QUINN EMANUEL URQUHART & SULLIVAN, LLP
Adam Wolfson (Bar No. 262125)
adamwolfson@quinnemanuel.com
Stephen A. Broome (Bar No. 314605)
stephenbroome@quinnemanuel.com
Kevin Teruya (Bar No. 235916)
kevinteruya@quinnemanuel.com
Valerie Roddy (Bar No. 235163)
valerieroddy@quinnemanuel.com
Lauren B. Lindsay (Bar No. 280516)
laurenlindsay@quinnemanuel.com
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

KELLER POSTMAN, LLC
Warren Postman (Bar No. 330869)
wdp@kellerpostman.com
Ashley Keller (*pro hac vice forthcoming*)
ack@kellerpostman.com
J.J. Snidow (*pro hac vice forthcoming*)
jj.snidow@kellerpostman.com
1101 Connecticut Avenue, N.W., Suite 1100
Washington, D.C. 20036
Telephone: (833) 633-0118

BARNETT LEGAL, PLLC
Jay W. Barnett (*pro hac vice forthcoming*)
jay@barnettlegal.net
3404 NW 135th Street
Oklahoma City, OK 73120
Telephone: (405) 456-9343

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

EMMA DAWSON, MICHAEL DAWSON, LUIZ FILHO, ALKA GAUR, DAMIAN REYEZ JAQUEZ, YOLISA MKELE, and FERNANDA TATTO, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

META PLATFORMS, INC., and WHATSAPP, LLC,

Defendants.

CASE NO. 26-cv-0751

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Page

Plaintiffs Emma Dawson, Michael Dawson, Luiz Filho, Alka Gaur, Damian Reyez Jaquez, Yolisa Mkele, and Fernanda Tatto ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Meta Platforms, Inc. ("Meta") and WhatsApp, LLC ("WhatsApp") (collectively, "Defendants"). Plaintiffs bring this action for Defendants' (1) violation of the Wiretap Act (18 U.S.C. § 2510 *et seq.*); (2) violation of the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502 *et seq.*); (3) violation of the California Invasion of Privacy Act (Cal. Penal Code § 630 *et seq.*); (4) invasion of privacy rights protected by Article 1, Section 1 of the California Constitution; (5) intrusion upon seclusion; (6) breach of contract; (7) breach of the implied covenant of good faith and fair dealing; (8) unjust enrichment under quasi-contract theories (pled in the alternative); (9) statutory larceny (Cal. Penal Code §§ 484, 496); and (10) violation of California's Unfair Competition Law (Cal. Bus. & Prof. Code § 17200).

INTRODUCTION

1. WhatsApp is the most popular messaging app in the world. It purports to offer its more than ***three billion*** users in over 180 countries[1] privacy, security, and peace of mind by making two important promises. First, WhatsApp has advertised that it is "***[e]ncrypted for everyone***" and allows users to "***[m]essage privately with everyone***."[2] Second, reinforcing the sense of privacy among users, WhatsApp claims it "does not store messages once they are delivered."[3] To this day, WhatsApp claims that "[y]our privacy is our priority. With end-to-end encryption on WhatsApp, your personal messages, photos, calls and more stay between you and the people you choose,

[1] WhatsApp, About WhatsApp, *available at* https://www.whatsapp.com/about (last accessed Jan. 19, 2026).

[2] WhatsApp, Homepage, *available at* https://www.whatsapp.com (last accessed Nov. 30, 2025) (emphases added).

[3] WhatsApp, Information for Law Enforcement Authorities, *available at* https://faq.whatsapp.com/444002211197967 (last accessed Jan. 19, 2026); *see also* WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026) ("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.").

meaning not even WhatsApp can see them."[4] Mark Zuckerberg, the founder, Chairman, and Chief Executive Officer of Meta (which has owned WhatsApp since 2014), reinforced this claim to the United States Senate in sworn public testimony, asserting that "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."[5] And, since at least 2016, WhatsApp chats begin with the following statement:

2. These claims are false. WhatsApp and its parent company, Meta, store, analyze, and can access virtually ***all*** of WhatsApp users' purportedly "private" communications. Senior leadership at Meta has tried over the years to prevent the dissemination of this information by siloing different teams that might be able to piece together the truth and directing them to "stay in [their] own lane[s]." Nevertheless, through the assistance of courageous whistleblowers, the truth can now come to light. On information and belief, to this day, Meta and WhatsApp store, maintain access to, and use WhatsApp's three billion users' "encrypted" messages. This lawsuit seeks to expose the fundamental privacy violations and fraud Meta is perpetrating against the billions of people

---

[4] WhatsApp, Privacy, *available at* https://www.whatsapp.com/privacy (last accessed Jan. 19, 2026) (emphasis added); *see also* WhatsApp, Does WhatsApp collect or sell your data?, *available at* https://faq.whatsapp.com/2779769622225319/?helpref=hc_fnav (last accessed Jan. 19, 2026) ("Every personal message, call, media, voice message, or document you send on WhatsApp is private and protected with end-to-end encryption by default. That means all your personal messages stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them.").

[5] Tr. of Testimony of Mark Zuckerberg, United States Senate, S. Hrg. 115-683, Joint Hearing Before the Committee on Commerce, Science and Transportation and the Committee on the Judiciary, "Facebook, Social Media Privacy, and the Use and Abuse of Data," 115th Cong., 2d Session (Apr. 10, 2018), *available at* https://www.congress.gov/event/115th-congress/senate-event/LC64510/text (last accessed Jan. 19, 2026).

worldwide who have used WhatsApp believing their communications would be private from everyone, even from WhatsApp and Meta.

3. The gravity of Meta's and WhatsApp's violation of users' privacy and trust cannot be overstated. Across the globe, activists, independent journalists, those living under authoritarian regimes, and many others rely on WhatsApp to communicate based on their erroneous (but well-justified) belief that the substance of their communications is beyond scrutiny by ***anyone*** without some element of self-reporting. Although unencrypted metadata alone can be used to identify and locate such users, for some, access to the ***substance*** of their communications can literally mean the difference between life or death. Even for users who do not face such high stakes if their communications are accessible to third parties, their belief in the inviolability of their private communications is an essential aspect of psychological health and well-being (among other things), particularly in a time when people's most intimate relationships are developed and maintained increasingly via digital communications instead of, and in addition to, face-to-face interactions. In any event, all users were entitled to believe their communications were private because WhatsApp and Meta unequivocally and repeatedly promised that they did not store users' delivered messages and that no one—not even WhatsApp and Meta—can access their encrypted messages.

