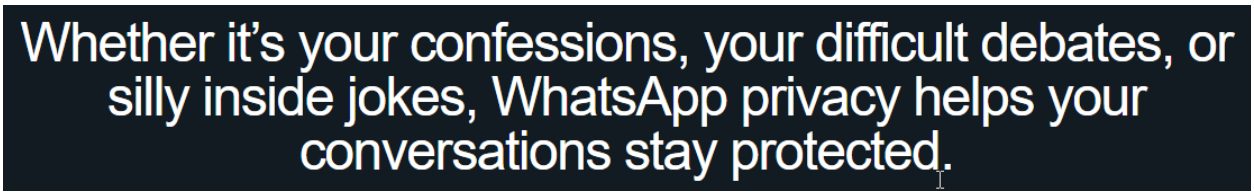
20. WhatsApp's "Privacy" page—which is the second section on the WhatsApp website, following only the "Features" section, highlights at the very top of the page that: users can "Message privately," "[y]our privacy is our priority," and "[w]ith end-to-end encryption on WhatsApp, ***your personal messages, photos, calls and more stay between you and the people you choose, meaning not even WhatsApp can see them"***:[20]

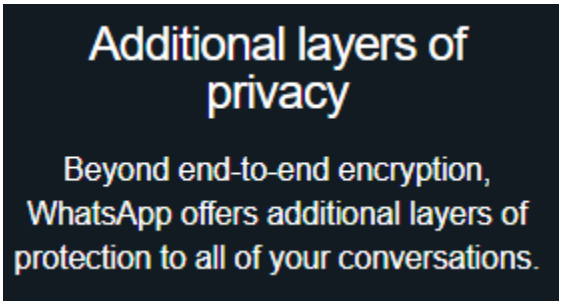
[19] Homepage, WhatsApp, https://www.whatsapp.com [https://perma.cc/99BT-P9CG] (last visited May 5, 2026).

[20] *Privacy*, WhatsApp, *supra* note 2 (emphasis added).



21. WhatsApp immediately continues boasting that ***only the recipient and the sender*** can read private conversations such as "confessions, . . . difficult debates, or silly inside jokes":[21]





22. WhatsApp's "FAQ" again reinforce that "not even WhatsApp[] can read, listen to, or share" users' personal images and calls":[22]

[21] *Privacy*, WhatsApp, *supra* note 2.

[22] *About End-to-End Encryption*, WhatsApp, https://faq.whatsapp.com/820124435853543/?locale=en_US [https://perma.cc/EG6U-VFB2] (last visited May 6, 2026).

How does WhatsApp work?

WhatsApp's end-to-end encryption is used when you chat with another person using WhatsApp Messenger. End-to-end encryption keeps your personal messages and calls between you and the person you're communicating with. No one outside of the chat, not even WhatsApp, can read, listen to, or share them. This is because with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. All of this happens automatically: no need to turn on any special settings to secure your messages.

23. WhatsApp makes similar representations in Apple's App Store, where it describes its application as "Simple[,] Reliable[,] Private[,]" tells prospective users that they can "**[m]essage privately** with end-to-end encryption," and promises those users that "Your privacy is our priority. With end-to-end encryption, you can be sure that your personal messages and calls stay between you and who you send them to. And no one, not even WhatsApp, can read or listen to them."[23]

24. Notably, every single chat on WhatsApp has this header emblazoned at the top:

25. Importantly, neither WhatsApp nor Meta discloses anywhere their unlimited access to users' encrypted communications—not even in the fine print. WhatsApp discloses only certain limited exceptions to its end-to-end encryption and the ability of WhatsApp, Meta, or third parties to access encrypted message content. For example, WhatsApp discloses that when a user reports another user in an individual chat, WhatsApp receives up to five of the last messages the reported

[23] *WhatsApp Messenger*, App Store for iPhone, https://apps.apple.com/us/app/whatsapp-messenger/id310633997 [https://perma.cc/XUM3-5422] (last visited May 6, 2026).

user sent to the reporting user.[24] Similarly, when a user reports abuse in a group chat, WhatsApp receives up to five of the last messages sent to the reporting user within the reported group. When calls take place in an individual chat, WhatsApp may also receive basic information about the last five calls with that user, such as who initiated the call and the duration of the call.[25] Nothing in these disclosures suggests that WhatsApp or Meta can access ***all*** of any user's communications.

26. WhatsApp likewise discloses that when customers contact WhatsApp for customer support, they may provide WhatsApp with information, "including copies of [their] messages."[26] Here too, however, this disclosure does not suggest WhatsApp and Meta can access any message the user does ***not*** provide to customer service.

27. WhatsApp also carves out certain specific use cases from its claims that WhatsApp and Meta cannot see users' messages, including business messaging services (which it says are clearly distinguished from personal messages) and communications that are not encrypted (such as communications with Meta services or "communications with businesses using Cloud API.")[27] Once again, nothing in these disclosures suggests WhatsApp and Meta can access all of a user's private messages.

