KESSLER TOPAZ
MELTZER & CHECK, LLP
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

KESSLER TOPAZ
MELTZER & CHECK, LLP
Joseph H. Meltzer (*pro hac vice* forthcoming)
jmeltzer@ktmc.com
Melissa L Yeates (*pro hac vice* forthcoming)
myeates@ktmc.com
Tyler S. Graden (*pro hac vice* forthcoming)
tgraden@ktmc.com
Jordan E. Jacobson (Bar No. 302543)
jjacobson@ktmc.com
Daniel S. Dicce (*pro hac vice* forthcoming)
ddicce@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiffs and the putative Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

BRIAN Y. SHIRAZI and NIDA SAMSON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC., WHATSAPP LLC, ACCENTURE PLC, and ACCENTURE LLP,

Defendants.

Case No. 26-cv-2615

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I. INTRODUCTION 1

II. JURISDICTION AND VENUE 3

III. PARTIES 4

A. Plaintiffs 4

B. Defendants 5

IV. FACTUAL ALLEGATIONS 5

A. Plaintiffs and Class Members Send Communications on the WhatsApp Platform 5

B. WhatsApp's Terms of Service Promise Plaintiffs and Other Users That Their Messages are Private 6

C. WhatsApp Markets Itself as a Secure Platform Where Users May Send Private Messages 7

D. Unbeknownst to Plaintiffs and Other Users, WhatsApp, Meta, Their Employees, and Third-Party Contractors, Including those Employed by Accenture, Have Access to Users' Communications 12

E. Plaintiffs and Class Members Did Not Consent to WhatsApp Intercepting, Reading, Storing, Accessing, and/or Viewing Their Communications Sent on the WhatsApp Platform and Sharing Their Communications With Third-Parties, Including Accenture and its Employees 17

F. Plaintiffs and Other WhatsApp Users Have a Reasonable Expectation That Their Communications are Private 18

G. Meta Consistently Fails to Protect Users' Privacy 20

H. Tolling 22

V. CLASS ACTION ALLEGATIONS 23

VI. CLAIMS FOR RELIEF 26

VII. PRAYER FOR RELIEF 50

VIII. DEMAND FOR JURY TRIAL 51

Plaintiffs Brian Y. Shirazi ("Plaintiff") and Nida Samson ("Plaintiff" and collectively "Plaintiffs") bring this proposed class action against Meta Platforms, Inc. ("Meta"),WhatsApp, LLC ("WhatsApp"), Accenture PLC ("Accenture"), and Accenture LLP (together with Accenture PLC, "Accenture")[1] individually and on behalf of all others similarly situated.[2]

I. INTRODUCTION

1. As any reasonable user would, Plaintiffs trusted WhatsApp, a popular messaging service, to abide by its foundational, years-long promises to keep users' messages private between senders and recipients. Since its inception in 2009, WhatsApp has consistently branded and marketed itself as a private and secure messaging service, explicitly stating that: "[w]ith end-to-end encryption on WhatsApp, your personal messages and calls are secured with a lock. ***Only you and the person you're talking to can read or listen to them***, and no one else, ***not even WhatsApp***."[3] WhatsApp further markets its platform as allowing users to "***[m]essage privately***."[4] And, reinforcing its supposed commitment to private messaging, WhatsApp also tells users: "[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."[5]

2. WhatsApp also states that "we do not keep logs of who everyone is messaging or calling."[6] Such statements were reinforced by Mark Zuckerberg, the Chairman and CEO of Meta which has owned WhatsApp since 2014, in sworn public Congressional testimony in which he

[1] Meta, WhatsApp, and the Accenture Defendants are collectively referred to herein as "Defendants."

[2] The allegations herein are based on personal knowledge as to Plaintiffs' own conduct, and are made on information and belief as to all other matters, based on an investigation by counsel. Upon information and belief, Plaintiffs submit that discovery will further support the allegations in this Class Action Complaint ("Complaint").

[3] WhatsApp, https://www.whatsapp.com/ (last visited Mar. 24, 2026).

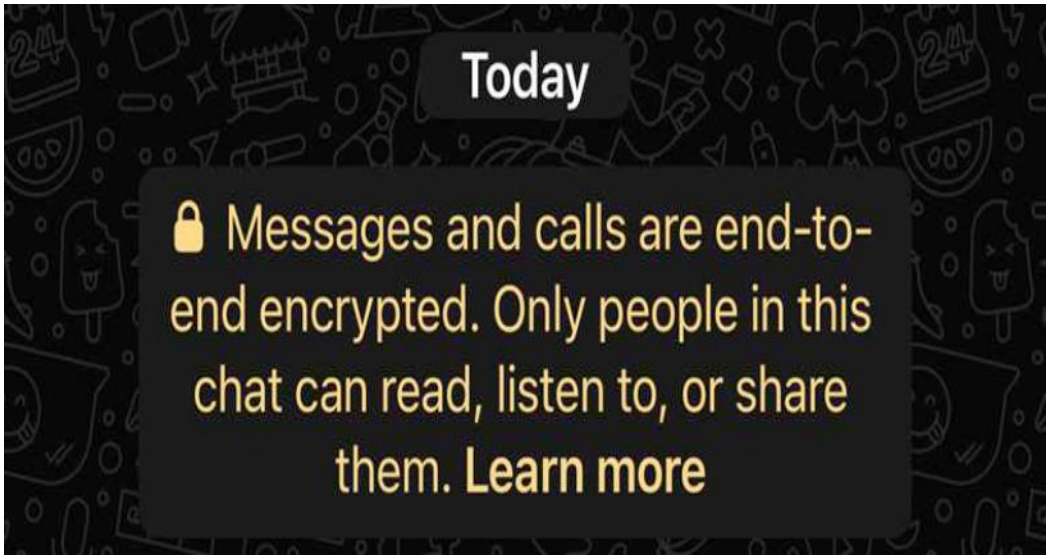
[4] *Id.*

[5] *Privacy*, WhatsApp, https://www.whatsapp.com/privacy (last visited Mar. 24, 2026).

[6] *Answering your questions about privacy on WhatsApp: What kind of information can WhatsApp see about how I'm using WhatsApp?*, WhatsApp, https://www.whatsapp.com/privacyquestions (last visited Mar. 24, 2026).

testified, "we do not see any of the content in WhatsApp; it is fully encrypted . . . Facebook systems do not see the content of messages being transferred over WhatsApp."[7]

3. WhatsApp also displays the following message before a user sends a new chat on WhatsApp, again assuring all users that the messages that they send on WhatsApp are supposedly private between sender(s) and recipient(s).



This message is displayed each time a user begins a new chat on WhatsApp.

4. Given WhatsApp's supposed commitment to keeping messages sent by users private, Plaintiffs reasonably believed that the messages they sent on WhatsApp were fully secure and not viewed by or shared with any third parties who were not recipients of messages sent by Plaintiffs. Plaintiffs further reasonably believed that neither WhatsApp, Meta, their respective employees, nor contractors employed by Accenture or other third parties could see the content of messages Plaintiffs sent on WhatsApp.

5. Notwithstanding Plaintiffs' and other WhatsApp users' reasonable expectation that their messages sent on the WhatsApp platform would not be viewed by, shared, seen, or stored by individuals who were not intended recipients of the messages, in truth, WhatsApp and its parent company Meta secretly intercept, read, store, access, and/or view the supposedly private messages

[7] *Facebook, Social Media Privacy, and the Use and Abuse of Data*: *Hearing Before the S. Comm. on Commerce, Science, and Transportation, and the S. Comm. on the Judiciary*, 115th Cong. 8 (2018) (Statement of Mark Zuckerberg, Chairman and Chief Executive Officer, Facebook), https://www.congress.gov/event/115th-congress/senateevent/LC64510/text.

users send on the WhatsApp platform and conspire to permit Accenture employees to also read, access, and/or view supposedly private messages.

6. Specifically, unbeknownst to Plaintiffs and other WhatsApp users, WhatsApp, Meta, their respective employees, Accenture contractors, and/or third parties had access to users' supposedly private and encrypted messages.[8] Indeed, according to recent reporting, whistleblowers have informed federal investigators that Meta employees and third-party contractors had "broad access to the substance of WhatsApp messages that were supposed to be encrypted and inaccessible" and can look "back aways into WhatsApp (encrypted) messages."[9] These revelations stand in stark contrast to WhatsApp's repeated commitments to keep messages private between senders and recipients.

7. WhatsApp's secret interception, reading, storing, accessing, and/or viewing of the messages it ensured Plaintiffs and similarly situated Class members were private, including without adequate disclosure to Plaintiffs and Class members, constitutes a serious invasion of Plaintiffs' and Class members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. Cons. Stat. §§ 5701 *et. seq*; the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.*; the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*; the California Constitution, Art. 1, § 1; common law intrusion upon seclusion; breach of express and implied contract; Statutory Larceny Through False Pretenses, Cal. Penal Code §§ 484, 496; the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*; and the California False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq.*

II. JURISDICTION AND VENUE

8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because this suit is brought under the laws of the United States, specifically the Electronic

[8] Jake Bleiberg, *US Has Investigated Claims WhatsApp Chats Aren't Private*, Bloomberg (Jan. 29, 2026, 17:22 ET), https://www.bloomberg.com/news/articles/2026-01-29/us-has-investigated-claims-that-whatsapp-chats-aren-t-private.

[9] *Id.*

Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because this is a proposed class action in which there are at least 100 Class members, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, and a member of the Class is a citizen of a different State than Defendant.

9. This Court also has supplemental jurisdiction over the state common law and statutory claims pursuant to 28 U.S.C. § 1367, as these claims are so related to the federal statutory claims over which this Court has original jurisdiction, that they form part of the same case or controversy.

10. This Court has general personal jurisdiction over Defendants because Defendants have sufficient minimum contacts with this District in that they operate and market their services throughout the region and in this District. Further, this Court has personal jurisdiction over Defendants because Defendants are headquartered in this District.

11. Venue is appropriate within this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' and the Classes' claims occurred in this District, Defendants conduct a substantial amount of business in this District, and Defendants are headquartered in this District.

12. No other forum would be more convenient for the parties and witnesses to litigate this case.

III. PARTIES

A. Plaintiffs

13. Plaintiff Brian Y. Shirazi is a citizen of California and resides in Los Angeles, California.

14. Plaintiff Shirazi downloaded the WhatsApp mobile application in or about April 2020 and created a WhatsApp account contemporaneously.

15. Plaintiff Shirazi regularly uses the WhatsApp platform to send and receive private messages, which he reasonably believed were encrypted and unable to be viewed by anyone other than the intended recipients.

16. Plaintiff Nida Samson is a citizen of Pennsylvania and resides in Media, Pennsylvania.

17. Plaintiff Samson downloaded the WhatsApp mobile application in or about March 2018 and created a WhatsApp account contemporaneously.