4. Plaintiffs bring this class action on behalf of themselves and all others similarly situated and, specifically, all users of WhatsApp worldwide since April 5, 2016, excluding users residing in the United States or Canada (who are subject to an arbitration requirement under WhatsApp Terms of Service), the "European Region"[6] (who are subject to Terms of Service that require users to bring claims in their own country—if jurisdiction exists there—or Ireland), or the

[6] WhatsApp defines the European Region as including "Andorra, Austria, Azores, Belgium, Bulgaria, Canary Islands, Channel Islands, Croatia, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Gibraltar, Greece, Guadeloupe, Hungary, Iceland, Ireland, Isle of Man, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Madeira, Malta, Martinique, Mayotte, Monaco, Netherlands, Norway, Poland, Portugal, Republic of Cyprus, Réunion, Romania, San Marino, Saint-Martin, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom sovereign bases in Cyprus (Akrotiri and Dhekelia), and Vatican City." *See, e.g.*, WhatsApp, "FAQ: Who is providing your WhatsApp services," *available at* https://faq.whatsapp.com/523679699550284/ (last accessed Jan. 19, 2026).

United Kingdom.[7] Under WhatsApp's own Terms of Service, all other users either must bring claims against WhatsApp in either this Court or the Superior Court of San Mateo County.[8]

5. Like other members of the Class, Plaintiffs are WhatsApp users whose end-to-end encrypted communications have been stored by and accessible to WhatsApp and Meta, notwithstanding WhatsApp's and Meta's assurances to the contrary. Plaintiffs bring this action to enforce their privacy rights and seek damages and other relief for the harm WhatsApp and Meta have caused them by willfully misrepresenting to them that their private communications were just that—***private and inaccessible even to WhatsApp and Meta***. In fact, WhatsApp and Meta have access to ***all*** WhatsApp users' encrypted communications in their entirety.

PARTIES

6. Plaintiff Emma Dawson is an adult domiciled in Australia. Dawson has been a WhatsApp user during the entire Class Period.

7. Plaintiff Michael Dawson is an adult domiciled in Australia. Dawson has been a WhatsApp user during the entire Class Period.

8. Plaintiff Luiz Filho is an adult domiciled in Brazil. Filho has been a WhatsApp user during the entire Class Period.

9. Plaintiff Alka Gaur is an adult domiciled in India. Gaur has been a WhatsApp user during the entire Class Period.

---

[7] WhatsApp, "FAQ: Who is providing your WhatsApp services," *available at* https://faq.whatsapp.com/523679699550284/ (last accessed Jan. 19, 2026).

[8] *See, e.g.*, WhatsApp, Terms of Service, "Dispute Resolution," *available at* https://www.whatsapp.com/legal/terms-of-service?lang=en#terms-of-service-dispute-resolution ("If you are not subject to the 'Special Arbitration Provision for United States or Canada Users' section below, you agree that any claim or cause of action you have against WhatsApp relating to, arising out of, or in any way in connection with our Terms or our Services, and for any claim or cause of action that WhatsApp files against you, you and WhatsApp agree that any such claim or cause of action . . . will be resolved exclusively in the United States District Court for the Northern District of California or a state court located in San Mateo County in California, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating any such claim or cause of action, and the laws of the State of California will govern any such claim or cause of action without regard to conflict of law provisions.") (last accessed Jan. 19, 2026).

10. Plaintiff Damian Reyez Jaquez is an adult domiciled in Mexico. Jaquez has been a WhatsApp user during the entire Class Period.

11. Plaintiff Yolisa Mkele is an adult domiciled in South Africa. Mkele has been a WhatsApp user during the entire Class Period.

12. Plaintiff Fernanda Tatto is an adult domiciled in Brazil. Tatto has been a WhatsApp user during the entire Class Period.

13. Defendant Meta is a Delaware corporation, organized and existing under the laws of the State of Delaware, with its principal place of business at 1 Meta Way, Menlo Park, California 94025. With a $1.72 trillion market capitalization (subject to market fluctuations), Meta is consistently ranked as one of the ten largest corporations in the world.[9] Prior to October 28, 2021, Meta operated as Facebook, Inc. ("Facebook").[10] For simplicity, this Complaint may refer to Meta and Facebook, Inc. (the corporate entity) interchangeably as "Meta."

14. Defendant WhatsApp is a Delaware limited liability company, organized and existing under the laws of the State of Delaware, with its principal place of business at 1 Meta Way, Menlo Park, California, 94025. Since 2014, WhatsApp has been a wholly-owned subsidiary of Meta, acquired by (then-)Facebook for approximately $19 billion in cash and stock.[11]

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over the federal claims in this action pursuant to 28 U.S.C. § 1331.

16. This Court also has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Class Members as defined below,

---

[9] J. Pinkerton, "The 10 Most Valuable Companies in the World by Market Capitalization," U.S. News (June 24, 2025), *available at* https://money.usnews.com/investing/articles/most-valuable-companies-in-the-world-by-market-cap (last accessed Jan. 19, 2026).

[10] Meta, "Introducing Meta: A Social Technology Company" (Oct. 28, 2021), *available at* https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ (last accessed Jan. 19, 2026).

[11] Meta, "Facebook to Acquire WhatsApp" (Feb. 19, 2014), *available at* https://about.fb.com/news/2014/02/facebook-to-acquire-whatsapp/ (last accessed Jan. 19, 2026).

at least one member of the putative class is a citizen of a foreign state, and Defendants are citizens of California and Delaware.

17. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

18. This Court has general personal jurisdiction over Defendants because their principal places of business are in California. Additionally, Defendants are subject to specific personal jurisdiction in this state because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in this state.

19. Venue is proper in this District under the provisions of 28 U.S.C. § 1391(b), because Defendants are headquartered in this district and a substantial portion of the events or omissions giving rise to the claims occurred in this judicial district.

FACTUAL ALLEGATIONS

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

20. Founded in 2009 by Jan Koum and Brian Acton, WhatsApp historically prided itself on being outside the big data economy driven by tech giants like Facebook—an oasis of privacy in a world where Facebook seemingly knew everything about everyone. In a 2009 blog post, Mr. Koum "set the record straight": "We have not, we do not and we will not **ever** sell your personal information to anyone. Period. End of story."[12] In 2012, WhatsApp's co-founders explained they charged for WhatsApp to keep it ad-free because "[a]t every company that sells ads, a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the servers that hold all the data and making sure it's all being logged and collated and sliced and packaged and shipped out[.]"[13] They cautioned: "Remember,

[12] WhatsApp, "Just wanted to say a few things" (Nov. 19, 2009), *available at* https://blog.whatsapp.com/just-wanted-to-say-a-few-things (last accessed Jan. 19, 2026).