28. Finally, regarding disclosures to law enforcement, WhatsApp states in relevant part:

---

[24] *About Reporting and Blocking on WhatsApp*, WhatsApp, https://faq.whatsapp.com/414631957536067/?helpref=faq_content&cms_platform=web [https://perma.cc/R4GP-L3YA] (last visited May 6, 2026).

[25] *Id.*

[26] *WhatsApp Privacy Policy*, WhatsApp (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy [https://perma.cc/64E2-KGMJ].

[27] *How You Interact with Others*, WhatsApp, https://faq.whatsapp.com/9658856237523915 [https://perma.cc/SAZ3-6AXL]; *About End-to-End Encryption*, WhatsApp, *supra* note 22; *WhatsApp Encryption Overview: Technical White Paper*, WhatsApp (updated Feb. 25, 2026), https://perma.cc/J336-JLWM.

> In the ordinary course of providing our service, ***WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages***. Undelivered messages are deleted from our servers after 30 days. . . . [W]e may collect, use, preserve, and share ***user information*** if we have a good-faith belief that it is reasonably necessary to (a) keep our users safe, (b) detect, investigate, and prevent illegal activity, (c) respond to legal process, or to government requests, (d) enforce our Terms and policies. This may include information about how some users interact with others on our service. ***We also offer end-to-end encryption for our services, which is always activated. End-to-end encryption means that messages are encrypted to protect against WhatsApp and third parties from reading them***.[28]

Here too, far from disclosing it can access users' encrypted communications, WhatsApp represents to both users and law enforcement authorities that it cannot read users' messages because they are encrypted.

II. WhatsApp's and Meta's Unrestricted Access to Users' Communications

29. End-to-end encryption is a method of securing digital communications wherein data is encrypted on the sender's device and only decrypted once it reaches the recipient's device. As WhatsApp analogizes, "with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. All of this happens automatically: no need to turn on any special settings to secure your messages."[29] In theory, even though encrypted communications may pass through a service provider's servers on their way to the intended recipient, they remain encrypted and unreadable to everyone but that intended recipient, because only the sender and the recipient have the key to "unlock" them on their respective devices.

---

[28] *Information for Law Enforcement Authorities*, WhatsApp (emphases added), https://faq.whatsapp.com/444002211197967 [https://perma.cc/KV3P-QP3G] (last visited May 6, 2026)

[29] *About End-to-End Encryption*, WhatsApp, *supra* note 22.

30. In November 2014, shortly after its acquisition by Facebook (now Meta), WhatsApp partnered with Open Whisper Systems to integrate the Signal Protocol, an end-to-end encryption cryptographic protocol, into its platform.[30] (Open Whisper Systems offers its own end-to-end encrypted messaging application, Signal.) By April 5, 2016, WhatsApp had completed integration of end-to-end encryption for all forms of communication across all user devices.[31]

31. Lest there be any confusion, the Signal Protocol does not protect ***all*** user information (nor does it purport to). Only the contents of the communication are encrypted; the metadata associated with the communication is not. Thus, as even they concede, Meta and WhatsApp have access to users' metadata, and can identify the who, when, and where (among other circumstances) of users' communications. Thus, if Alice and Bob message each other 90 times between 2 a.m. and 3 a.m. while Alice is in Seattle and Bob is in Sacramento, all of that metadata is undisputedly available to Meta and WhatsApp (and any other parties to whom they may make it available). Meta and WhatsApp represent to consumers that the ***content*** of those messages, however, should be undiscoverable, based on Defendants' representations. That notion assumes the Signal Protocol has been implemented without the inclusion of any "backdoor" in the application's source code that would allow either the platform itself or third parties to circumvent encryption. Such backdoors are called "kleptographic backdoors."

32. Signal itself notably makes its source code available for public inspection to promote both transparency and security (by allowing the public at large, including security analysts and researchers, to test for and identify vulnerabilities), and reviews of Signal's source code have

---

[30] *Open Whisper Systems Partners with WhatsApp To Provide End-to-End Encryption*, Signal (Nov. 18, 2014), https://signal.org/blog/whatsapp/ [https://perma.cc/NZX8-HYLN].

[31] *WhatsApp's Signal Protocol Integration Is Now Complete*, Signal (Apr. 5, 2016), https://signal.org/blog/whatsapp-complete/ [https://perma.cc/HDY5-KRKX].

in fact confirmed that it has no backdoor to its end-to-end encryption. WhatsApp, however, does not make its source code available to the public or even to third party security auditors. Accordingly, although cryptosecurity experts are confident the Signal app functions without any kleptographic backdoor, the public can only take the word of Meta and WhatsApp that they do not have access to the substance of WhatsApp users' communications.