18. Plaintiff Samson regularly uses the WhatsApp platform to send and receive private messages, which she reasonably believed were encrypted and unable to be viewed by anyone other than the intended recipients.

B. Defendants

19. Defendant Meta Platforms, Inc. ("Meta") is a multinational technology conglomerate, organized and existing under the laws of the State of Delaware, and having its principal place of business in Menlo Park, California. Meta was initially incorporated in Delaware on July 29, 2004, as "TheFacebook, Inc." ("Facebook"). Facebook and Meta are collectively referred to as Meta in the Complaint. On October 28, 2021, the company assumed its current designation.

20. Defendant WhatsApp LLC ("WhatsApp") is a Delaware limited liability company, organized and existing under the laws of the State of Delaware, and having its principal place of business in Menlo Park, California. WhatsApp has been a wholly-owned subsidiary of Meta (then Facebook) since 2014.

21. Defendant Accenture PLC ("Accenture") is a multinational technology consulting company incorporated in Ireland, and having its principal place of business in Dublin, Ireland.

22. Defendant Accenture LLP ("Accenture") is a limited liability partnership. Accenture LLP has three partners: Accenture Inc., Accenture Sub II Inc., and Accenture LLC. Accenture Inc. and Accenture Sub II Inc. are incorporated under the laws of Delaware and have their principal places of business in Delaware. Accenture LLC has one member, Accenture Sub LLC. Accenture Sub LLC also has one member, Accenture Inc., which as noted above is incorporated in Delaware. Accenture LLP is a wholly owned subsidiary of Accenture PLC with which it has consolidated financial statements.

IV. FACTUAL ALLEGATIONS

A. Plaintiffs and Class Members Send Communications on the WhatsApp Platform

23. WhatsApp operates a mobile and desktop application on which users can send messages.

24. Users download WhatsApp from the Google Play Store, Apple App Store, or Microsoft Store to their mobile devices, or onto their computer desktop, and can create an account by accepting WhatsApp's Terms of Service and Privacy Policy and by providing a cell phone number and a profile name.

25. Once a user has created his or her profile, he or she is able to send written messages to other individuals on their mobile device as well as voice messages. Users may also make voice calls and video calls using the application.

26. Users may also transmit photographs and documents via messages on WhatsApp.

B. WhatsApp's Terms of Service Promise Plaintiffs and Other Users That Their Messages are Private

27. To create a user profile and begin using the platform, WhatsApp requires individuals to agree to its Terms of Service and Privacy Policy.[10]

28. By accepting WhatsApp's Terms of Service and incorporated Privacy Policy before creating a profile and using the platform, Plaintiffs and Class members enter into an express and/or implied contract with WhatsApp regarding the parties' respective rights, responsibilities, and obligations governing their conduct on the WhatsApp platform and messages sent on the WhatsApp platform, with the contract terms detailed by WhatsApp's Terms of Service and incorporated Privacy Policy.

29. Plaintiffs and other WhatsApp users provide WhatsApp with a valuable benefit by agreeing to the Terms of Service and Privacy Policy and by agreeing to use the platform and share metadata collected via cookies, usage and log information, device and connection information including IP addresses. In return, WhatsApp agrees to abide by the promises set forth in its Terms of Service and Privacy Policy.

30. The WhatsApp Terms of Service and incorporated Privacy Policy are available when an individual first downloads the application, are provided on WhatsApp's website, and are attached hereto as Exhibit 1 and 2 respectively.

[10] *How to get started on WhatsApp Messenger*, WhatsApp, https://www.whatsapp.com/coronavirus/get-started (last visited Mar. 24, 2026).

31. WhatsApp's Terms of Service begin with a clause detailing "Privacy and Security Principles" which asserts: "Since we started WhatsApp, we've built our Services with strong privacy and security principles in mind."[11]

32. The WhatsApp Terms of Service also state that the "laws of the State of California govern our Terms, as well as any Disputes . . . in court."[12]

33. WhatsApp's Privacy Policy states that: "We do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers."[13]

34. The Privacy Policy further asserts: "We offer end-to-end encryption for our Services. End-to-end encryption means that your messages are encrypted to protect against us and third parties from reading them."[14]

35. Significantly, nowhere does WhatsApp disclose to Plaintiffs and other users that WhatsApp, Meta, and their employees and/or Accenture contractors may access the messages sent by users on the WhatsApp platform.

36. Despite its express and implied assurances of privacy, WhatsApp has, in fact, secretly allowed access to and/or disclosed the contents of users' communications on the WhatsApp platform to itself, Meta, their employees and Accenture contractors, and/or other third parties.

C. WhatsApp Markets Itself as a Secure Platform Where Users May Send Private Messages

37. From its inception, WhatsApp has held itself out to users as a secure platform where users can send entirely private messages. Indeed, a 2009 blog post by WhatsApp co-founder Jan Koum stated: "We have not, we do not and we will not ever sell your personal information to anyone.

[11] *WhatsApp Terms of Service*, WhatsApp (effective Jan. 4, 2021), https://www.whatsapp.com/legal/terms-of-service.

[12] *Id.*

[13] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

[14] *Id.*

Period. End of story."[15] Similarly, in 2012, WhatsApp's co-founder stated: "[y]our data isn't even in the picture. We are simply not interested in any of it."[16]

38. When Meta acquired WhatsApp in 2014, the companies' co-founders publicly disclaimed concerns that this acquisition would compromise WhatsApp's commitment to privacy with Mr. Koum again writing a blog post regarding WhatsApp's supposed continued focus on privacy. Mr. Koum stated: "[r]espect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible."[17] Mr. Koum emphasized that WhatsApp had historically not collected private information and said "we really have no plans to change that"[18] and "[i]f partnering with Facebook meant that we had to change our values, we wouldn't have done it."[19] Mr. Koum then concluded, "[o]ur 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."[20]

39. Meta founder and CEO Mark Zuckerberg also made public statements assuring users that WhatsApp would continue to be a private message service stating "[t]he vision is to keep the service exactly the same," and that content on WhatsApp is deleted "almost instantly," which he acknowledged is "what people want" and that "we would be pretty silly to get in the way of that."[21]

40. Aware of users' desire to keep messages sent on WhatsApp private, in the years since Meta acquired WhatsApp, the company has continued to market itself as a secure, private messaging platform and has repeatedly assured Plaintiffs and other users that no one, including WhatsApp and Meta, can see users' messages sent on the platform.

---

[15] *Just wanted to say a few things*, WhatsApp Blog, (Nov. 19, 2009), https://blog.whatsapp.com/just-wanted-to-say-a-few-things.

[16] *Why we don't sell ads*, WhatsApp Blog, (June 18, 2012), https://blog.whatsapp.com/why-we-don-t-sell-ads.

[17] *Setting the Record Straight*, WhatsApp Blog, (Mar. 17, 2014), https://blog.whatsapp.com/setting-the-record-straight.

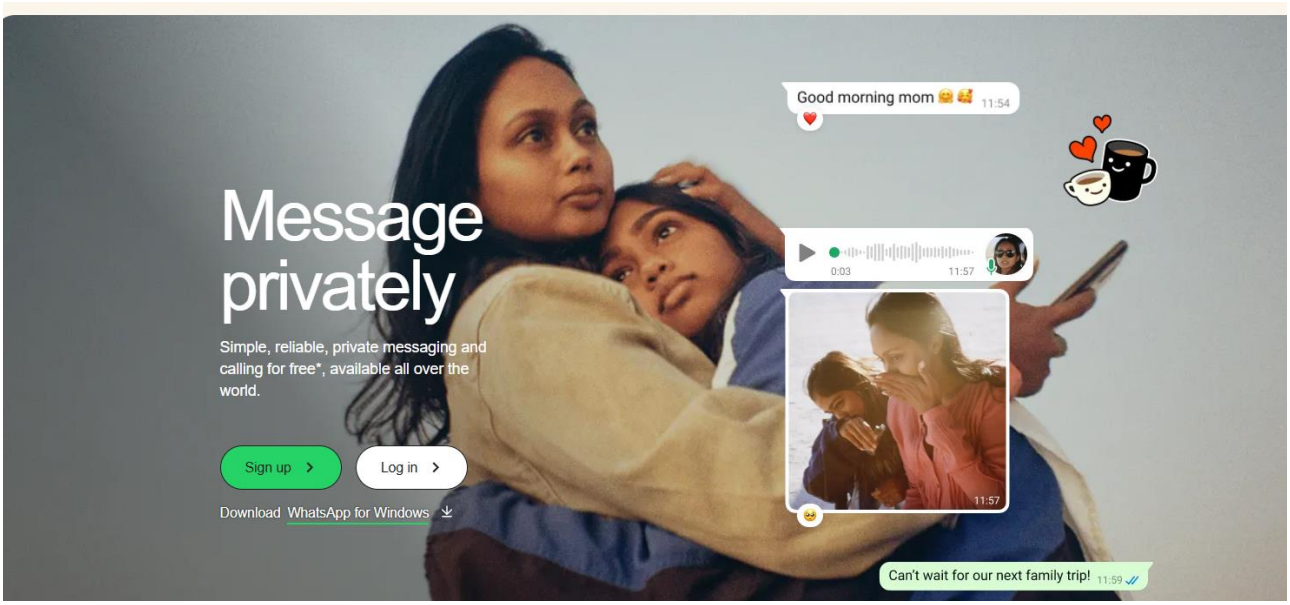
[18] *Id.*

[19] *Id.*

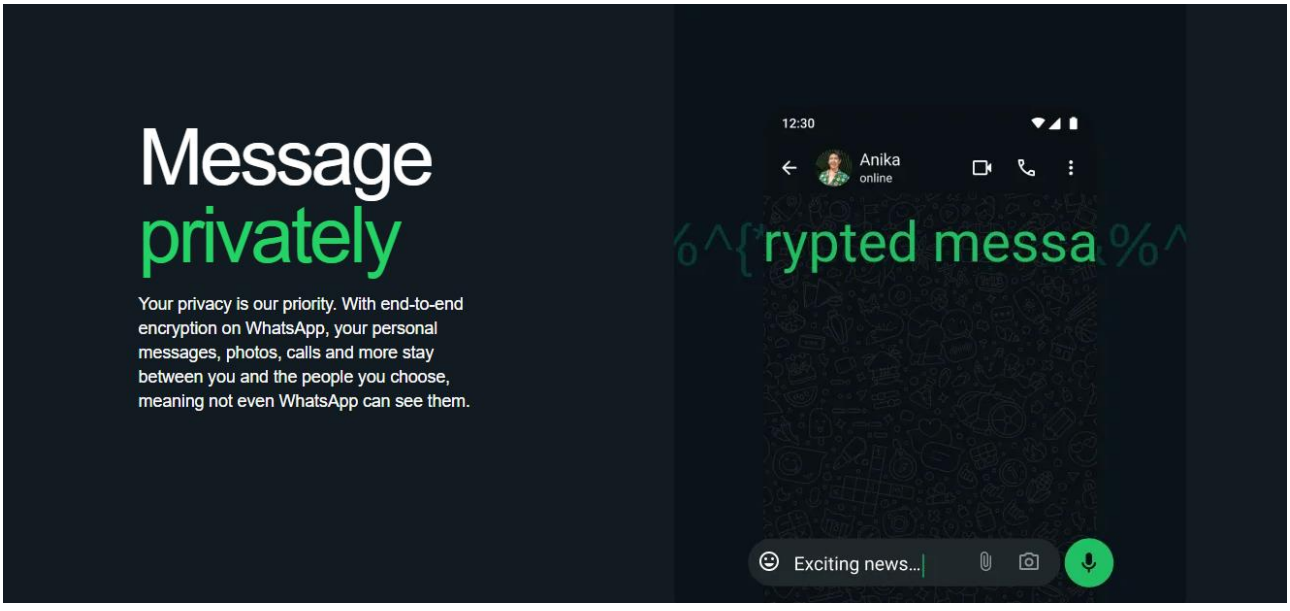
[20] *Id.*

[21] Bianca Bosker, *Zuckerberg Promises Facebook Won't Read Your WhatsApp Chats*, HuffPost (Feb. 14, 2014), https://www.huffpost.com/entry/zuckerberg-facebook-whatsapp_n_4848205.