[13] WhatsApp, "Why we don't sell ads" (Jun. 18, 2012), *available at* https://blog.whatsapp.com/why-we-don-t-sell-ads (last accessed Jan. 19, 2026).

when advertising is involved **you the user** are the product."[14] But at WhatsApp, they stressed, ***"[y]our data isn't even in the picture. We are simply not interested in any of it."***[15]

21. When Facebook acquired WhatsApp in 2014, there was widespread concern that WhatsApp's respect for users' data and privacy would be compromised. But Mr. Koum again "set[] the record straight," reminding users of his experience growing up in Ukraine, where KGB monitoring of phone calls was commonplace and part of the reason his family emigrated; at WhatsApp, he stated, ***"[r]espect for your privacy is coded into our DNA[.]"***[16] Complaining that speculation that WhatsApp's partnership with Facebook would change its core principles was "baseless," "unfounded," and "irresponsible," Mr. Koum assured users that WhatsApp's "focus remains on delivering the promise of WhatsApp far and wide, ***so that people around the world have the freedom to speak their mind without fear."***[17] Facebook CEO Mark Zuckerberg also assured the public that "[t]he vision is to keep the [WhatsApp] service exactly the same," noting WhatsApp "neither uses nor stores any of the billions of photos and chats exchanged on the app daily." Instead, WhatsApp content is deleted "almost instantly," which is "what people want," and "[w]e would be pretty silly to get in the way of that."[18]

22. Given the consumer concern that Meta might obtain access to WhatsApp messages, WhatsApp has repeatedly and emphatically promised that end-to-end encryption for everyone prevents anyone—even WhatsApp and Meta—from accessing private communications. It is clear WhatsApp and Meta marketed WhatsApp in this way because they (correctly) determined that this

---

[14] *Id.* (emphasis original).

[15] *Id.* (emphases added).

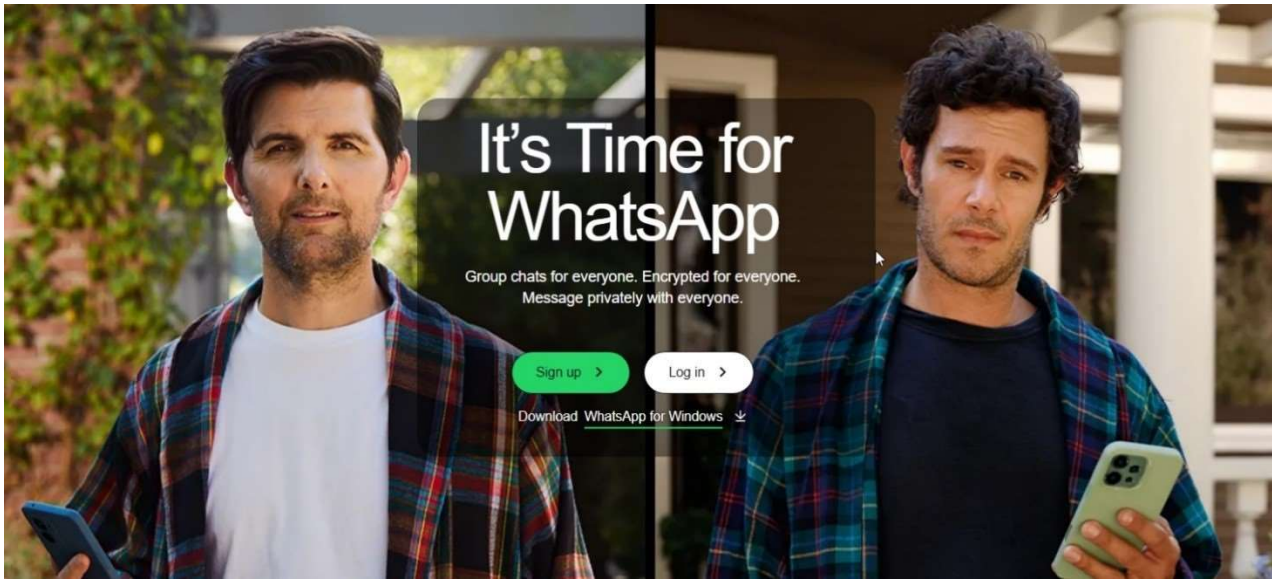
[16] WhatsApp, "Setting the record straight" (Mar. 17, 2014), *available at* https://blog.whatsapp.com/setting-the-record-straight (last accessed Jan. 19, 2026) (emphases added).

[17] *Id.* (emphases added).

[18] *See, e.g.*, B. Bosker, "Zuckerberg Promises Facebook Won't Read Your WhatsApp Chats," *The Huffington Post* (Feb. 24, 2014), *available at* https://www.huffpost.com/entry/zuckerberg-facebook-whatsapp_n_4848205#:~:text=top%20stories%20here.-,Zuckerberg%20Promises%20Facebook%20Won't%20Read%20Your%20WhatsApp%20Chats,of%20that%2C%22%20he%20added (last accessed Jan. 19, 2026).

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

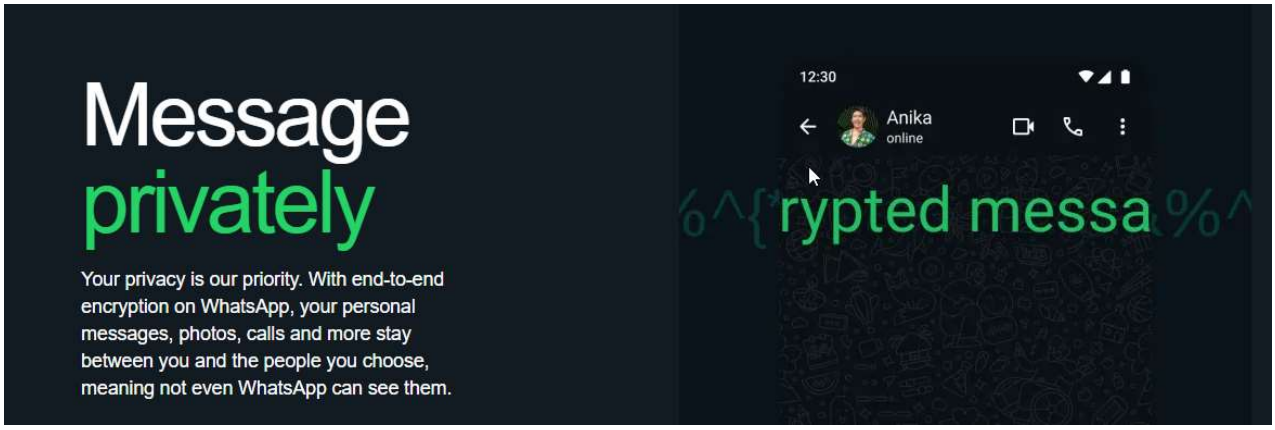
23. For example, until recently, the first image that greeted users upon visiting WhatsApp's website touted that WhatsApp is "[e]ncrypted for everyone" and allows users to "[m]essage privately with everyone":[19]



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

[19] WhatsApp, Homepage, *available at* https://www.whatsapp.com (last accessed Nov. 30, 2025).

[20] WhatsApp, "Privacy," *available* at https://www.whatsapp.com/privacy (last accessed Jan. 19, 2026) (emphases added).