33. That word is false. As reported by Bloomberg and others, a special agent for the Office of Export Enforcement—which operates within the Commerce Department's Bureau of Industry and Security—examined claims that Meta employees and contractors had the capability to view WhatsApp message content and concluded those claims were meritorious.[32] "Meta stores and can view WhatsApp messages."[33] "Meta can and does view and store all the text messages, photographs, audio and video recordings" and does so "in an unencrypted format."[34] Meta also maintains a "tiered permissions system" that allows it to grant different employees or contractors access to different sets of WhatsApp content, a power it has used to allow access to a "significant number of foreign/overseas workers in India."[35] For example, those tasked with "doing content moderation work for Meta" were sometimes granted access to WhatsApp message content.[36] The special agent's investigation was based in part on a November 2024 whistleblower complaint to the SEC.[37]

[32] Jake Bleiberg, *supra* note 4.

[33] *Id*.

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] *Id*.

34. Defendants' core claim that WhatsApp messages are accessible only to chat participants is false.

III. The Value of *Truly* Private, End-to-End Encrypted Messages Cannot Be Overstated

35. In an age where (i) Meta can trace Facebook users' every click and scroll and (ii) Internet surfers are called on to choose (or ignore) cookie preferences multiple times per day, invasions of online privacy can too easily be undervalued. But that is not the case for the perceived private substance of WhatsApp users' encrypted communications, which both WhatsApp and Meta have conditioned WhatsApp users to believe are inviolate.

36. Digital communications are an essential (and even the primary) component of how people develop and conduct their most intimate relationships today.[38] Intimacy requires self-disclosure and vulnerability, which depends on a sense of control (*i.e.*, privacy).[39] Fear that communications may be monitored by others can thus produce chilling effects that inhibit authentic disclosure. Without reasonable expectations of privacy in digital communication, individuals will avoid the authentic self-disclosure necessary for intimate relationships and engage in self-censorship.[40] Accordingly, privacy of digital communications is essential to the development of most close personal and intimate relationships in the modern era.

---

[38] *See, e.g.*, Samuel Hardman Taylor & Natalya N. Bazaroya, *Always Available, Always Attached: A Relational Perspective on the Effects of Mobile Phones and Social Media on Subjective Well-Being*, 26 *J. of Comp.-Mediated Commc'n* 187, 188 (Aug. 24, 2021) https://doi.org/10.1093/jcmc/zmab004.

[39] *See, e.g.*, Avelle Stuart, Arosha K. Bandara & Mark Levine, *The Psychology of Privacy in the Digital Age*, 13 Soc. Personal. Psychol. Compass e12507, 2 (Nov. 2019), https://compass.onlinelibrary.wiley.com/doi/10.1111/spc3.12507.

[40] *See, e.g.*, Moritz Büchi, Noemi Festic & Michael Latzer, *The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda*, 9 Big Data & Society (2022), https://doi.org/10.1177/20539517211065368.

IV. Meta's History of Blatant Disregard for User Privacy and Subsequent Cover-Ups

37. Over the years, Meta's name has become synonymous with user privacy violations. Again and again, Meta/Facebook has violated users' privacy rights by using their information in undisclosed ways, such as disclosing their personal data *en masse* to third parties with no verified need for the information in violation of stated privacy policies, failing to apprise users of data breaches—such as the infamous 2016 Cambridge Analytica scandal—and then affirmatively misleading the public as to whether such breaches had occurred. One would think Meta would have learned from this history. It clearly has not.

38. For example, on November 29, 2011, the United States Federal Trade Commission ("FTC") announced Facebook had agreed to enter into a 20-year consent order (finalized in 2012) to settle an eight-count complaint that alleged Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing [that information] to be shared and made public."[41] Among other things, the FTC charged Facebook with (i) failing to warn users that information they designated private (such as their "Friends List[s]") would be made public; (ii) giving third-party apps access to "nearly all of users' personal data"—data the apps did not need—despite Facebooks representations these apps would have access only to user information needed to operate; (iii) misrepresenting to users that they could restrict data sharing to "Friends Only" when that information was shared with third-party applications their friends used; (iv) claiming it certified the security of apps in its "Verified Apps" program when it did not;

[41] Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises; Agreement Containing Consent Order, *In re Facebook, Inc.*, No. 092 3184 (FTC Nov. 11, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/A3EW-U2FR].

(v) falsely promising it would not share users' personal information with advertisers; and (vi) allowing access to users' photos and videos even after users deactivated or deleted their accounts, despite claiming they would be inaccessible.[42]

39. The consent order (among other things) barred Facebook from making any further misrepresentations about the privacy or security of consumers' personal information; required Facebook to get consumers' affirmative express consent before enacting changes overriding their privacy preferences; required Facebook to establish and maintain a "comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services and to protect the privacy and confidentiality of consumers' information"; and subjected Facebook to periodic assessments of its privacy practices by independent, third-party auditors for the 20-year life of the consent order.[43]

40. The FTC commenced a wide-ranging investigation into Facebook's continuing privacy violations in March 2018 that began with the revelation of Cambridge Analytica's use of data from tens of millions of Facebook users to build voter profiles and expanded from there.[44] On July 24, 2019, the FTC announced it was levying a historic ***$5 billion*** penalty against Facebook (approved by a court in 2020) for violations of the 2012 consent order, which was "the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the

[42] Press Release FTC (Nov. 29, 2011), *supra* note 41.