41. Indeed, current and prospective users continue to be greeted by the below message on the WhatsApp website which touts the platform as being for "private messaging."[22]



42. Moreover, the "Privacy" page on WhatsApp's website, which is listed second only following the websites' "Features" section, states "[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."[23]



[22] WhatsApp, https://www.whatsapp.com/ (last visited Mar. 24, 2026).

[23] *Privacy*, WhatsApp, https://www.whatsapp.com/privacy (last visited Mar. 24, 2026).

43. WhatsApp's "Privacy" page further assures users that: "Personal messages, calls, photos and videos are secured with a lock with end-to-end encryption on WhatsApp, only the recipient and you have the special key needed to unlock and read them."

44. WhatsApp also makes assurances of privacy on its "Help Center" page which includes a "Safety and Security" section stating: "Your privacy and security are important to us, which is why we built end-to-end encryption into our app."[24] The Help Center also includes a page "[a]bout end-to-end encryption" which asserts: "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."[25]

[24] *Safety and Security*, WhatsApp, https://faq.whatsapp.com/898107234497196/?helpref=popular_topics (last visited Mar. 24, 2026).

[25] *About end-to-end encryption*, WhatsApp, https://faq.whatsapp.com/820124435853543 (last visited Mar. 24, 2026).

About end-to-end encryption

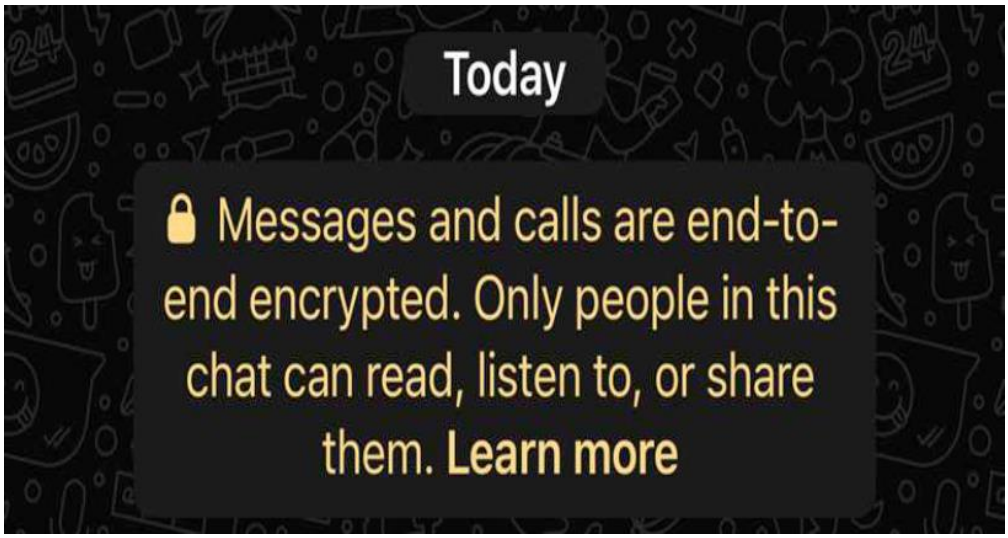
Copy link

Privacy and security is in our DNA, which is why we built end-to-end encryption into our app. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, live location, status updates, and calls are secured from falling into the wrong hands.

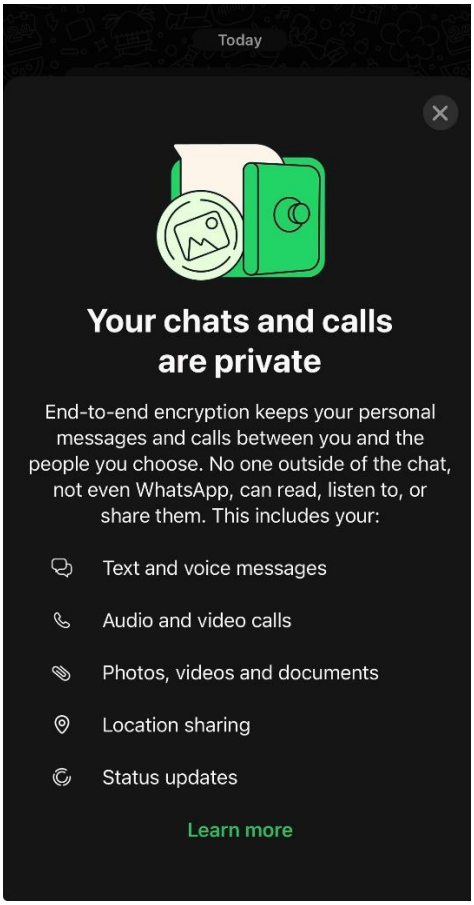
How does WhatsApp work?

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.

45. Moreover, whenever a user begins a new chat on WhatsApp, the platform displays the below statement, again assuring users that only the chat's recipients will be able to read, listen to, or share any messages sent by the user.



46. When a user clicks on the "Learn more" under this message, they are shown the below pop up which tells users: "End-to-end encryption keeps your personal messages and calls between you and the people you choose" and that no one else, including WhatsApp, "can read, listen to, or share them."



D. Unbeknownst to Plaintiffs and Other Users, WhatsApp, Meta, Their Employees, and Third-Party Contractors, Including those Employed by Accenture, Have Access to Users' Communications

47. End-to-end encryption is a means of securing digital communications whereby data is encrypted on a sender's device and is only decrypted once it reaches the recipient's device. The use of this method of transmission, in theory, means that while a sender's encrypted communication may pass through a service provider's servers on way to the intended recipient, the communication is unreadable to everyone but the intended recipient because only the sender and recipient have the necessary "key" to unlock the communication on their respective devices.

48. After Meta acquired WhatsApp in 2014, WhatsApp partnered with Open Whisper Systems to integrate the Signal Protocol, which is an end-to-end encryption cryptographic protocol, into the WhatsApp platform.[26] The integration of the Signal Protocol onto the WhatsApp platform was completed by April 5, 2016.[27]

49. By representing that the Signal Protocol has been integrated into WhatsApp, WhatsApp represented that the contents of users' messages (although not other metadata associated with communications sent on WhatsApp, such as information about who sent the communication, when the communication was sent, and where the communication was sent from) are undiscoverable by non-recipients of the message. This claim, along with WhatsApp's many other statements about the privacy and security of messages sent on the WhatsApp's platform, represents that there is no "backdoor" in the application's source code that would allow WhatsApp or third parties to circumvent the encryption.

50. Signal offers its own messaging platform and uses open source code, which means it makes its source code available to the public for inspection. This promotes transparency and allows security checks by any member of the public, including security analysts and researchers, who may review the source code and confirm that there is no backdoor to its end-to-end encryption. Rather than following this transparent approach, Meta hides its encryption source code in a black box. WhatsApp's closed source code is not available to the public, so independent third parties are unable to confirm that the platform functions without a backdoor in the end-to-end encryption, which would permit non-recipients to access users' communications. Researchers who have attempted to reverse engineer WhatsApp's source code with the limited information that is publicly available have been unable to confirm there is no backdoor in the end-to-end encryption, but have identified that WhatsApp's code deviates from Signals' source code.

51. Notably, certain countries require, or have announced their intention to require, messaging services to provide governments with access to messages as part of investigations

[26] Moxie Marlinspike, *Open Whisper Systems partners with WhatsApp to provide end-to-end encryption*, Signal (Nov. 18, 2014), https://signal.org/blog/whatsapp/.

[27] Moxie Marlinspike, *WhatsApp's Signal Protocol integration is now complete*, Signal (Apr. 5, 2016), https://signal.org/blog/whatsapp-complete/.

regarding CSAM and other criminal offenses. For instance, Indian courts have interpreted Section 69 of India's Technology Act, 2000 to allow the government to require companies to de-encrypt messages if the government claims it needs access to messages for "the "sovereignty or integrity of India," the "security of the State," "friendly relations with foreign states", or "public order."[28] Moreover, in 2021 the Indian Government enacted the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which "introduces a requirement for Indian 'significant social media intermediaries' to implement traceability."[29] This statute, "empower[s] national security agencies to trace the 'originator' of encrypted communications pursuant to an order from a court under Section 69 of the IT Act."[30] Similarly, the United Kingdom has required companies to decrypt messages "in the interests of national security" and France is considering legislation requiring companies like WhatsApp to provide law enforcement with decrypted data.[31]

52. The only way for WhatsApp to provide access to user messages in order to comply with these laws is if there is a backdoor in the Signal protocol implemented by WhatsApp.

53. Upon information and belief, there is in fact a backdoor in WhatsApp's source code that allows Meta/WhatsApp, certain Meta/WhatsApp employees, and approved third-party contractors to circumvent the encryption in order to view users' private messages. This access is provided to certain managers and certain groups, like Cyber Security, Risk Operations and/or Trust and Safety. Upon further information and belief, while backdoor access is primarily used to review messages flagged for fraud or conduct that violates company policies, it allows WhatsApp/Meta employees and third-party contractors, including those employed by Accenture, broad access to users' messages. Once access is provided by a WhatsApp/Meta manager, user messages can be

[28] Jyoti Panday, *Encryption Under Siege in India: National Security & the Erosion of Digital Privacy*, Internet Governance Project (Oct. 20, 2024), https://www.internetgovernance.org/2024/10/20/encryption-under-siege-in-india-national-security-the-erosion-of-digital-privacy/.