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

[21] WhatsApp, "Privacy," *available* at https://www.whatsapp.com/privacy (last accessed Jan. 19, 2026) (excerpted).

26. WhatsApp's "FAQ" again reinforces that "not even WhatsApp[] can read, listen to, or share" users' personal images and calls," emphasizing that end-to-end encryption happens "automatically":[22]

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.

27. Notably, WhatsApp chats have this header emblazoned at the top:

28. Importantly, neither WhatsApp nor Meta discloses anywhere their unlimited access to users' encrypted communications—not even in the fine print. WhatsApp discloses only certain limited exceptions to its end-to-end encryption and the ability of WhatsApp, Meta, and third parties to access encrypted message content. For example, WhatsApp discloses that when a user reports another user in an individual chat, WhatsApp receives up to five of the last messages the reported user sent to the reporting user.[23] Similarly, when a user reports abuse in a group chat, WhatsApp receives up to five of the last messages sent to the reporting user within the reported group. Where

---

[22] WhatsApp, "About end-to-end encryption," *available at* https://faq.whatsapp.com/820124435853543/?locale=en_US (last accessed Jan. 19, 2026) (annotations added).

[23] WhatsApp, "About reporting and blocking on WhatsApp," *available at* https://faq.whatsapp.com/414631957536067/?helpref=faq_content&cms_platform=web (last accessed Jan. 19, 2026).

calls take place in an individual chat, WhatsApp may also receive basic information about the last five calls with that user, such as who initiated the call and the duration of the call.[24] Nothing in these disclosures suggests that WhatsApp or Meta can access ***all*** of any user's communications. Nor do the disclosures suggest that WhatsApp or Meta can access a user's communications even when the limited circumstances identified in the disclosures do not apply.

29. WhatsApp likewise discloses that when customers contact WhatsApp for customer support, they may provide WhatsApp with information, "including copies of [their] messages."[25] Here too, however, this disclosure does not suggest WhatsApp and Meta can access any message the user does ***not*** provide to customer support.

30. WhatsApp also carves out from its claims that WhatsApp and Meta cannot see users' messages certain specific use cases, including business messaging services (which it says are clearly distinguished from personal messages) and communications that are not encrypted (such as communications with Meta services or communications with businesses using Cloud API.[26] Once again, nothing in these disclosures suggests WhatsApp and Meta can access all of a user's encrypted messages.

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

> In the ordinary course of providing our service, ***WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages***. Undelivered messages are deleted from our servers after 30 days. . . [W]e may collect, use, preserve, and share ***user information*** if we have a good-faith belief that it is reasonably necessary to (a) keep our users safe, (b) detect, investigate, and

---

[24] *Id.*

[25] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

[26] WhatsApp, "How you interact with others," *available at* https://faq.whatsapp.com/9658856237523915 (last accessed Jan. 19, 2026); WhatsApp, "About end-to-end encryption," *available at* https://faq.whatsapp.com/820124435853543/ (last accessed Jan. 19, 2026); WhatsApp, "WhatsApp Encryption Overview: Technical White Paper," *available at* https://scontent.xx.fbcdn.net/v/t39.8562-6/455962147_1148247109601582_1673264986279156121_n.pdf?_nc_cat=101&ccb=1-7&_nc_sid=e280be&_nc_ohc=QeHE3hZyqTUQ7kNvwHTaYvz&_nc_oc=AdnI2TA1TwLkU-lslAuP5ZdFKjtEW2P5xXkvd1XDRqebpLQHtAmKQUBysG47pnDIsbw&_nc_zt=14&_nc_ht=scontent.xx&_nc_gid=zODDu4H8Iis7NtbQUdNW6Q&oh=00_AfrHORvnclt45MEsoeo1KIAhIOvsvWV8uzMwxNqLPGAaJA&oe=69747019 (last accessed Jan. 19, 2026).

> prevent illegal activity, (c) respond to legal process, or to government requests, (d) enforce our Terms and policies. This may include information about how some users interact with others on our service. ***We also offer end-to-end encryption for our services, which is always activated. End-to-end encryption means that messages are encrypted to protect against WhatsApp and third parties from reading them***.[27]

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

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

32. End-to-end encryption is a method of securing digital communications wherein data is encrypted on the sender's device and only decrypted once it reaches the recipient's device. As WhatsApp analogizes, "with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. All of this happens automatically: no need to turn on any special settings to secure your messages."[28] In theory, even though encrypted communications may pass through a service provider's servers on their way to the intended recipient, they remain encrypted and unreadable to everyone but that intended recipient, because only the sender and the recipient have the key to "unlock" them on their respective devices.

33. In November 2014, shortly after its acquisition by Facebook (now Meta), WhatsApp partnered with Open Whisper Systems to integrate the Signal Protocol, an end-to-end encryption cryptographic protocol, into its platform.[29] (Open Whisper Systems offers its own end-to-end encrypted messaging application, called Signal.) By April 5, 2016, WhatsApp had completed integration of end-to-end encryption for all forms of communication across all user devices.[30]

---

[27] WhatsApp, "Information for Law Enforcement Authorities," *available at* https://faq.whatsapp.com/444002211197967 (last accessed Jan. 19, 2026) (emphases added).

[28] WhatsApp, "FAQ: How does WhatsApp work?" *available at* https://faq.whatsapp.com/820124435853543 (last accessed Jan. 19, 2026).

[29] Signal, "Open Whisper Systems partners with WhatsApp to provide end-to-end encryption" (Nov. 18, 2014), *available at* https://signal.org/blog/whatsapp/ (last accessed Jan. 19, 2026).

[30] Signal, "WhatsApp's Signal Protocol integration is now complete," (Apr. 5, 2016), *available at* https://signal.org/blog/whatsapp-complete/ (last accessed Jan. 19, 2026).

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

35. Signal itself notably makes its source code available for public inspection to promote both transparency and security (by allowing the public at large, including security analysts and researchers, to test for and identify vulnerabilities), and reviews of Signal's source code have in fact confirmed that it has no backdoor to its end-to-end encryption. But under Meta's ownership, WhatsApp does not make its source code available to the public or even to third party security auditors. Accordingly, although cryptosecurity experts are confident the Signal app functions without any kleptographic backdoor, the public can only take the word of Meta and WhatsApp that they do not have access to the substance of WhatsApp users' communications.

36. Meta's and WhatsApp's claim that they do not have access to the substance of WhatsApp users' communications is false. As the whistleblowers here have explained, WhatsApp and Meta store and have unlimited access to WhatsApp encrypted communications, and the process for Meta workers to obtain that access is quite simple. A worker need only send a "task" (*i.e.*, request via Meta's internal system) to a Meta engineer with an explanation that they need access to WhatsApp messages for their job. The Meta engineering team will then grant access—often without any scrutiny at all—and the worker's workstation will then have a new window or widget available

that can pull up any WhatsApp user's messages based on the user's User ID number, which is unique to a user ***but identical across all Meta products***.