[43] *Id.*

[44] Tony Romm & Craig Timberg, *FTC Opens Investigation into Facebook After Cambridge Analytica Scrapes Millions of Users' Personal Information*, Wash. Post (Mar. 20, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/ [https://perma.cc/Q9GX-FXRF].

largest privacy or data security penalty ever imposed worldwide" and "one of the largest penalties ever assessed by the U.S. government for any violation" of any kind.[45]

41. As then-FTC Chairman Joe Simons explained, "[d]espite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers' choices."[46] Specifically, notwithstanding the 2012 consent order, Facebook "repeatedly used deceptive disclosures and settings to undermine users' privacy preferences" and "share[d] users' personal information with third party-apps that were downloaded by the user's Facebook 'friends.'"[47]

42. In addition to requiring Facebook to pay $5 billion in fines, the 2019 announcement required Facebook CEO Mark Zuckerberg (and others) to submit independently to the FTC quarterly certifications that Facebook is compliant with the privacy program mandated by the order and annual certifications that Facebook is in overall compliance with the order. Any false certifications can subject the signatories to individual civil and criminal penalties.[48]

43. Unfortunately, the FTC grossly overestimated the impact of the $5 billion fine and strengthened reporting requirements on trillion-dollar Meta. Indeed, the value of Facebook's stock actually *went up* by 1% following the announcement of the $5 billion penalty; the market—like Facebook—realized that "despite the penalty's unprecedented size," it was "still just a drop in the

---

[45] Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook: FTC Settlement Imposes Historic Penalty, and Significant Requirements To Boost Accountability and Transparency (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/R2MJ-D58R].

[46] *Id.*

[47] *Id.*; Compl. for Civ. Penalties, Inj., & Other Relief, *United States v. Facebook, Inc.*, No. 19-cv-2185 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf [https://perma.cc/WX7G-TTUA].

[48] Press Release, FTC (July 24, 2019), *supra* note 45.

ocean compared to the gigantic amount of cash Facebook regularly produces."[49] Following the announcement of the penalty, Facebook CEO Mark Zuckerberg's shares increased in value by more than $1 billion in just thirty minutes.[50]

44. Although the FTC claimed the $5 billion penalty was "designed . . . to change Facebook's entire privacy culture to decrease the likelihood of continued violations,"[51] as the facts alleged in this Petition show, Meta has not only failed to "change [its] entire privacy culture," but has continued full speed ahead and business-as-usual in both its violations of its users' privacy and its misleading claims to the public regarding their privacy.

45. Indeed, in May 2023, the FTC charged Meta with violations of the 2020 order that was entered at the conclusion of the 2019 proceedings, alleging (among other things) that Meta had "misled parents about their ability to control with whom their children communicated through its Messenger Kids app" and "misrepresented the access it provided some app developers to private user data."[52] Once again, the FTC expressed its dismay with Meta's behavior, with the Director of the FTC's Bureau of Consumer Protection stating, "Facebook has repeatedly violated its privacy

---

[49] Rob Price, *Why Facebook's Stock Jumped Despite Facing a Record-Breaking $5 Billion FTC Penalty: 'A Slap on the Wrist*, Business Insider (July 12, 2019), https://www.businessinsider.com/facebook-stock-rose-news-5-billion-ftc-settlement-why-critics-2019-7 [https://perma.cc/UFG2-9TEU].

[50] Ben Gilbert, *Mark Zuckerberg Actually Got $1 Billion Richer Following the News of Facebook's $5 Billion Fine for the Biggest Scandal in the Company's History*, Business Insider (July 15, 2019), https://www.businessinsider.com/mark-zuckerberg-net-worth-increases-after-5-billion-facebook-fine-2019-7 [https://perma.cc/F5CW-UCDF].

[51] Press Release, FTC (July 24, 2019), *supra* note 45.

[52] Press Release, FTC, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data; FTC Says that the Company Violated 2020 Privacy Order; Proposes New Protections for Children and Teens (May 3, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data [https://perma.cc/EM25-WMK2].

promises. The company's recklessness has put young users at risk, and Facebook needs to answer for its failures."[53] These proceedings against Meta are ongoing.

46. The SEC also fined then-Facebook $100 million for misleading the public regarding the Cambridge Analytica data breach.[54] For more than two years, Facebook knew Cambridge Analytica had actually used tens of millions of Facebook users' data, but misrepresented the risk of misuse of user data as a purely hypothetical occurrence in its communications to investors (and, by extension, the public generally).[55] The SEC noted "Facebook exacerbated its disclosure failures when it misled reporters who asked the company about its investigation into Cambridge Analytica."[56]

47. Meta's disregard for user privacy has also resulted in European regulators imposing penalties against it totaling billions of dollars for its repeated violation of the General Data Protection Regulation (GDPR). For example, in November 2022, the Irish Data Protection Commission fined Meta €265 million for a massive data leak that occurred between 2018 and 2019 and was discovered in 2021.[57] That leak resulted in the data—including mobile numbers, Facebook IDs, names, genders, locations, relationship statuses, occupations, dates of birth, and

---

[53] *Id.*

[54] Press Release, SEC, *Facebook To Pay $100 Million for Misleading Investors About the Risks It Faced from Misuse of User Data* (July 24, 2019), https://www.sec.gov/newsroom/press-releases/2019-140 [https://perma.cc/GW2J-G8XM].