[29] *Id.*

[30] *Id.*

[31] Zoe Kleinman, *WhatsApp tells BBC it backs Apple in legal row with UK over user data*, BBC (June 11, 2025), https://www.bbc.com/news/articles/cgmjrn42wdwo; Bill Goodwin, *France pushes for law enforcement access to Signal, WhatsApp and encrypted email*, ComputerWeekly.com (Feb. 28, 2025),https://www.computerweekly.com/news/366619707/France-pushes-for-law-enforcement-access-to-Signal-WhatsApp-and-encrypted-email

viewed by employees and contractors simply by scrolling through a dashboard. This broad access to users' messages directly contradicts the assurances WhatsApp provides to users about the level of privacy provided through end-to-end encryption.

54. Upon information and belief, in or around 2021-2022, WhatsApp used hundreds of Accenture content reviewers to review and moderate the content of purportedly encrypted user messages. Many of these content reviewers were located in Meta's Austin, Texas office. Others were located in Ireland and Singapore. Upon information and belief, these contractors understood that certain WhatsApp/Meta employees had backdoor access to all WhatsApp user messages from which they pulled messages to provide to outside investigators in response to requests regarding criminal investigations and/or to Accenture reviewers to review for criminal investigations and/or investigations into violations of company policies.

55. There were also Accenture content moderators assigned to investigate fraud on Facebook Marketplace. Upon information and belief, these contractors were employed by Accenture LLP and were provided purportedly encrypted WhatsApp messages through Workplace, Meta's internal portal. Upon further information and belief, once a user message was flagged for potential fraud, days of messages would be sent through the portal to be reviewed. Usernames and profile information was visible to the reviewers, along with the content of the messages, which could be viewed by scrolling through the dashboard on the portal.

56. Accenture managers held monthly meetings with Meta/WhatsApp managers at Meta's Austin office where they shared data regarding the results of their investigations based on their review of user messages.

57. Given that certain Meta/WhatsApp employees had broad access to user messages, Accenture employees were concerned that their purportedly encrypted WhatsApp messages were being viewed by WhatsApp employees and warned colleagues.

58. Recent reporting has confirmed that WhatsApp's numerous promises that no one other than intended recipients has access to users' communications is false. Indeed, contrary to WhatsApp's

repeated assurances otherwise, Meta, WhatsApp, their employees, contractors, and/or third-parties' personnel have access to users' WhatsApp messages.[32]

59. According to whistleblower accounts reported to federal investigators, employees of Meta and WhatsApp and third-party contractors employed by Accenture are able to access the contents of users' messages, contrary to the privacy representations made by the company.[33]

60. Former Meta contractors reported to special agents with the U.S. Department of Commerce's Bureau of Industry and Security that "they and some of their colleagues had broad access to the substance of WhatsApp messages that were supposed to be encrypted and inaccessible."[34] The two sources "confirmed that they had employees within their physical work locations who had unfettered access to WhatsApp," and one stated that she "spoke with a Facebook team employee and confirmed that they could go back aways into WhatsApp (encrypted) messages."[35]

61. Moreover, these whistleblowers have "outlined much broader access" by Meta employees and third-party contractors than the limited access described in WhatsApp's Privacy Policy and website.[36]

62. These whistleblower complaints have prompted an investigation by special agents with the US Department of Commerce.[37]

63. Reporting also indicates that "[s]imilar claims were also the subject of a 2024 whistleblower complaint to the US Securities and Exchange Commission."[38]

---

[32] *E.g.*, Jake Bleiberg, *US Has Investigated Claims WhatsApp Chats Aren't Private*, Bloomberg (Jan. 29, 2026, at 16:22 ET), https://www.bloomberg.com/news/articles/2026-01-29/us-has-investigated-claims-that-whatsapp-chats-aren-t-private.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

E. Plaintiffs and Class Members Did Not Consent to WhatsApp Intercepting, Reading, Storing, Accessing, and/or Viewing Their Communications Sent on the WhatsApp Platform and Sharing Their Communications With Third-Parties, Including Accenture and its Employees

64. WhatsApp and Meta do not ask WhatsApp users to consent to having the contents of their messages sent on the platform intercepted, read, stored, accessed, and/or or viewed by WhatsApp, Meta, their respective employees, contractors, or other third parties.

65. To the contrary, WhatsApp's Privacy Policy states that, "[w]e do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers" and "[w]e offer end-to-end encryption for our Services. End-to-end encryption means that your messages ***are encrypted to protect against us and third parties from reading them***."[39]

66. Nowhere does WhatsApp disclose that it, Meta, their respective employees, Accenture contractors, and/or third parties may read, access, or view the contents of all messages users send on WhatsApp, nor that all messages sent by users are intercepted and stored. Instead, WhatsApp discloses only certain limited exceptions to its supposedly default policy of not storing or viewing the contents of messages.

67. For instance, in its Help Center, WhatsApp states that: "When you report a user in an individual chat, WhatsApp receives up to five of the last messages they've sent to you. When you report a group, WhatsApp receives up to five of the last messages sent to you in the reported group."[40] Nothing in this statement discloses that WhatsApp, Meta, its employees, contractors, and/or third parties may intercept, read, store, access, and/or view any communications sent by the user on the platform even when the limited circumstances outlined in this exception apply.

68. Similarly, in its Privacy Policy, WhatsApp states that if a user communicates with a business on WhatsApp the "business may give . . . third-party service provider access to its

[39] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

[40] *About reporting and blocking on WhatsApp*, WhatsApp, https://faq.whatsapp.com/414631957536067/?cms_platform=web (last visited Mar. 24, 2026).

communications to send, store, read, manage, or otherwise process them for the business."[41] This assertion again provides an extremely limited carve out and does not disclose that WhatsApp, Meta, their respective employees, and/or third parties including Accenture contractors have the ability to intercept, read, store, access, and/or view messages sent on the WhatsApp platform, even if such communications do not fit within this narrow exception.

69. The Privacy Policy also asserts that "Undelivered Messages" that "cannot be delivered immediately (for example, if the recipient is offline)" are kept "in encrypted form on our servers for up to 30 days as we try to deliver it" and that "[i]f a message is still undelivered after 30 days, we delete it."[42] Critically, this statement does not assert that all messages, not just this limited subset, may be stored for significant periods of time by Meta and/or WhatsApp or that the contents of any messages may be intercepted, read, stored, accessed, and/or viewed by Defendants, their employees, and/or third parties.

70. Further, the Privacy Policy states that: "[w]hen a user forwards media within a message, we store that media temporarily in encrypted form on our servers to aid in more efficient delivery of additional forwards."[43] Again, this statement does not assert that all messages, not just this limited subset, may be stored for significant periods of time by Meta and/or WhatsApp or that the contents of any messages may be intercepted, read, accessed, and/or viewed by Defendants their employees, and/or third parties.

71. Accordingly, WhatsApp and Meta knowingly and willfully permitted themselves, their respective employees, Accenture Contractors and/or third parties to view the contents of communications users sent on the WhatsApp platform without the user's consent.

F. Plaintiffs and Other WhatsApp Users Have a Reasonable Expectation That Their Communications are Private

72. WhatsApp users have a reasonable expectation of privacy in their communications sent via WhatsApp rooted in privacy laws as well as WhatsApp's express and implied contracts and

[41] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

[42] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

[43] *Id.*

disclosures. This includes a reasonable expectation that WhatsApp, Meta, their employees, Accenture contractors and/or other third parties would not have access to users' private communications sent on the WhatsApp platform.

73. Plaintiffs and Class members did not have a reasonable opportunity to discover Defendants' unlawful and unauthorized interception, reading, storing, accessing, and/or viewing of their communications because Defendants did not disclose its actions nor seek consent from Plaintiffs or Class members.

74. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares personal data.

75. For example, a study by the Pew Research Center indicated that an overwhelming majority of Americans—approximately 79%—are concerned about how data is collected about them by companies.[44]

76. Moreover, Defendants understood that because WhatsApp has consistently marketed itself as a secure and private messaging service, reasonable users would expect Defendants to seek consent before undermining its consistent promises and representations that messages sent on WhatsApp cannot be viewed by anyone other than an intended recipient.

77. Plaintiffs' and Class members' reasonable expectation of privacy in their communications sent only to intended recipients on WhatsApp is derived from several sources including:

a. Defendants' common law obligations to not intrude on private communications;

b. State and federal laws and regulations protecting the confidentiality of communications and computer data;

c. Defendants' express promises of privacy; and

[44] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

d. Defendants' implied promises of privacy.

G. Meta Consistently Fails to Protect Users' Privacy

78. Meta has a long history of disregarding and covering up breaches of users' privacy rights.

79. This history dates back to, at least, November 29, 2011, when Facebook entered into a 20-year consent order with the United States Federal Trade Commission ("FTC") to settle the FTC's eight-count complaint alleging that 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."[45]

80. Despite entering into this 20-year consent order, Facebook did not begin to better abide by promises to protect users' privacy. Thus, in March 2018, the FTC commenced an investigation into Facebook's continued privacy violations spurred by the public disclosure that Cambridge Analytica had used data from millions of Facebook users to build voter profiles.[46]

81. This renewed FTC investigation eventually led to the FTC announcing a historic $5 billion penalty against Facebook 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 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."[47] Notably, even though Facebook had entered into the 2012 consent order, in the intervening years, Facebook nonetheless "repeatedly used

[45] 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 the Matter of Facebook, Inc*., No. 092 3184, (FTC Nov. 11, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf.

[46] Tony Romm and Craig Timberg, *FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information*, Washington Post (Mar. 20, 2018, at 11:50 ET), 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/.

[47] 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.

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.'"[48]

82. Then, in May 2023, the FTC alleged that Meta "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."[49]

83. The SEC also fined Facebook $100 million for misleading the public regarding the Cambridge Analytica scandal based on Facebook's failure to disclose this data breach and misrepresentations about the breach.

84. Meta's continued failure to protect users' privacy, or to even abide by its own privacy policies, has also led to European regulators imposing billions of dollars in penalties on Meta for its repeated violations of data privacy statutes like the General Data Protection Regulation ("GDPR").[50]

85. Yet, even as Meta continually comes under scrutiny from regulators for failing to protect user privacy, Meta has chosen to downsize its internal departments tasked with safeguarding user information in what employees described as "as a 'gutting' of the workers in the department who review projects at Meta for privacy and integrity risks."[51]

86. Meta also has a history of failing to disclose known information to the public. For instance, a Facebook employee's 2021 disclosure of "The Facebook Papers" revealed that Meta had conducted internal research regarding the negative impact of Instagram on teenage mental health

[48] *Id.*; Complaint for Civil Penalties, Injunction, and Other Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184, (D.D.C. July 24, 2019), ECF No. 1, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

[49] 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.

[50] *E.g.*, *1.2 billion euro fine for Facebook as a result of EDPB binding decision*, European Data Protection Board, (May 22, 2023), https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en; Press Release, An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), Irish Data Protection Commission fines Meta €91 million (Sep. 27, 2024), https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta#Meta.

[51] Mike Isaac and 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.