37. Once the Meta worker has this access, they can read users' messages by opening the widget; no separate decryption step is required. The WhatsApp messages appear in widgets commingled with widgets containing messages from unencrypted sources. Messages appear almost as soon as they are communicated—essentially, in real-time. Moreover, access is unlimited in temporal scope, with Meta workers able to access messages from the time users first activated their accounts, including those messages users believe they have deleted.

38. Some users—such as certain celebrities, politicians, and Meta employees—are afforded special handling by Meta such that access to their encrypted messages is more closely ***tracked*** within Meta and WhatsApp. Meta workers still have access to these users' messages, but their access of the accounts flags the worker for investigation. Even as to these privileged few WhatsApp users, however, Meta and WhatsApp are still misleading them and violating their privacy by storing their supposedly private, end-to-end encrypted, messages.

39. Although Meta has kept the circle on its fraud small, it has not kept it small enough. It attempted to prevent dissemination of this information by heavily siloing workers in different groups and telling them to "stay in [their] lane" when and if they started to piece together the truth. As discussed below, Meta also actively misrepresented the facts about its access and storage when journalists came close to discovering the truth. Meta has also tried to prevent the truth from coming out by imposing onerous nondisclosure agreements on its workers, essentially threatening the full force of one of the world's richest companies if any of these individuals dared reveal what goes on behind closed doors at the company. These efforts have now failed, but they worked for many, many years by obscuring the truth.

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

40. In an age where (i) Meta can trace Facebook users' every click and scroll and (ii) Internet surfers are called on to choose (or ignore) cookie preferences multiple times per day, invasions of online privacy can too easily be undervalued. But that is not the case for the private

substance of WhatsApp users' encrypted communications, which both WhatsApp and Meta have conditioned WhatsApp users to believe are inviolate.

41. Indeed, WhatsApp has long been used throughout the world by journalists, dissidents, activists, and others for whom maintaining confidences can mean the difference between life and death, freedom and incarceration, or exposing truth and letting it languish in shadows.

42. For example, end-to-end encryption of voice memos, which prevents access by third parties, is a particularly useful feature of WhatsApp for journalists reporting news from war-torn regions. As CBS reporter Amjad Tadros explained: "I use it a lot, especially in covering the news in Yemen as it is hard to get a clean phone line there. I end up sending the questions on WhatsApp and get the answers back in text or voice."[31]

43. In Venezuela, for example, where state surveillance under the authoritarian dictatorship of Nicolas Maduro reached a "massive scale," independent media advocates urged "[m]embers of at-risk organizations such as journalists, human rights defenders, and social and political activists" to "take measures to protect the security and privacy of their communications" by using "instant messaging apps that have end-to-end encryption such as . . . WhatsApp."[32]

44. In many countries in which WhatsApp is a popular communication tool, a person's private expressions of intimacy can expose them to dire penalties. Nearly 40% of people use WhatsApp in Egypt, for example, where the United States Department of State cautions that Egyptian authorities use both social media and dating apps to entrap suspected gay and lesbian people for "debauchery," a crime punishable there by up to 10 years in prison.[33] In such places, the ability to send truly private messages to intimate partners is priceless.

---

[31] *See, e.g.*, Foreign Press Correspondents USA, "*Using WhatsApp as a Journalistic Tool*," (June 26, 2022), available at https://foreignpress.org/journalism-resources/using-whatsapp-as-a-journalistic-tool (last accessed Jan. 19, 2026).

[32] D. Aragort, "The Reality of Digital Authoritarianism in Venezuela," *Center for International Media Assistance* (Sept. 20, 2022), *available at* https://www.cima.ned.org/blog/the-reality-of-digital-authoritarianism-in-venezuela/ (last accessed Jan. 19, 2026).

[33] *See, e.g.*, U.S. Dept. of State, "Egypt," *available at* https://travel.state.gov/en/international-travel/travel-advisories/egypt.html#local (last accessed Jan. 19, 2026).

45. The life-or-death stakes for dissidents who mistakenly believe their communications on WhatsApp are private is illustrated by the fallout from the Pegasus spyware, developed by Israeli surveillance firm NSO Group and sold only to governments. Most prominently, self-exiled Saudi activist Omar Abdulaziz communicated with (also self-exiled) Saudi journalist and regime critic Jamal Khashoggi in hundreds of WhatsApp messages they believed were private and encrypted. As CNN journalists Nina dos Santos and Michael Kaplan noted, Mr. Khashoggi's public criticism of Saudi Crown Prince Mohammad bin Salman was "measured," but "[*i*]*n private, the Washington Post columnist didn't hold back*," calling the Crown Prince a "'beast' [and] a 'pac-man' who would devour all in his path," citing hundreds of WhatsApp messages they were provided to review.[34] Messrs. Abdulaziz and Khashoggi used WhatsApp to coordinate funding and SIM cards for a cyber-army of social media warriors to combat state-sponsored propaganda in Saudi Arabia in messages that would be deemed "treasonous" by Saudi authorities.[35] Just one day after the University of Toronto's Citizen Lab published a report detailing how it had concluded with "high confidence" that a Saudi "operator" infected Mr. Abdulaziz's cell phone with Pegasus spyware that permitted the Saudis to surveil his communications (including his WhatsApp messages),[36] Mr. Khashoggi was killed and dismembered in the Saudi embassy in Istanbul, Turkey.[37] To be clear, Plaintiffs do not allege—or even suggest—that Meta's and WhatsApp's secret access to Mr. Khashoggi's private WhatsApp communications caused or contributed to his death. Indeed, WhatsApp obtained a legal

---

[34] N. dos Santos and M. Kaplan, "Jamal Khashoggi's private WhatsApp messages may offer new clues to killing," CNN World (Dec. 4, 2018), *available at* https://edition.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html (last accessed Jan. 19, 2026) (emphases added).

[35] *Id.*

[36] B. Marczak *et al.*, "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," Citizen Lab (Oct. 1, 2018), *available at* https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/ (last accessed Jan. 19, 2026).

[37] A. Schmidt, "'I know why Jamal was killed': Saudi activist in Canada says hacked phones led to Jamal Khashoggi's murder," *CBC* (Nov. 1, 2021), *available at* https://www.cbc.ca/documentaries/the-passionate-eye/i-know-why-jamal-was-killed-1.6232638 (last accessed Jan. 19, 2026).

victory against the NSO Group for its targeting of WhatsApp users using spyware exploits (not decryption). But Mr. Khashoggi's experience illustrates two important points that are relevant to Plaintiffs' allegations in this case: (i) people are more likely to express uninhibited and private thoughts—even those for which they could be targeted or severely punished—when they believe their communications with trusted individuals cannot be compromised; and (ii) unintended access to such private communications on trusted platforms can have devastating consequences.