[55] *Id.*

[56] *Id.*

[57] Press Release, An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission) ("IDPC"), Data Protection Commission Announces Decision in Facebook "Data Scraping" Inquiry (Nov. 28, 2022), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry#Meta [https://perma.cc/3964-T4NZ]; Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*, NPR (Apr. 9, 2021), https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users [https://perma.cc/4ZUM-PCEE].

email addresses—of 533 million Facebook users in 106 countries worldwide appearing in a public hacking forum.[58] In addition to drawing the ire and penalties of regulators, Meta's initial decision ***not to notify impacted users individually*** was roundly condemned by security experts because the data could be used for targeted phishing attacks and identity theft.[59]

48. In January 2023, the Irish Data Protection Commission fined Meta €390 million for improperly processing user data for targeted advertising purposes in violation of the GDPR.[60]

49. Then, on May 22, 2023, the Irish Data Protection Commission, acting on findings by the European Data Protection Board, imposed the largest GDPR fine ever issued—€1.2 billion—on Meta's Irish subsidiary for "systematic, repetitive and continuous" illegal transfers of the personal data of millions of European users to the United States.[61]

50. On September 27, 2024, the Irish Data Protection Commission fined Meta €91 million for storing user passwords in plain text (without encryption or other protective measures).[62] As the Data Protection Deputy Commissioner noted, "It is widely accepted that user passwords should not be stored in plaintext, considering the risks of abuse that arise from persons accessing

---

[58] *Id*.

[59] *Id.*; *Facebook Breach Exposes 533 Million Users*, Sec. (Apr. 6, 2021), https://www.securitymagazine.com/articles/94962-facebook-breach-exposes-533-million-users [https://perma.cc/H56Q-4Z4H].

[60] Press Release, IDPC, Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland (Jan. 4, 2023), https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland#Meta [https://perma.cc/DMX8-D7JU].

[61] Press Release, European Data Protection Board, 1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision" (May 22, 2023), https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en [https://perma.cc/BH2U-YAPX].

[62] Press Release, IDPC, Irish Data Protection Commission Fines Meta €91 Million (Sept. 27, 2024), https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta#Meta [https://perma.cc/6QSD-RQ5A].

such data. It must be borne in mind, that the passwords the subject of consideration in this case, are particularly sensitive, as they would enable access to users' social media accounts."[63] Notably, although the violation was self-reported by Meta in 2019, regulators reprimanded Meta's Irish subsidiary for failing to report and document the violation appropriately.[64] According to one Facebook source, between 200 million and 600 million users' account passwords were plaintext searchable by more than 20,000 Facebook employees, and some 2,000 engineers and developers made approximately nine million internal queries for data elements that contained plain text user passwords during the time the passwords were mishandled.[65]

51. Yet again, on December 17, 2024, the Irish Data Protection Commission imposed an additional €251 million fine on Meta for a 2018 data breach compromising data including the full names, email addresses, phone numbers, locations, places of work, dates of birth, religions, genders, timeline posts, group memberships, and children's personal data of approximately 29 million users, including 3 million users in Europe.[66] Once again, the Data Protection Commission reprimanded Meta for failing to document and make a full disclosure to the Commission regarding the breach.[67] The Deputy Commission noted the severity and dangers of the breach: "[F]ailure to build in data protection requirements . . . can expose individuals to very serious risks and harms, including a risk to the fundamental rights and freedoms of individuals. Facebook profiles can, and

---

[63] *Id.*

[64] *Id.*

[65] Brian Krebs, *Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years*, Krebs on Sec. (Mar. 21, 2019), https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/ [https://perma.cc/2EPK-TQLN].

[66] Press Release, IDPC, Irish Data Protection Commission Fines Meta €251 Million" (Dec. 17, 2024), https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million [https://perma.cc/73G3-ZMVH].

[67] *Id.*

often do, contain information about matters such as religious or political beliefs, sexual life or orientation, and similar matters that a user may wish to disclose only in particular circumstances."[68]

52. These examples of regulatory penalties imposed on Meta and Facebook are merely representative and not exhaustive (even for Europe/Ireland). Yet they reveal a pattern of misconduct: Meta violates or disregards user privacy, fails to disclose or document the full extent of the problem, receives its "punishment" from regulators in the form of fines that—even at hundreds of millions of pounds—barely register on Meta's balance sheet, and continues on, business as usual.