(concluding, for example, that "[Facebook-owned Instagram] make[s] body image issues worse for one in three teen girls").[52] However, despite these concerning findings, Meta concealed these findings from regulators and the public while downplaying these risks to the public.

87. Moreover, a bipartisan group of United States Senators have sent a letter to Meta CEO Mark Zuckerberg regarding apparent misrepresentations to Congress.[53]

88. This record presents a clear pattern in which Meta fails to respect user privacy and conceals potentially negative information from the public, which it has continued by failing to abide by its promises not to access and/or disclose the contents of messages on WhatsApp to anyone other than a sender's intended recipient.

H. Tolling

89. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

90. The statutes of limitations applicable to Plaintiffs' and the Classes' claims were tolled by Defendants' conduct and Plaintiffs' and Class members' delayed discovery of their claims.

91. As alleged above, Plaintiffs and members of the Classes did not know, and could not have known, when they sent messages on WhatsApp that, contrary to assertions from Defendants otherwise, WhatsApp, Meta, their respective employees, and/or third parties had access to Plaintiffs' and Class members' communications. Plaintiffs and members of the Classes could not have discovered Defendants' unlawful conduct with reasonable diligence.

---

[52] Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, Wall St. J. (Sep. 14, 2021, at 7:59 ET), https://www.wsj.com/tech/personal-tech/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739; Vanessa Romo, *Whistleblower's testimony has resurfaced Facebook's Instagram problem*, NPR (Oct. 5, 2021, at 18:00 ET), https://www.npr.org/2021/10/05/1043194385/whistleblowerstestimony-facebook-instagram; J. Wakefield, *Facebook under fire over secret teen research*, BBC (Sep. 15, 2021), https://www.bbc.com/news/technology-58570353.

[53] Press Release, Dick Durbin, Senator, 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.

92. Defendants had exclusive and superior knowledge of their internal policy of permitting access to Plaintiffs' and Class members' communications.

93. The earliest Plaintiffs and Class members could have known about Defendants' conduct was shortly before the filing of this Complaint.

V. CLASS ACTION ALLEGATIONS

94. Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) on behalf of the following Class and Sub-Classes:

> **Nationwide Class:** All WhatsApp users residing in the United States who, between April 5, 2016 and the present, sent or received communications via the WhatsApp platform.
>
> **California Sub-Class:** All WhatsApp users residing in the State of California who, between April 5, 2016 and the present, sent or received communications via the WhatsApp platform.
>
> **Pennsylvania Sub-Class**: All WhatsApp users residing in the Commonwealth of Pennsylvania who, between April 5, 2016 and the present, sent or received communications via the WhatsApp platform.

95. Excluded from the Class are Defendants and their parents, subsidiaries, corporate affiliates, and governmental entities. Plaintiffs reserve the right to revise the definition of the Class based upon subsequently discovered information and reserves the right to establish Sub-Classes where appropriate.

96. Members of the Class are so numerous that joinder of all members is impracticable. The precise number of Class members and their identities are unknown to Plaintiffs at this time. Plaintiffs believe that there are at least millions of proposed members of the Class throughout the United States.

97. Common questions of law and fact exist as to all the Class members and predominate over any issues solely affecting individual Class members. The common and predominating questions of law and fact, each of which may also be certified under Rule 23(c)(4), include, but are not limited to:

a. Whether the Meta and WhatsApp Defendants' acts and practices violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;

b. Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

c. Whether the Meta and WhatsApp Defendants' acts and practices violated Pennsylvania's Wiretapping and Electronic Surveillance Act, Pa. Cons. Stat. §§ 5701 *et seq.*;

d. Whether the Meta and WhatsApp Defendants' acts and practices violated 18 U.S.C. §§ 2701, *et seq.*

e. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

f. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Constitution, art. 1, § 1;

g. Whether the Meta and WhatsApp Defendants' acts and practices constitute Statutory Larceny, Cal. Penal Code §§ 484, 496;

h. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*

i. Whether the Meta and WhatsApp Defendants' acts and practices violated California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq.*

j. Whether Defendants' acts and practices violate Plaintiffs' and Class members' common law privacy rights;

k. Whether the Meta and WhatsApp Defendants breached an express contract;

l. Whether the Meta and WhatsApp Defendants breached an implied contract; and

m. Whether damages, restitution, injunctive, equitable, compulsory, or other relief is warranted.

98. Plaintiffs' claims are typical of the claims of the Class that Plaintiffs seeks to represent. As alleged herein, Plaintiffs and the Class sustained damages arising out of the same unlawful actions and conduct by Defendants.

99. Plaintiffs are willing and prepared to serve the Class in a representative capacity with all of the obligations and duties material thereto. Plaintiffs will fairly and adequately protect the interests of the Class and have no interests adverse to or in conflict with the interests of the other Class members.

100. Plaintiffs' interests are co-extensive with and are not antagonistic to those of absent members within the Class. Plaintiffs will undertake to represent and protect the interests of absent members within the Class and will vigorously prosecute this action.

101. Plaintiffs have engaged the services of the undersigned counsel. Counsel is experienced in complex class action litigation, will adequately prosecute this action, and will assert and protect the rights of, and otherwise represent, Plaintiffs and the absent Class members.

102. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

103. The damages or other financial detriment suffered by individual Class members are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

104. Superiority is particularly satisfied in these circumstances, where the law of a single state will apply to all state law claims. Under the uniform contract terms with Defendants, the law of California will apply to each Class member's claims, allowing the Court to adjudicate the claims of all Class members under a single state analysis.

105. Class action status is warranted under Rule 23(b)(3) because questions of law or fact common to the Class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

106. The interest of members within the Class individually controlling the prosecution of separate actions is theoretical and not practical. The Class have a high degree of similarity and are cohesive, and Plaintiffs anticipate no difficulty in the management of this matter as a class action.

107. The nature of notice to the proposed Class is contemplated to be the best notice practicable under the circumstances including, *inter alia*, email, publication in major newspapers, and/or on the internet.

VI. CLAIMS FOR RELIEF

COUNT I

Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*
On Behalf of the Nationwide Class
(Against the Meta and WhatsApp Defendants)

108. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

109. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class members against Meta and WhatsApp.

110. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510, *et seq.*, prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

111. The ECPA confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

112. The ECPA protects both the sending and receipt of communications.

113. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

114. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

115. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

116. "Contents" includes "any information concerning the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

117. An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

118. Plaintiffs' and Nationwide Class members' communications on the WhatsApp platform are electronic communications under the ECPA.

119. Defendants intercept the "contents" of Plaintiffs' and the Nationwide Class members' communications where they acquire the text or other substance of a communication sent by a user on the WhatsApp platform.

120. Whenever Plaintiffs and the Nationwide Class members communicated with other WhatsApp users, Defendants contemporaneously and intentionally intercepted, and endeavored to intercept, Plaintiffs' and the Nationwide Class members' electronic communications without authorization or consent of the individual sending the communication or the individual receiving the communication.

121. Plaintiffs and the Nationwide Class members have not consented to the interception of their communications sent via WhatsApp, including because such interceptions are explicitly disclaimed by the WhatsApp Privacy Policy. Indeed, the Privacy Policy promises that "[w]e offer end-to-end encryption for our Services," meaning "your messages are encrypted to protect against us and third parties from reading them."[54]

122. Further, the Privacy Policy states that "[w]e do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers."[55]

[54] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

[55] *Id.*

123. The Meta and WhatsApp Defendants' interception, reading, storing, accessing, and/or viewing of Plaintiffs' and the Nationwide Class members' communications was not done in the "ordinary course" of Defendants' business because the interceptions are explicitly disclaimed by the WhatsApp Privacy Policy and other statements made by WhatsApp asserting that communications sent via WhatsApp are private and cannot be viewed by anyone other than intended recipients. 18 U.S.C. § 2510(5).

124. The Meta and WhatsApp Defendants' actions were at all relevant times knowing, willful, and intentional.

125. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Nationwide Class members have been damaged by the interception of their communications in violation of the ECPA and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II

Violation of the California Invasion of Privacy Act

Cal. Penal Code §§ 630, *et. seq.*

On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class

(Against All Defendants)

126. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

127. Plaintiffs bring this cause of action individually and on behalf of the Class members against all Defendants.

128. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA"), to address "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of

such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630.

129. Although the "declaration of policy" for CIPA provides that CIPA is intended "to protect the right of privacy of the people of this state," CIPA Section 637.2—titled "Civil action by persons injured; injunction"—provides that an action under CIPA can be brought by "[a]ny person who has been injured by a violation of this chapter . . . against the person who committed the violation" Cal. Penal Code § 637.2. To establish liability under section 631(a), Plaintiffs need only establish that a Defendant, "by means of any machine, instrument, or contrivance, or in any other manner," did any of the following:

> [i] [I]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> [ii] [W]illfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state,
>
> Or
>
> [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> [iv] [A]ids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

130. Under § 631, a defendant must show it had the consent of all parties to a communication. Meta Platforms Inc. and WhatsApp LLC are each a "person" for the purposes of CIPA.

131. Meta Platforms Inc. and WhatsApp LLC maintain their headquarters in California, where they willfully and without the consent of all parties to the communications, or in any unauthorized manner, tapped or made unauthorized connections with Plaintiffs' and the Class members' telephones and/or read, or attempted to read, or learn the contents or meaning of Plaintiffs'

and the Class members' communications while the same were in transit or passing over any wire, line, or cable, or as being sent from or received at any place within the State of California.

132. The Meta and WhatsApp Defendants' code and servers, Plaintiffs' and the Class members' browsers, and Plaintiffs' and Class members' computing and mobile devices are all a "machine, instrument, or contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here. Cal. Penal Code § 631.

133. The Meta and WhatsApp Defendants require Plaintiffs and Class members to provide their cellular phone number in order to create a profile and use the WhatsApp platform.

134. The Meta and WhatsApp Defendants tapped and/or made unauthorized use of computer code that secretly intercepted Plaintiffs' and Class members' private WhatsApp messages.

135. At all relevant times, the Meta and WhatsApp Defendants' interception of Plaintiffs' and the Class members' communications with other WhatsApp users was without Plaintiffs' and the Class members' consent.

136. At all relevant times, the Meta and WhatsApp Defendants intentionally tapped or made unauthorized connections with, the lines of communication between Plaintiffs and the Class members and other WhatsApp users without the consent of all parties to the communication.

137. Moreover, at all relevant times, Defendant Accenture conspired with the Meta and WhatsApp Defendants to engage in this non-consensual tapping and interception of the communications of Plaintiffs and Class members.

138. Defendants willfully read or attempted to read or learn the contents or meaning of Plaintiffs' and the Class members' communications with other WhatsApp users while the communications were in transit or passing over any wire, line, or cable, or were being received at any place within California when it intercepted Plaintiffs' and the Class members' communications with other WhatsApp users.