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

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

47. Over the years, Meta's name has become synonymous with user privacy violations. Again and again, Meta/Facebook has violated users' privacy rights by using their information in undisclosed ways, such as disclosing their personal data *en masse* to third parties with no verified need for the information in violation of stated privacy policies, failing to apprise users of data

---

[38] *See, e.g.*, S. Hardman Taylor & N. Bazaroya, "Always Available, Always Attached: A Relational Perspective on the Effects of Mobile Phones and Social Media on Subjective Well-Being," 26 *J. of Comp.-Mediated Commc'n* 187 (Aug. 24, 2021), *available at* https://doi.org/10.1093/jcmc/zmab004 (last accessed Jan. 19, 2026).

[39] *See, e.g.*, A. Stuart, A. Bandara & M. Levine, "The Psychology of Privacy in the Digital Age," *Social and Personality Psychology Compass* (Nov. 2019), *available at* https://www.researchgate.net/publication/337190293_The_psychology_of_privacy_in_the_digital_age (last accessed Jan. 19, 2026).

[40] *See, e.g.*, M. Büchi, N. Festic & M. Latzer, "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda," *Big Data & Society* (2022), *available at* https://doi.org/10.1177/20539517211065368 (last accessed Jan. 19, 2026).

breaches and misuses—including in the data misuse at the center of the infamous 2016 Cambridge Analytica scandal—and then affirmatively misleading the public as to whether such privacy violations had occurred. One would think Meta would have learned from this history. It clearly has not.

48. For example, on November 29, 2011, the United States Federal Trade Commission ("FTC") announced Facebook had agreed to enter into a 20-year consent order (finalized in 2012) in settlement of an eight-count complaint alleging Facebook "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing [that information] to be shared and made public."[41] Among other things, the FTC charged Facebook with (i) failing to warn users that information they designated private (such as their "Friends List[s]") would be made public; (ii) giving third-party apps access to "nearly all of users' personal data"—data the apps did not need—despite Facebook's representations these apps would have access only to user information needed to operate; (iii) misrepresenting to users that they could restrict data sharing to "Friends Only" when that information was shared with third-party applications their friends used; (iv) claiming it certified the security of apps in its "Verified Apps" program when it did not; (v) falsely promising it would not share users' personal information with advertisers; and (vi) allowing access to users' photos and videos even after users deactivated or deleted their accounts, despite claiming they would be inaccessible.[42]

49. The consent order (among other things) barred Facebook from making any further misrepresentations about the privacy or security of consumers' personal information; required

---

[41] Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises" (Nov. 29, 2011), *available at* https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises (last accessed Jan. 19, 2026); *In the Matter of Facebook, Inc.*, No. 092 3184, Agreement Containing Consent Order, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf (last accessed Jan. 19, 2026).

[42] Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises" (Nov. 29, 2011), *available at* https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises (last accessed Jan. 19, 2026).

Facebook to get consumers' affirmative express consent before enacting changes overriding their privacy preferences; required Facebook to establish and maintain a "comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services and to protect the privacy and confidentiality of consumers' information"; and subjected Facebook to periodic assessments of its privacy practices by independent, third-party auditors for the 20-year life of the consent order.[43]

50. The FTC commenced a wide-ranging investigation into Facebook's continuing privacy violations in March 2018, catalyzed by the revelation of Cambridge Analytica's use of data from tens of millions of Facebook users to build voter profiles and sprawled from there.[44] On July 24, 2019, the FTC announced it was levying an historic ***$5 billion*** penalty against Facebook (approved by a court in 2020) for violations of the 2012 consent order, which was "the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide" and "one of the largest penalties ever assessed by the U.S. government for any violation" of any kind.[45]

51. As then-FTC Chairman Joe Simons explained, "[d]espite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers' choices."[46] Specifically, notwithstanding the 2012 consent order, Facebook "repeatedly used deceptive disclosures and settings to undermine users' privacy

---

[43] *Id.*

[44] T. Romm & C. Timberg, "FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information," *Washington Post* (Mar. 20, 2018), *available at* 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/ (last accessed Jan. 19, 2026).

[45] Federal Trade Commission, "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), *available at* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (last accessed Jan. 19, 2026).

[46] *Id.*

preferences" and "share[d] users' personal information with third party-apps that were downloaded by the users' Facebook 'friends.'"[47]

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

53. Unfortunately, the FTC grossly overestimated the impact of the $5 billion fine and strengthened reporting requirements on trillion-dollar Meta. Indeed, the value of Facebook's stock actually *went up* by 1% following the announcement of the $5 billion penalty; the market—like Facebook—realized that "despite the penalty's unprecedented size," it was "still just a drop in the ocean compared to the gigantic amount of cash Facebook regularly produces."[49] Following the announcement of the penalty, Facebook CEO Mark Zuckerberg's shares increased in value by more than $1 billion in just thirty minutes.[50]

---

[47] *Id.*; *United States v. Facebook, Inc.*, No. 19-cv-2184, ECF No. 1, Complaint for Civil Penalties, Injunction, and Other Relief (D.D.C. July 24, 2019), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf (last accessed Jan. 19, 2026).

[48] Federal Trade Commission, "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), *available at* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (last accessed Jan. 19, 2026).

[49] R. Price, "Why Facebook's stock jumped despite facing a record-breaking $5 billion FTC penalty: 'A slap on the wrist,'" *Business Insider* (July 12, 2019), *available at* https://www.businessinsider.com/facebook-stock-rose-news-5-billion-ftc-settlement-why-critics-2019-7 (last accessed Jan. 19, 2026).

[50] B. Gilbert, "Mark Zuckerberg actually got $1 billion richer following the news of Facebook's $5 billion fine for the biggest scandal in the company's history," *Business Insider* (July 15, 2019), *available at* https://www.businessinsider.com/mark-zuckerberg-net-worth-increases-after-5-billion-facebook-fine-2019-7 (last accessed Jan. 19, 2026).

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

55. Indeed, in May 2023, the FTC charged Meta with violations of the 2020 order that was entered at the conclusion of the 2019 proceedings, alleging (among other things) that Meta had "misled parents about their ability to control with whom their children communicated through its Messenger Kids app" and "misrepresented the access it provided some app developers to private user data."[52] Once again, the FTC expressed its dismay with Meta's behavior, with the Director of the FTC's Bureau of Consumer Protection stating, "Facebook has repeatedly violated its privacy promises. . . . The company's recklessness has put young users at risk, and Facebook needs to answer for its failures."[53] These proceedings against Meta are ongoing.

56. The SEC also fined then-Facebook $100 million for misleading the public regarding the Cambridge Analytica scandal.[54] For more than two years, Facebook knew Cambridge Analytica had actually used tens of millions of Facebook users' data, but misrepresented the risk of misuse of user data as a purely hypothetical occurrence in its communications to investors (and, by extension,

---

[51] Federal Trade Commission, "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), *available at* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook (last accessed Jan. 19, 2026).