53. Aside from privacy violations, on May 18, 2017, European regulators also fined then-Facebook for providing "incorrect or misleading information" during European review of Facebook's acquisition of WhatsApp in 2014.[69] Specifically, Facebook assured regulators that any technical integration of Facebook and WhatsApp users accounts could not be accomplished reliably.[70] Yet in 2016, when WhatsApp announced changes in its Terms of Service and Privacy Policy, it expressly included the possibility of linking WhatsApp users' phone numbers with Facebook user identities—precisely what Facebook had assured European regulators it could not do.[71] Although the European Commission did not take steps to unwind the long-closed merger, it fined Facebook, finding that contrary to Facebook's statements to regulators during the merger review process, "the technical possibility of automatically matching Facebook and WhatsApp

---

[68] *Id.*

[69] Press Release, Eur. Comm'n, Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information About WhatsApp Takeover (May 18, 2017), https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1369 [https://perma.cc/4LQC-8FXC].

[70] *Id.*

[71] *Id.*

users' identities already existed in 2014, and that Facebook staff were aware of such a possibility."[72] Accordingly, Meta's and WhatsApp's false claims it cannot access WhatsApp users' encrypted communications are not the first time Meta has misrepresented its technical capabilities with respect to WhatsApp' users data.

54. At the same time regulators have been reprimanding and fining Meta for its repeated privacy violations and failures to safeguard users' information, Meta has downsized several of the very business units charged with user protection. For example, Meta recently laid off more than 100 people in its risk review organization, which includes the employees responsible for making sure Meta's platforms comply with its obligations under the FTC consent order and privacy requirements imposed by regulatory bodies worldwide.[73] Meta employees described the layoffs "as a 'gutting' of the workers in the department who review projects at Meta for privacy and integrity risks."[74] According to Meta insiders, "Meta executives have become frustrated with the pace of product development," and "[o]ne division holding things up—by design—was the company's risk organization."[75] Although Meta claims the layoffs reflect a transition to automated processes that will be superior to manual review, "[c]urrent and former employees in the risk organization said they were skeptical that replacing [the laid-off employees] with automated systems would be as effective, particularly around issues as sensitive as user privacy."[76]

---

[72] *Id*.

[73] Mike Isaac & Eli Tan, *Meta Layoffs Included Employees Who Monitored Risks to User Privacy*, N.Y. Times (Oct. 23, 2025), https://www.nytimes.com/2025/10/23/technology/meta-layoffs-user-privacy.html [https://perma.cc/5A7H-QA4R].

[74] *Id.*

[75] *Id.*

[76] *Id.*

55. Meta also has a prolific track record of deceiving the public. In addition to its concealment of the Cambridge Analytica data breach and its repeated censure by European regulators for its failure to disclose breaches fully, Meta has come under fire for its concealment and misrepresentation of information regarding risks posed by its platforms. As but one example, former Facebook employee and whistleblower Frances Haugen's 2021 disclosure of "The Facebook Papers" revealed that Meta had conducted internal research regarding the negative impact of Instagram on teenage mental health (concluding, for example, that "[w]e [Facebook-owned Instagram] make body image issues worse for one in three teen girls"), yet concealed these findings from regulators and the public while downplaying these risks to the public.[77] Meta reportedly abandoned a research project into the effects of a Facebook/Instagram hiatus after data suggested users benefited. One Meta employee warned Meta's concealment of its research findings could be likened to the tobacco industry's concealment of negative research findings relating to the dangers of cigarettes.[78]

56. According to filings in a recent multi-district litigation against Meta by parents, children, school districts, and state attorneys general, Meta "was aware that millions of adult strangers were contacting minors on its sites; that its products exacerbated mental health issues in

---

[77] Georgia Wells, Jeff Horowitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sept. 14, 2021), https://www.wsj.com/tech/personal-tech/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 [https://perma.cc/W353-Z5PD]; Vanessa Romo, *Whistleblower's Testimony Has Resurfaced Facebook's Instagram Problem*, NPR (Oct. 5, 2021), https://www.npr.org/2021/10/05/1043194385/whistleblowers-testimony-facebook-instagram [https://perma.cc/P2FM-RVB5]; Jane Wakefield, *Facebook Under Fire Over Secret Teen Research*, BBC (Sept. 15, 2021), https://www.bbc.com/news/technology-58570353 [https://perma.cc/66J2-PQJM]; Clare Duffy, *Lawsuit Alleges Social Media Giants Buried Their Own Research on Teen Mental Health Harms*, CNN (Nov. 26, 2025), https://www.cnn.com/2025/11/25/tech/social-media-youth-mental-health-lawsuit-meta-tiktok-snap-youtube [https://perma.cc/JME8-R2SD].