139. Defendants' secret interception of Plaintiffs' and Class members' messages sent via the WhatsApp platform occurred while Plaintiffs' and Class member's communications on the WhatsApp platform were in transit. Moreover, Plaintiffs' and Class members' messages sent via the WhatsApp platform were essentially available to Defendants to access, read, and/or view in real time.

140. As set forth above, Defendants' conduct posed a materially enhanced risk that Plaintiffs' and the Class members' privacy would be compromised.

141. Plaintiffs and the Class members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

COUNT III

Pennsylvania Wiretapping and Electronic Surveillance Act

On Behalf of the Pennsylvania Sub-Class

18 Pa. Cons. Stat. §§ 5701 *et. seq.*

(Against the Meta and WhatsApp Defendants)

142. Plaintiff Samson incorporates by reference and re-alleges the allegations contained in the preceding paragraphs of this Complaint.

143. Plaintiff Samson brings this cause of action individually and on behalf of the Pennsylvania Sub-Class members against the Meta and WhatsApp Defendants.

144. The Pennsylvania Wiretap Act prohibits: (1) the interception or endeavoring to intercept any wire, electronic or oral communication; and (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication. 18 Pa. Cons. Stat. § 5703(1)-(2).

145. The Meta and WhatsApp Defendants developed code or otherwise engaged in practices which permitted Defendants, their employees, and/or third parties to intercept, read, store, access, and/or view Plaintiff Samson's and the Pennsylvania Sub-Class members' communications while in transmission, enabling Defendants to access the contents in real time.

146. At all relevant times, the Meta and WhatsApp Defendants' interception of Plaintiff Samson's and the Pennsylvania Sub-Class Members' communications with other WhatsApp users was without Plaintiff Samson's and the Pennsylvania Sub-Class members' consent.

147. By developing this code or otherwise engaging in practices which permitted Defendants, their employees, and/or third parties to intercept, read, store, access, and/or view Plaintiff

Samson's and the Pennsylvania Sub-Class members' communications with other WhatsApp users, the Meta and WhatsApp Defendants intentionally caused Plaintiff Samson's and Class members' communications to be intercepted, read, stored, accessed, and/or viewed.

148. At all relevant times, the Meta and WhatsApp Defendants intentionally tapped or made unauthorized connections with the lines of internet communication between Plaintiff Samson and the Pennsylvania Sub-Class members and other WhatsApp users without the consent of all parties to the communications.

149. The Meta and WhatsApp Defendants willfully read or attempted to read or learn the contents or meaning of Plaintiff Samson's and the Pennsylvania Sub-Class members' communications with other WhatsApp users while the communications were in transit or passing over any wire, line, or cable, or were being received at any place within Pennsylvania when Defendants intercepted Plaintiff Samson's and the Pennsylvania Sub-Class members' communications with other WhatsApp users.

150. Pursuant to Pa. Const. Stat. § 5725, Plaintiff Samson and the Pennsylvania Sub-Class members seek (1) actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT IV

Violation of the California Comprehensive Computer Data Access and Fraud Act

Cal. Penal Code § 502, *et seq.*

On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class

(Against the Meta and WhatsApp Defendants)

151. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

152. Plaintiffs bring this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

153. The "owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss" may seek redress pursuant to Cal. Penal Code § 502(e)(1).

154. A violation of Cal. Penal Code § 502(c)(1) occurs when any person "[k]nowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . devise or execute any scheme or artifice to defraud, deceive, or extort."

155. The Meta and WhatsApp Defendants knowingly accessed the contents of users' communications in service of its scheme to defraud and/or deceive, by intentionally engaging in data collections that are contrary to its Privacy Policy and other public representations that only senders and recipients of communications via the WhatsApp platform can see the contents of messages sent via the WhatsApp platform and that no one else, including WhatsApp, could see the contents of these messages.

156. A violation of Cal. Penal Code § 502(c)(2) occurs when any person "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network . . . whether existing or residing internal or external to a computer, computer system, or computer network."

157. The Meta and WhatsApp Defendants access, copy, and make use of data from Plaintiffs' and the Class members' devices—the contents of their messages—without permission where their data collections exceed the authority granted in the Privacy Policy and run counter to their public statements.

158. As a direct result of the Meta and WhatsApp Defendants' unlawful conduct and violations, Plaintiffs and the Class members have suffered loss in an amount to be proven at trial.

159. Plaintiffs and the Class members, in accordance with Cal. Penal Code § 502(e), seek: (1) compensatory damages in an amount to be determined at trial; (2) appropriate injunctive or other equitable relief; (3) reasonable attorneys' fees; and (4) punitive or exemplary damages for the Meta and WhatsApp Defendants' willful violations as, upon information and belief, Defendants are guilty of oppression, fraud, or malice as defined by Cal. Civ. Code § 3294(c).

COUNT V

Violations of the Stored Communications Act ("SCA")

18 U.S.C. §§ 2701, *et seq.*

On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class and Pennsylvania Sub-Class

(Against the Meta and WhatsApp Defendants)

160. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

161. Plaintiffs bring this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

162. The SCA provides that a person "providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service[.]" 18 U.S.C. §2702(a)(1).

163. "Electronic communication" is broadly defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]" 18 U.S.C. §2510(12).

164. "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication[.]" 18 U.S.C. §2510(17)(A)-(B).

165. "Electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. §2510(15).

166. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. §2510(6).

167. Each of Defendants Meta and WhatsApp are a corporation and a person as defined under 18 U.S.C. §2510(6).

168. Plaintiffs and Class members are persons as defined under 18 U.S.C. §2510(6).

169. Plaintiffs and Class members reasonably expected that the Meta and WhatsApp Defendants would not disclose their "electronic communications," i.e., messages sent on the WhatsApp platform to be intercepted, read, stored, accessed, and/or viewed by individuals other than the intended recipients of the messages sent on the WhatsApp platform. Defendants (including Accenture) and their employees were not intended parties or recipients of the messages sent by Plaintiffs and Class members on the WhatsApp platform. Plaintiffs and members of the Class did not consent or authorize Meta and WhatsApp to disclose their communications to either themselves, Accenture contractors or third parties.

170. Defendant Meta stores Plaintiffs' and members of the Class's electronic communications but alleges to do so with end-to-end encryption. While the messages were stored, the Meta and WhatsApp Defendants, without authorization, knowingly and intentionally divulged and transmitted Plaintiffs' and Class member's recorded communications to themselves, their employees, Accenture contractors and/or third parties in intentional or in reckless disregard for Plaintiffs' and members of the Class's privacy rights. Defendants Meta and WhatsApp did so for their own benefit.

171. The Meta and WhatsApp Defendants were at all relevant times knowing, willful, and intentional, given that this was the Meta and WhatsApp Defendants' routine business practice, and Defendants purposefully failed to disclose this practice to consumers. As a result of the Meta and WhatsApp Defendants violations of the SCA, Plaintiffs and Class members have suffered harm and injury, including, but not limited to, the invasion of their privacy rights.

172. Pursuant to 18 U.S.C. §2707, Plaintiffs and members of the Class are entitled to: (i) appropriate equitable or declaratory relief; (ii) damages, in an amount to be determined at trial, assessed as the sum of the actual damages suffered by Plaintiffs and members of the Class and any profits made by the Meta and WhatsApp Defendants as a result of the violation, but in no case less than the minimum statutory damages of $1,000 per person; and (iii) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VI

Invasion of Privacy in Violation of the California Constitution, Art. 1, § 1

On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class

(Against All the Meta and WhatsApp Defendants)

173. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

174. Plaintiffs bring this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

175. The Meta and WhatsApp Defendants are headquartered in California and their conduct took place in California.

176. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Cons. art. I, § 1.

177. The right to privacy in California's constitution creates a right of action against private entities such as the Meta and WhatsApp Defendants.

178. To state a California constitutional privacy claim, a plaintiff must establish: (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy; and (3) conduct by the defendant constituting an intrusion of privacy so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

179. Plaintiffs and Class members possess a legally protected interest in their communications with other WhatsApp users and in using the Meta and WhatsApp Defendants' platform without that information being intercepted, read, stored, accessed, and/or viewed. This legally-protected interest is derived from the common law, the California Constitution's article I, section 1 guarantee of the right to privacy, the ECPA, and CIPA.

180. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, including that: (i) WhatsApp's Privacy Policy promised that "[w]e do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored

on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers" and that "[w]e offer end-to-end encryption for our Services. End-to-end encryption means that your messages are encrypted to protect against us and third parties from reading them."[56]; (ii) Meta and WhatsApp made numerous public representations that messages sent on the WhatsApp platform were private and secure and could not be viewed by anyone other than intended receipts; and (iii) Plaintiffs and Class members did not consent or otherwise authorize Meta and WhatsApp to intercept, read, store, access, and/or view their communications with other WhatsApp users.

181. The Meta and WhatsApp Defendants' conduct constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the information intercepted, read, stored, accessed, and/or viewed by the Meta and WhatsApp Defendants was private and personal, as protected by the California Constitution; (ii) the Meta and WhatsApp Defendants did not have authorization or consent to intercept, read, store, access, and/or view these communications; and (iii) the invasion deprived Plaintiffs and the Class members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

182. The Meta and WhatsApp Defendants' invasion violated the privacy rights of millions of Class members, including Plaintiffs, without authorization or consent. Their conduct constitutes a severe and egregious breach of social norms.

183. As a direct and proximate result of the Meta and WhatsApp Defendants' actions, Plaintiffs and the Class members have had their privacy invaded and sustained damages, and will continue to suffer damages.

184. Plaintiffs and the Class members seek appropriate relief for that injury, including but not limited to injunctive relief and damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of their intrusions upon Plaintiffs' and Class members' privacy.

185. Plaintiffs also seek such other relief as the Court may deem just and proper.

[56] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

COUNT VII

Common Law Invasion of Privacy — Intrusion Upon Seclusion

On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class and Pennsylvania Sub-Class

(Against All Defendants)

186. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

187. Plaintiffs bring this cause of action individually and on behalf of Class members against all Defendants.

188. Intrusion upon seclusion occurs when: (1) Defendants intrude into a private place, conversation, or matter in which Plaintiffs and Class members have a reasonable expectation of privacy; and (2) Defendants do so in a manner that is highly offensive to a reasonable person.

189. Defendants intentionally intruded upon Plaintiffs' and Class members' solitude or seclusion when they intercepted, read, stored, accessed, and/or viewed the contents of private communications sent via WhatsApp that users only intended to share with intended recipients.

190. Plaintiffs and Class members did not consent to or authorize, nor were they aware of Defendants' conduct.

191. Plaintiffs and Class members had a reasonable expectation of privacy over their communications sent via WhatsApp, which Defendants assured users were private and could not be seen by anyone other than intended recipients.

192. Defendants knew that by intercepting, reading, storing, accessing, and/or viewing messages sent via WhatsApp they were intruding on private conversations.