[52] Federal Trade Commission, "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), *available at* https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data (last accessed Jan. 19, 2026).

[53] *Id.*

[54] Securities & Exchange Commission, "Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data" (July 24, 2019), *available at* https://www.sec.gov/newsroom/press-releases/2019-140 (last accessed Jan. 19, 2026).

the public generally).[55] The SEC noted "Facebook exacerbated its disclosure failures when it misled reporters who asked the company about its investigation into Cambridge Analytica."[56]

57. Meta's disregard for user privacy has also resulted in European regulators imposing penalties against it totaling billions of dollars for its repeated violation of the General Data Protection Regulation ("GDPR"). For example, in November 2022, the Irish Data Protection Commission fined Meta €265 million for a massive data leak in 2021 that resulted in the data—including mobile numbers, Facebook IDs, names, genders, locations, relationship statuses, occupations, dates of birth, and email addresses—of 533 million Facebook users in 106 countries worldwide appearing in a public hacking forum.[57] In addition to drawing the ire and penalties of regulators, Meta's initial decision ***not to notify impacted users individually*** was roundly condemned by security experts because the data could be used for targeted phishing attacks and identity theft.[58]

58. In January 2023, the Irish Data Protection Commission fined Meta €390 million for improperly processing user data for advertising targeting purposes in violation of the GDPR.[59]

59. Then, on May 22, 2023, the Irish Data Protection Commission, acting on findings by the European Data Protection Board, imposed the largest GDPR fine ever issued—€1.2 billion—on

---

[55] *Id.*

[56] *Id.*

[57] An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), "Data Protection Commission announces decision in Facebook 'Data Scraping' Inquiry" (Nov. 28, 2022), *available at* https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry#Meta (last accessed Jan. 19, 2026); E. Bowman, "After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users," *NPR* (Apr. 9, 2021), *available at* https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users (last accessed Jan. 19, 2026).

[58] *Id.*; *Sec. Mag.*, "Facebook breach exposes 533 million users" (Apr. 6, 2021), *available at* https://www.securitymagazine.com/articles/94962-facebook-breach-exposes-533-million-users (last accessed Jan. 19, 2026).

[59] An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), "Data Protection Commission announces conclusion of two inquiries into Meta Ireland" (Jan. 4, 2023), *available at* https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland#Meta (last accessed Jan. 19, 2026).

Meta's Irish subsidiary for "systematic, repetitive and continuous" illegal transfers of the personal data of millions of European users to the United States.[60]

60. On September 27, 2024, the Irish Data Protection Commission fined Meta €91 million for storing user passwords in plain text ***without encryption or other protective measures***.[61] As the Data Protection Deputy Commissioner noted, "It is widely accepted that user passwords should not be stored in plaintext, considering the risks of abuse that arise from persons accessing such data. It must be borne in mind, that the passwords the subject of consideration in this case, are particularly sensitive, as they would enable access to users' social media accounts."[62] Notably, although the violation was self-reported by Meta in 2019, regulators reprimanded Meta's Irish subsidiary for failing to report and document the violation appropriately.[63] According to one Facebook source, between 200 million and 600 million users' account passwords were plaintext searchable by more than 20,000 Facebook employees, and some 2,000 engineers and developers made approximately nine million internal queries for data elements that contained plain text user passwords during the time the passwords were mishandled.[64]

61. Yet again, on December 17, 2024, the Irish Data Protection Commission imposed an additional €251 million fine on Meta for a 2018 data breach compromising data including the full names, email addresses, phone numbers, locations, places of work, dates of birth, religions, genders, timeline posts, group memberships, and children's personal data of approximately 29 million users,

---

[60] European Data Protection Board, "1.2 billion euro fine for Facebook as a result of EDPB binding decision" (May 22, 2023), *available at* https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (last accessed Jan. 19, 2026).

[61] An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), "Irish Data Protection Commission fines Meta €91 million" (Sept. 27, 2024), *available at* https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta#Meta (last accessed Jan. 19, 2026).

[62] *Id.*

[63] *Id.*

[64] B. Krebs, "Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years" (Mar. 21, 2019), *Krebs on Security*, *available at* https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/ (last accessed Jan. 19, 2026).

including three million users in Europe.[65] Once again, the Data Protection Commission reprimanded Meta for failing to document and make a full disclosure to the Commission regarding the breach.[66] The Deputy Commission noted the severity and dangers of the breach: "[F]ailure to build in data protection requirements . . . can expose individuals to very serious risks and harms, including a risk to the fundamental rights and freedoms of individuals. Facebook profiles can, and often do, contain information about matters such as religious or political beliefs, sexual life or orientation, and similar matters that a user may wish to disclose only in particular circumstances."[67]

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

63. Aside from privacy violations, on May 18, 2017, European regulators also fined then-Facebook for providing "incorrect or misleading information" during European review of Facebook's acquisition of WhatsApp in 2014.[68] Specifically, Facebook assured regulators that any technical integration of Facebook and WhatsApp users' accounts could not be accomplished reliably.[69] Yet in 2016, when WhatsApp announced changes to its Terms of Service and Privacy Policy, it expressly included the possibility of linking WhatsApp users' phone numbers with Facebook user identities—precisely what Facebook had assured European regulators it could not

---

[65] An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), "Irish Data Protection Commission fines Meta €251 million" (Dec. 17, 2024), *available at* https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million (last accessed Jan. 19, 2026).

[66] *Id.*

[67] *Id.*

[68] European Commission, "Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover" (May 17, 2017), *available at* https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1369 (last accessed Jan. 19, 2026).

[69] *Id.*

do.[70] Although the European Commission did not take steps to unwind the long-closed merger, it fined Facebook, finding that contrary to Facebook's statements to regulators during the merger review process, "the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility."[71] Accordingly, Meta's and WhatsApp's false claims they cannot access WhatsApp users' encrypted communications are not the first time Meta has misrepresented its technical capabilities with respect to WhatsApp users' data to get what it wanted.

64. At the same time regulators have been reprimanding and fining Meta for its repeated privacy violations and failures to safeguard users' information, Meta has downsized several of the very business units charged with user protection. For example, Meta recently laid off more than 100 people in its risk review organization, which includes the employees responsible for making sure Meta's platforms comply with its obligations under the FTC consent order and privacy requirements imposed by regulatory bodies worldwide.[72] Meta employees described the layoffs "as a 'gutting' of the workers in the department who review projects at Meta for privacy and integrity risks."[73] According to Meta insiders, "Meta executives have become frustrated with the pace of product development," and "[o]ne division holding things up—by design—was the company's risk organization."[74] Although Meta claims the layoffs reflect a transition to automated processes that will be superior to manual review, "[c]urrent and former employees in the risk organization said they were skeptical that replacing [the laid-off employees] with automated systems would be as effective, particularly around issues as sensitive as user privacy."[75]

---

[70] *Id.*

[71] *Id.*

[72] M. Isaac & E. Tan, "Meta Layoffs Included Employees Who Monitored Risks to User Privacy," *New York Times* (Oct. 23, 2025), *available at* https://www.nytimes.com/2025/10/23/technology/meta-layoffs-user-privacy.html (last accessed Jan. 19, 2026).