[78] *Id.*

teens; and that content related to eating disorders, suicide, and child sexual abuse was frequently detected, yet rarely removed," but Meta failed to disclose these dangers to the public or to Congress.[79] In fact, when the Senate Judiciary Committee asked Meta in written questions in December 2020 whether it could "determine whether increased use of its platform among teenage girls has any correlation with increased signs of depression" and "increased signs of anxiety," the company answered simply "No."[80]

57. On November 14, 2023, a bipartisan group of United States Senators sent a letter to Meta CEO Mark Zuckerberg accusing Meta of misleading Congress.[81] According to these Senators, "Meta's representations to the public and in response to Congressional inquiries concealed and misrepresented its extensive knowledge about the threats to young people on its platforms."[82] They also stated: "Members of Congress have repeatedly asked Meta for information on its awareness of threats to young people on its platforms and the measures that it has taken, only to be stonewalled and provided non-responsive or misleading information. . . . Rather than act on the stunning findings, Meta hid this information from the public and Congressional oversight while providing misleading statistics, ignoring recommendations to protect teens, and

[79] Charlotte Alter, *Court Filings Allege Meta Downplayed Risks to Children and Misled the Public*, Time (Nov. 22, 2025), https://time.com/7336204/meta-lawsuit-files-child-safety/ [https://perma.cc/FY73-NEPW].

[80] *Id.*

[81] Press Release, Sen. Dick Durbin, Durbin, Blumenthal, Bipartisan Group of Senators Demand Documents from Mark Zuckerberg After Newly Unsealed Court Filing Alleges Meta Hid Evidence of Harms to Kids: Newly Unsealed Disclosures Suggest Meta Executives' Direct Knowledge of the Harms of Its Product & Concealment from Congress and the Public, Supporting Whistleblower Arturo Béjar's Testimony to the Senate Judiciary Committee (Nov. 15, 2023), https://www.durbin.senate.gov/newsroom/press-releases/durbin-blumenthal-bipartisan-group-of-senators-demand-documents-from-mark-zuckerberg-after-newly-unsealed-court-filing-alleges-meta-hid-evidence-of-harms-to-kids [https://perma.cc/D9CW-P8MJ].

[82] *Id.*

even rolling back safety tools."[83] That Meta is misleading the public, the U.S. Congress and regulators worldwide regarding the extensive evidence of the risks its platforms to teens is consistent with what one whistleblower described as Meta's fostered culture of "see no evil, hear no evil."[84]

58. Meta's documented misrepresentations are not limited to risks to youth posed by its platform. Meta has also recently come under fire for misrepresenting its activities in China and sharing of certain user data with the Chinese Communist Party following the release of former Meta employee Sarah Wynn-Williams' best-selling, revealing memoir, *Careless People*.[85]

59. As one Republican U.S. Senator said of Mark Zuckerberg's testimony over the course of multiple Congressional hearings, "[e]very time it's a different answer. Every time it's a different façade. But every time the one consistent through-line is every time it's something misleading. Every time is something other than the truth."[86]

60. The pattern is clear: Meta has a rich track record of (i) choosing profit and "efficiency" over meaningful user protections; and (ii) speaking in half-truths (at best) when it comes to reporting breaches or other potentially negative information to the public, investors, and regulators. Because even record-breaking fines imposed by regulators are essentially rounding errors to Meta's bottom line, Meta's conduct continues undeterred and unabated, as evidenced by

---

[83] *Id.*

[84] Dara Kerr, *Meta Failed To Address Harm to Teens, Whistleblower Testifies as Senators Vow Action*, NPR (Nov. 7, 2023), https://www.npr.org/2023/11/07/1211339737/meta-failed-to-address-harm-to-teens-whistleblower-testifies-as-senators-vow-act [https://perma.cc/Y5BJ-NPR8].

[85] David Ingram, *Senators Vow to Keep Investigating Meta Over Its China Record After Ex-Employee Testifies*, NBC News (Apr. 9, 2025), https://www.nbcnews.com/tech/social-media/facebook-meta-whistleblower-senate-video-book-careless-people-rcna200517 [https://perma.cc/8KAU-A93V].

[86] *Id.*

Meta's brazen willingness to mislead WhatsApp users regarding its and WhatsApp's ability to access users' encrypted communications.

CAUSE OF ACTION

Count I — DTPA Violations (All Defendants)

61. The State re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

62. The State may bring an action against a person when it has reason to believe the person is engaging in, has engaged in, or is about to engage in any act or practice declared unlawful under the DTPA. Tex. Bus. & Com. Code Ann. § 17.47(a).

63. The DTPA prohibits all false, misleading, or deceptive acts or practices in the conduct of any trade or commerce. Tex. Bus. & Com. Code Ann. § 17.46(a).

64. Defendants are "persons" as defined by the section 17.45(3) of the Texas Business and Commerce Code.

65. Defendants have, while engaged in trade and commerce, engaged in false, misleading, and deceptive acts and practices declared unlawful by sections 17.46(a) and (b) of the DTPA, including, but not limited to:

a. Representing, directly or by implication, that Defendants were unable to and would not access the contents of communications of WhatsApp users when in fact Defendants were able to and did access the contents of the communications of WhatsApp users in violation of Texas Business and Commerce Code section 17.46(b)(5);

b. Representing, directly or by implication, that Defendants' services have characteristics, uses, or benefits that they do not have by claiming, among other things, that "all your personal messages stay between you and who

you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them" in violation of Texas Business and Commerce Code section 17.46(b)(5); and

c. Failing to disclose information concerning goods or services that was known at the time with the intent to induce users into using Defendants' goods and services, which users would not have done had the information been disclosed in violation of Texas Business and Commerce Code section 17.46(b)(24).