193. Defendants' secret interception, reading, storage, accessing, and/or viewing of Plaintiffs' and Class members' communications is highly offensive to a reasonable person. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal information is collected or shared.

194. Defendants' interception, reading, storage, accessing, and/or viewing of Plaintiffs' and Class members' communications occurred in a manner highly offensive to a reasonable person in that

it violated: (1) Defendants' own Privacy Policy and public representations that messages sent on WhatsApp are private and cannot be viewed by anyone other than intended recipients; (2) federal and state criminal law; and (3) civil laws designed to protect individual privacy.

195. Defendants' reckless disregard for the privacy of Plaintiffs and the Class members is highly offensive to a reasonable person. Defendants knew of the privacy risks posed by its conduct and chose to proceed with the invasion of privacy, as well as deliberately misrepresenting the extent of its access and storage to Plaintiffs and Class members through inaccurate and/or incomplete disclosures.

196. Plaintiffs and Class members have suffered harm and injury as a direct and proximate result of Defendants' invasion of their privacy.

197. Plaintiffs and Class members are entitled to reasonable compensation, including but not limited to monetary damages.

198. Plaintiffs and Class members seek appropriate relief for that injury, including, but not limited to injunctive relief and damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of its intrusions upon Plaintiffs' and Class members' privacy.

199. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT VIII

Breach of Express Contract

On Behalf of the Nationwide Class or alternatively, on behalf of the California Sub-Class and Pennsylvania Sub-Class

(Against the Meta and WhatsApp Defendants)

200. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

201. Plaintiffs brings this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

202. There exists an express contract between Plaintiffs and Class members on one side and WhatsApp on the other where, upon creating WhatsApp accounts, Plaintiffs and Class members agreed to the WhatsApp Terms of Service. The Terms of Service incorporate WhatsApp's Privacy

Policy. A true and correct copy of the Terms of Service last updated January 2021, is attached hereto as Exhibit 1, and a copy of the Privacy Policy, incorporated into the Terms of Service, is attached as Exhibit 2.

203. To use WhatsApp, Defendants expressly required Plaintiffs to accept and consent to Defendants' Terms and Conditions and the incorporated Privacy Policy.

204. To create a WhatsApp account, Plaintiff Shirazi clicked buttons signifying acceptance of WhatsApp's Terms of Service and thus entered into a contract with Defendants regarding the use of WhatsApp.

205. To create a WhatsApp account, Plaintiff Samson clicked buttons signifying acceptance of WhatsApp's Terms of Service and thus entered into a contract with Defendants regarding the use of WhatsApp.

206. By creating WhatsApp accounts Class members similarly entered into an express contract with WhatsApp regarding their respective rights and responsibilities with respect to use of the WhatsApp platform.

207. WhatsApp's Privacy Policy provides repeated promises that the communications users send via WhatsApp will be private and that no one other than intended recipients can obtain the communications.

208. However, nowhere in the Privacy Policy do Meta and WhatsApp disclose that they have access to the communications users send via WhatsApp and that those messages can be intercepted, read, stored, accessed, and/or viewed by individuals other than the intended recipient.

209. The Meta and WhatsApp Defendants breached the contract when they secretly intercepted, read, stored, accessed, and/or viewed users' communications sent via WhatsApp.

Consent

210. WhatsApp requires users to create an account before being able to send communications via WhatsApp.

211. Plaintiffs and Class members consented to the Terms of Service and incorporated Privacy Policy by signing up for, and using, the WhatsApp platform.

Consideration

212. The WhatsApp platform is not a service the Meta and WhatsApp Defendants provide without receiving anything from Plaintiffs and Class members in return. To the contrary, Plaintiffs' and Class members' use of the WhatsApp platform confers significant benefits on Defendants—a benefit to which Defendants are not entitled—including to use the platform and share metadata collected via cookies, usage and log information, device and connection information, including IP addresses, with Meta and WhatsApp.

213. The Terms of Service and incorporated Privacy Policy are presented to WhatsApp users before they may create a WhatsApp account and WhatsApp users read these documents before tapping a link that says "Agree and Continue" in order to "accept the terms," create a profile, and begin using the WhatsApp platform.[57]

214. Agreeing to the Terms of Service and incorporated Privacy Policy is additional consideration that Plaintiffs and Class members provide to the Meta and WhatsApp Defendants in exchange for the Meta and WhatsApp Defendants permitting them to use the WhatsApp platform.

215. In return for the valuable consideration provided by Plaintiffs and Class members, WhatsApp agrees to abide by the promises set forth in its Terms of Service and Privacy Policy.

Performance

216. Plaintiffs and Class members performed under the express contract.

The Meta and WhatsApp Defendants Breached the Express Contract

217. The Meta and WhatsApp Defendants breached the express contract with Plaintiffs and Class members by secretly intercepting, reading, storing, accessing, and/or viewing WhatsApp users' communications sent via the WhatsApp platform.

218. WhatsApp's Privacy Policy promises that: "[w]e offer end-to-end encryption for our Services," meaning "your messages are encrypted to protect against us and third parties from reading them."[58]

---

[57] *How to get started on WhatsApp Messenger*, WhatsApp, https://www.whatsapp.com/coronavirus/get-started (last visited Mar. 24, 2026).

[58] *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), https://www.whatsapp.com/legal/privacy-policy.

219. The Meta and WhatsApp Defendants breached this promise by intercepting, reading, storing, accessing, and/or viewing Plaintiffs' and Class members' communications with other WhatsApp users.

220. Further, the Privacy Policy states that "[w]e do not retain your messages in the ordinary course of providing our Services to you. Instead, your messages are stored on your device and not typically stored on our servers. Once your messages are delivered, they are deleted from our servers."[59]

221. The Meta and WhatsApp Defendants breached this promise by intercepting, reading, accessing, viewing, and/or indefinitely storing all of Plaintiffs' and Class members' communications with other WhatsApp users such that Defendants could read, access, or view the communications at any time.

222. In the Privacy Policy, the Meta and WhatsApp Defendants assert that communications may be stored and/or viewed in certain limited instances such as "Undelivered Messages" and "Media Forwarding." However, these statements are false and misleading because Defendants store and may read, access, or view all communications rather than the limited subset promised.[60]

Plaintiffs and Class Members Were Damaged

223. The Meta and WhatsApp Defendants' breach caused Plaintiffs and Class members the following damages, among others:

a. Nominal damages for each breach of contract by the Meta and WhatsApp Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private;

d. Plaintiffs and Class members did not get the full value of the benefit of their bargain, which included the Meta and WhatsApp Defendants' duty to abstain from intercepting, reading, storing, accessing, and/or viewing Plaintiffs' and Class members' communications;

e. Plaintiffs and Class members provided the Meta and WhatsApp Defendants with valuable consideration—namely access to certain personal information such as metadata collected via cookies, usage and log information, device and connection information, including IP addresses—which the Meta and WhatsApp Defendants

[59] *Id.*

[60] *Id.*

monetized and which Plaintiffs and Class members would not have provided had they known about the Meta and WhatsApp Defendants' misrepresentations; and

f. The Meta and WhatsApp Defendants' actions violated the property rights that Plaintiffs and Class members enjoy in their private communications.

224. Plaintiffs and Class members also seek attorneys' fees and costs on this claim to the extent allowable.

COUNT IX

Breach of Implied Contract

On Behalf of the Nationwide Class or alternatively, on behalf of the California Sub-Class and Pennsylvania Sub-Class

(Against the Meta and WhatsApp Defendants)

225. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

226. Plaintiffs bring this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

227. An implied contract was created between the Meta and WhatsApp Defendants, on the one side, and Plaintiffs and Class members on the other, whereby the Meta and WhatsApp Defendants offered to provide what they represented to be a secure "end-to-end" encrypted messaging application through which Plaintiffs and Class members could communicate with other WhatsApp users without the Meta and WhatsApp Defendants or any other party intercepting, reading, storing, accessing, and/or viewing the content of those communications. In accepting the Terms and Service and the Privacy Policy there incorporated, Plaintiffs and Class members agreed to use WhatsApp for its communications as opposed to other means.

Mutual Assent

228. Such an implied contract was created by virtue of the relationship and conduct of the parties, as well as the surrounding circumstances, including, but not limited to: 1) the purported encrypted nature of WhatsApp; 2) the private nature of the communications WhatsApp was used for; 3) the public assurances on WhatsApp's website that the Meta and WhatsApp Defendants prioritize privacy and that messages sent on WhatsApp can be sent securely and without disclosure to individuals other than intended recipients; 4) WhatsApp's in-app assurances that others cannot read, listen, or share the contents of the messages; 5) the integration of Signal Protocol into WhatsApp;

and 6) the Meta and WhatsApp Defendants' express promises, as noted above, not to intercept, read, store, access, and/or view Plaintiffs' and Class members' communications.

229. The Meta and WhatsApp Defendants knew, or had reason to know, that Plaintiffs and Class members would interpret the parties' relationship and conduct as an agreement to keep Plaintiffs' and Class members' communications confidential.

Consideration

230. The WhatsApp platform is not a service the Meta and WhatsApp Defendants provide without receiving anything from Plaintiffs and Class members in return. To the contrary, Plaintiffs' and Class members' use of the WhatsApp platform confers significant benefits on the Meta and WhatsApp Defendants—a benefit to which Defendants are not entitled—including to use the platform and share metadata collected via cookies, usage and log information, device and connection information, including IP addresses, with the Meta and WhatsApp Defendants.

231. The Terms of Service and incorporated Privacy Policy are presented to WhatsApp users before they may create a WhatsApp account and WhatsApp instructs users to read these documents before tapping a link that says "Agree and Continue" in order to "accept the terms," before a user can create a profile, and begin using the WhatsApp platform.

232. Agreeing to the Terms of Service and incorporated Privacy Policy is additional consideration that Plaintiffs and Class members provide to the Meta and WhatsApp Defendants in exchange for the Meta and WhatsApp Defendants permitting them to use the WhatsApp platform.

233. In return for the valuable consideration provided by Plaintiffs and Class members, the Meta and WhatsApp Defendants agrees to abide by the promises set forth in its Terms of Service and Privacy Policy.

Performance

234. Plaintiffs and Class members performed under the implied contract.

The Meta and WhatsApp Defendants' Breach of the Implied Contract

235. The Meta and WhatsApp Defendants breached their implied contract with Plaintiffs and Class members by intercepting, reading, storing, accessing, and/or viewing Plaintiffs' and Class members' communications with other WhatsApp users.

236. In breach of the promises implied by its conduct and memorialized in its Privacy Policy and other assurances, the Meta and WhatsApp Defendants secretly provided the contents of users' communications on the WhatsApp platform to themselves, their employees, and/or other third parties.

237. The Meta and WhatsApp Defendants have failed and refused to cure these breaches and continue to intercept, read, store, access, and/or view Plaintiffs' and Class members' communications with other WhatsApp users.

Plaintiffs and Class Members Were Damaged

238. The Meta and WhatsApp Defendants' breach caused Plaintiffs and Class members the following damages, among others:

a. Nominal damages for each breach of contract by Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private;

d. Plaintiffs and Class members did not get the full value of the benefit of their bargain, which included Defendants' duty to abstain from intercepting, reading, storing, accessing, and/or viewing Plaintiffs' and Class members' communications;

e. Plaintiffs and Class Members provided Defendants with valuable consideration—namely access to certain personal information such as metadata collected via cookies, usage and log information, device and connection information, including IP addresses—which Defendants monetized and which Plaintiffs and Class members would not have provided had they known about Defendants' misrepresentations; and

f. Defendants' actions violated the property rights that Plaintiffs and Class members enjoy in their private communications.

239. Plaintiffs and Class members also seek attorneys' fees and costs on this claim to the extent allowable.

COUNT X

Statutory Larceny Through False Pretenses

Cal. Penal Code §§ 484, 496

On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class

(Against the Meta and WhatsApp Defendants)

240. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

241. Plaintiffs brings this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants.

242. Cal. Penal Code § 496(a) prohibits the obtaining of property "in any manner constituting theft."

243. "Theft" is prohibited by Cal. Penal Code § 484(a), and a person is guilty of theft, *inter alia*, where they "fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of . . . personal property."

244. The Meta and WhatsApp Defendants acted in a manner constituting theft by false pretenses pursuant to Cal. Penal Code § 484(a) by representing that WhatsApp communications would not be intercepted, read, stored, accessed, and/or viewed and then acting in such a manner that enabled the Meta and WhatsApp Defendants, their employees, and/or third parties to intercept, read, store, access, and/or view Plaintiffs' and the Class members' communications with other WhatsApp users.

245. Plaintiffs and the Class members relied on the Meta and WhatsApp Defendants' consistent representations that messages sent on the WhatsApp platform are private and cannot be viewed by anyone other than an intended recipient when deciding to use the platform to send purportedly encrypted messages.

246. The Meta and WhatsApp Defendants knew they obtained the content of Plaintiffs' and the Class members' communications with other WhatsApp users in a manner constituting theft, because it developed access to the communications while expressly informing its users that it could and would not.

247. Pursuant to Cal. Penal Code § 496(c), Plaintiffs and the Class have been injured by a violation of § 496(a), and are entitled to: (1) treble damages; (2) attorneys' fees reasonably incurred; and (3) costs of suit.

COUNT XI

Violations of Cal. Bus. & Prof. Code § 17200, *et seq.*

Unlawful, Unfair, and Fraudulent Business Practices

On Behalf of Plaintiffs Individually

(Against the Meta and WhatsApp Defendants)

248. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

249. Plaintiffs bring this cause of action individually and on behalf of Class members against the Meta and WhatsApp Defendants..

250. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200.

251. The Meta and WhatsApp Defendants have engaged, and continue to engage in, unlawful, unfair, or fraudulent business practices in connection with WhatsApp's Privacy Policy and other public facing statements about WhatsApp's privacy practices.

252. The Meta and WhatsApp Defendants' business practices deceptively lead reasonable consumers to believe that WhatsApp did not and could not intercept, read, store, access, and/or view WhatsApp user's communications sent via WhatsApp. In reality, the Meta and WhatsApp Defendants have developed, maintained, and practiced the ability to intercept, read, store, access, and/or view the communications.

253. The acts and practices of the Meta and WhatsApp Defendants as alleged herein constitute "unlawful" business practices and acts under the UCL in that Defendants' conduct violates California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq.*, as set forth below. These acts also constitute "unfair" business acts and practices under the UCL in that the Meta and WhatsApp Defendants' conduct is unconscionable, immoral, deceptive, unfair, illegal, unethical, oppressive, and/or unscrupulous. These acts also constitute "fraudulent" business acts and practices under the UCL in that Defendants' conduct is false and has a tendency to deceive the general public.

254. The Meta and WhatsApp Defendants' business practices are misleading and/or have a capacity, likelihood, or tendency to deceive or confuse the public.

255. Plaintiffs relied, to their detriment, on the Meta and WhatsApp Defendants' misleading and deceptive practices, including each of the misrepresentations and omissions set forth above. Had Plaintiffs been adequately informed and not misled by the Meta and WhatsApp Defendants, they would have acted differently.

256. Plaintiffs suffered an injury in fact as a result of the Meta and WhatsApp Defendants' unlawful, unfair, or fraudulent business practices. The harm from the Meta and WhatsApp Defendants' conduct was not reasonably avoidable by Plaintiffs because only the Meta and WhatsApp Defendants were aware of the true facts concerning its privacy practices, and Defendants did not sufficiently disclose those facts.

257. The Meta and WhatsApp Defendants' acts and omission are likely to deceive the general public.

258. The Meta and WhatsApp Defendants engaged in these unlawful, unfair, and fraudulent practices to obtain more WhatsApp users and to increase their profits. Accordingly, the Meta and WhatsApp Defendants have engaged in these unlawful, unfair, and fraudulent business acts and practices, as defined and prohibited by section 17200, *et seq.* of the California Business and Professions Code.

259. The Meta and WhatsApp Defendants' wrongful conduct emanated out of California where they are headquartered and where relevant decisions giving rise to the wrongful conduct alleged herein occurred.

260. Upon information and belief, the Meta and WhatsApp Defendants also authored the Terms of Service and Privacy Policy, which they failed to abide by, in California.

261. Upon information and belief, the Meta and WhatsApp Defendants also engaged in the wrongful interception, reading, storing, accessing, and/or viewing of the contents of user's WhatsApp communications in California.

262. Plaintiffs seek an injunction to prohibit the Meta and WhatsApp Defendants from continuing to engage in the unlawful, unfair, or fraudulent business acts and practices described herein. Unless and until the Meta and WhatsApp Defendants are enjoined by an order of this Court, the Meta and WhatsApp Defendants will continue to cause injury to the general public and violate

the laws of California by continuing to deceptively advertise its services. Plaintiffs, on behalf of the general public, has no other adequate remedy at law to ensure compliance with Cal. Bus. and Prof. Code § 17200, *et seq.* going forward. Plaintiff also seeks disgorgement, as the equitable relief sought herein is more adequate, certain, prompt, and efficient than any legal remedy available.

263. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT XII

Violations of Cal. Bus. & Prof. Code § 17500, *et seq.*

False or Misleading Representations

On Behalf of Plaintiffs Individually

(Against the Meta and WhatsApp Defendants)

264. Plaintiffs incorporate by reference and re-allege the allegations contained in the preceding paragraphs of this Complaint.

265. Plaintiffs bring this claim individually.

266. The Meta and WhatsApp Defendants have made, and continue to make, untrue, false, deceptive, and/or misleading statements in connection with WhatsApp's Privacy Policy and other public facing advertisements as to WhatsApp's privacy practices.

267. The Meta and WhatsApp Defendants made, and continue to make, representations and statements (by omission and commission) that lead reasonable consumers to believe that WhatsApp did not and could not intercept, read, store, access, and/or view WhatsApp users' communications with other WhatsApp users. In reality, the Meta and WhatsApp Defendants have developed, maintained, and practiced the ability to intercept, read, store, access, and/or view users' communications sent via WhatsApp.

268. Plaintiffs suffered an injury in fact as a result of the Meta and WhatsApp Defendants' unlawful, unfair, or fraudulent business practices.

269. The Meta and WhatsApp Defendants' acts and omissions are misleading and/or have a capacity, likelihood, or tendency to deceive or confuse the public.

270. Plaintiffs relied, to their detriment, on the Meta and WhatsApp Defendants' misleading and deceptive practices, including each of the misrepresentations and omissions set forth

above. Had Plaintiffs been adequately informed and not misled by the Meta and WhatsApp Defendants, they would have acted differently.

271. The Meta and WhatsApp Defendants' acts and omissions are likely to deceive the general public.

272. Upon information and belief, the Meta and WhatsApp Defendants' advertisements, and the misrepresentations and omissions therein, are drafted in, emanate from, and are overseen by the Meta and WhatsApp Defendants' headquarters located in California.

273. The Meta and WhatsApp Defendants engaged in the misleading and deceptive advertising and marketing practices set forth above to obtain more WhatsApp users and increase its profits. Accordingly, the Meta and WhatsApp Defendants have engaged in false advertising, as defined and prohibited by § 17500, *et seq.* of the California Business and Professions Code.

274. Plaintiffs seeks an injunction to prohibit the Meta and WhatsApp Defendants from continuing to engage in the misleading and deceptive advertising practices described herein. Unless and until Defendants are enjoined by an order of this Court, the Meta and WhatsApp Defendants will continue to cause injury to the general public and violate the laws of California by continuing to deceptively advertise its privacy practices. Plaintiffs, on behalf of the general public, have no other adequate remedy at law to ensure compliance with Cal. Bus. & Prof. Code § 17500, *et seq.* going forward. Plaintiff also seeks restitution, as the equitable relief sought herein is more adequate, certain, prompt, and efficient than any legal remedy available.

275. Plaintiffs also seek such other relief as the Court may deem just and proper.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that this Court enter judgment against Defendants and in favor of Plaintiffs and the Classes, and award the following relief:

a. An order certifying this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiffs as the representatives of the Classes, and Plaintiffs' counsel as counsel for the Classes;

b. An order issuing a public injunction enjoining the Meta and WhatsApp Defendants from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint, by making untrue, false, deceptive, and/or misleading statements in connection with WhatsApp's Privacy Policy and other public facing advertisements informing users that WhatsApp does not and cannot intercept, read, store, access, and/or view WhatsApp users' communications with other users while, in truth, engaging in such conduct;

c. A declaration that Defendants are financially responsible for all Class notice and the administration of Class relief;

d. An order awarding costs, restitution, disgorgement, punitive damages, statutory damages, treble damages, and exemplary damages under applicable law, and compensatory damages for economic loss, and out-of-pocket costs in an amount to be determined at trial;

e. An order requiring Defendants to pay both pre- and post-judgment interest on any amounts awarded;

f. An award of costs, expenses, and attorneys' fees as permitted by law; and

g. Such other or further relief as the Court may deem appropriate, just, and equitable.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

DATED: March 25, 2026

Respectfully submitted,

/s/ *Jennifer L. Joost*

Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
KESSLER TOPAZ MELTZER & CHECK, LLP
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and–

Joseph H. Meltzer (*pro hac vice* forthcoming)
jmeltzer@ktmc.com
Melissa L Yeates (*pro hac vice* forthcoming)
myeates@ktmc.com
Tyler S. Graden (*pro hac vice* forthcoming)
tgraden@ktmc.com
Jordan E. Jacobson (Bar No. 302543)
jjacobson@ktmc.com
Daniel S. Dicce (*pro hac vice* forthcoming)
ddicce@ktmc.com
KESSLER TOPAZ
MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiffs and the Putative Classes