JURY TRIAL DEMAND

66. The State requests a jury trial and tenders the jury fee to the Harrison County District Clerk's Office pursuant to Texas Rule of Civil Procedure 216 and Texas Government Code section 51.604.

PRAYER

67. The State prays that the Court enter judgment in its favor and, among other things:

a. Enter a permanent injunction enjoining Defendants and their officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise, from accessing the content of any Texan's WhatsApp communications absent their consent;

b. Order Defendants to pay civil penalties to the State in the amount of $10,000 per DTPA violation;

c. Order Defendants to pay pre-judgment and post-judgment interest on all monetary awards, as provided by law;

d. Order Defendants to pay all court costs, investigatory costs, and the State's attorneys' fees, as provided by law; and

e. Grant the State such other relief which is proper and just.

Dated: May 21, 2026

Respectfully submitted,

/s/Johnathan Stone

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

RALPH MOLINA
Deputy First Assistant Attorney General

AUSTIN KINGHORN
Deputy Attorney General for Civil Litigation

JOHNATHAN STONE, Lead Counsel
Chief, Consumer Protection Division
Texas State Bar No. 24071779

JERRY BERGMAN
Deputy Chief, Consumer Protection Division
Texas State Bar No. 24081694

JOHN C. HERNANDEZ
Assistant Attorney General
Texas State Bar No. 24095819

KAYLIE BUETTNER
Assistant Attorney General
Texas State Bar No. 24109082

Consumer Protection Division
Office of the Texas Attorney General
P.O. Box 12548
Austin, Texas 78711
Telephone: (512) 463-2185
Fax: (512) 473-8301

Johnathan.Stone@oag.texas.gov
Jerry.Bergman@oag.texas.gov
JC.Hernandez@oag.texas.gov
Kaylie.Buettner@oag.texas.gov

Ashley C. Keller (*pro hac vice* forthcoming)
J. Dominick Larry (*pro hac vice* forthcoming)
Keller Postman LLC
150 N. Riverside Plaza, Suite 4100
Chicago, IL 60606
Telephone: (312) 741-5220
ack@kellerpostman.com
nl@kellerpostman.com

John J. Snidow (*pro hac vice* forthcoming)
Keller Postman LLC
1101 Connecticut Ave. NW, Suite 1100
Washington, DC 20036
Telephone: (202) 918-1123
jj.snidow@kellerpostman.com
john.masslon@kellerpostman.com
roseann.romano@kellerpostman.com

/s/ Lauren E. Schultz
Lauren E. Schultz (TX Bar No. 24071496)
Keller Postman LLC
2333 Ponce de Leon Blvd., Suite R-240
Coral Gables, FL 33134
Telephone: (312) 896-4516
lauren.schultz@kellerpostman.com

Counsel for the State of Texas

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Glenn Gallegos on behalf of Johnathan Stone
Bar No. 24071779
glenn.gallegos@oag.texas.gov
Envelope ID: 115189152
Filing Code Description: Plaintiff'S Original Petition
Filing Description: 20260521 Plaintiffs Original Petition_WhatsApp
Status as of 5/21/2026 11:34 AM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Kaylie Buettner		Kaylie.Buettner@oag.texas.gov	5/21/2026 10:14:48 AM	SENT
Olivia Adendorff		olivia.adendorff@kirkland.com	5/21/2026 10:14:48 AM	SENT
Winn Allen		winn.allen@kirkland.com	5/21/2026 10:14:48 AM	SENT
Jordan L.Greene		jordan.greene@kirkland.com	5/21/2026 10:14:48 AM	SENT
Jerry Bergman		jerry.bergman@oag.texas.gov	5/21/2026 10:14:48 AM	SENT
JC Hernandez		jc.hernandez@oag.texas.gov	5/21/2026 10:14:48 AM	SENT
Ashley Keller		ack@kellerpostman.com	5/21/2026 10:14:48 AM	SENT
John Snidow		jj.snidow@kellerpostman.com	5/21/2026 10:14:48 AM	SENT
John Masslon II		john.masslon@kellerpostman.com	5/21/2026 10:14:48 AM	SENT
Roseann R. Romano		roseann.romano@kellerpostman.com	5/21/2026 10:14:48 AM	SENT
J. Dominick Larry		nl@kellerpostman.com	5/21/2026 10:14:48 AM	SENT
Andrea Thomas		andrea.thomas@oag.texas.gov	5/21/2026 10:14:48 AM	SENT
Glenn Gallegos		glenn.gallegos@oag.texas.gov	5/21/2026 10:14:48 AM	SENT