[73] *Id.*

[74] *Id.*

[75] *Id.*

65. Meta also has a prolific track record of deceiving the public. In addition to its concealment of the Cambridge Analytica scandal and its repeated censure by European regulators for its privacy and disclosure failures, Meta has come under fire for its concealment and misrepresentation of information regarding risks posed by its platforms. As but one example, former Facebook employee and whistleblower Frances Haugen's 2021 disclosure of "The Facebook Papers" revealed that Meta had conducted internal research regarding the negative impact of Instagram on teenage mental health (concluding, for example, that "[w]e [Facebook-owned Instagram] make body image issues worse for one in three teen girls"), yet concealed these findings from regulators and the public while downplaying these risks to the public.[76] Meta reportedly abandoned a research project into the effects of a Facebook/Instagram hiatus after data suggested users benefited. One Meta employee warned Meta's concealment of its research findings could be likened to the tobacco industry's concealment of negative research findings relating to the dangers of cigarettes.[77]

66. According to filings in a recent multi-district litigation against Meta by parents, children, school districts, and state attorneys general, Meta "was aware that millions of adult strangers were contacting minors on its sites; that its products exacerbated mental health issues in teens; and that content related to eating disorders, suicide, and child sexual abuse was frequently detected, yet rarely removed," but Meta failed to disclose these dangers to the public or to Congress.[78] In fact, when the Senate Judiciary Committee asked Meta in written questions in

---

[76] S. Ramachandran, "Whistleblower's testimony has resurfaced Facebook's Instagram problem," *NPR* (Oct. 5, 2021), *available at* https://www.npr.org/2021/10/05/1043194385/whistleblowers-testimony-facebook-instagram (last accessed Jan. 19, 2026); J. Wakefield, "Facebook under fire over secret teen research," *BBC* (Sept. 15, 2021), *available at* https://www.bbc.com/news/technology-58570353 (last accessed Jan. 19, 2026); C. Duffy, "Lawsuit alleges social media giants buried their own research on teen mental health harms," *CNN* (Nov. 26, 2025), *available at* https://www.cnn.com/2025/11/25/tech/social-media-youth-mental-health-lawsuit-meta-tiktok-snap-youtube (last accessed Jan. 19, 2026).

[77] *Id.*

[78] C. Alter, "Court Filings Allege Meta Downplayed Risks to Children and Misled the Public," *Time* (Nov. 22, 2025), *available at* https://time.com/7336204/meta-lawsuit-files-child-safety/ (last accessed Jan. 19, 2026).

December 2020 whether it could "determine whether increased use of its platform among teenage girls has any correlation with increased signs of depression" and "increased signs of anxiety," the company answered simply "No."[79]

67. On November 14, 2023, a bipartisan group of United States Senators sent a letter to Meta CEO Mark Zuckerberg accusing Meta of misleading Congress.[80] According to these Senators, "Meta's representations to the public and in response to Congressional inquiries concealed and misrepresented its extensive knowledge about the threats to young people on its platforms."[81] They also stated: "Members of Congress have repeatedly asked Meta for information on its awareness of threats to young people on its platforms and the measures that it has taken, only to be stonewalled and provided non-responsive or misleading information. . . . Rather than act on these stunning findings, Meta hid this information from the public and Congressional oversight while providing misleading statistics, ignoring recommendations to protect teens, and even rolling back safety tools."[82] That Meta is misleading the public, the U.S. Congress, and regulators worldwide regarding the extensive evidence of the risks its platforms pose to teens is consistent with what one whistleblower described as Meta's fostered culture of "see no evil, hear no evil."[83]

68. Meta's documented misrepresentations are not limited to risks to youth posed by its platforms. Meta has also recently come under fire for misrepresenting its activities in China and

---

[79] *Id.*

[80] Office of Senator Dick Durbin (R.-Ill.), "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), *available at* 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 (last accessed Jan. 19, 2026).

[81] *Id.*

[82] *Id.*

[83] D. Kerr, "Meta failed to address harm to teens, whistleblower testifies as senators vow action," *NPR* (Nov. 7, 2023), *available at* https://www.npr.org/2023/11/07/1211339737/meta-failed-to-address-harm-to-teens-whistleblower-testifies-as-senators-vow-act (last accessed Jan. 19, 2026).

sharing certain user data with the Chinese Communist Party following the release of former Meta employee Sarah Wynn-Williams' best-selling, revealing memoir, *Careless People*.[84]

69. As one Republican U.S. Senator said of Mark Zuckerberg's testimony over the course of multiple Congressional hearings, "[e]very time it's a different answer. Every time it's a different façade. . . . But every time the one consistent through-line is every time it's something misleading. Every time is something other than the truth."[85]

70. The pattern is clear: Meta consistently prioritizes profit over the privacy and safety of its users and is willing to lie to achieve its priorities. Because even record-breaking fines imposed by regulators are essentially rounding errors to Meta's bottom line, Meta's conduct continues undeterred and unabated, as evidenced by Meta's brazen willingness to mislead WhatsApp users regarding its and WhatsApp's ability to access users' encrypted communications.

CLASS ACTION ALLEGATIONS

71. Class: Plaintiffs seek to represent the following Class of similarly situated individuals defined as follows:

> All WhatsApp users, excluding residents of the United States, Canada, Andorra, Austria, Azores, Belgium, Bulgaria, Canary Islands, Channel Islands, Croatia, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Gibraltar, Greece, Guadeloupe, Hungary, Iceland, Ireland, Isle of Man, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Madeira, Malta, Martinique, Mayotte, Monaco, Netherlands, Norway, Poland, Portugal, Republic of Cyprus, Réunion, Romania, San Marino, Saint-Martin, Slovakia, Slovenia, Spain, Sweden, Switzerland, the United Kingdom, United Kingdom sovereign bases in Cyprus (Akrotiri and Dhekelia), and Vatican City, who between April 5, 2016 and the present sent or received any communications via WhatsApp.

72. Excluded from the Class are Defendants, any affiliate, parent, or subsidiary of Defendants; any entity in which any Defendant has a controlling interest; any officer, director, or employee of any Defendant; any successor or assign of any Defendant; anyone employed by counsel

---

[84] K. Collier, "Senators vow to continue probe of Meta over its China record after ex-employee testifies," *NBC News* (Apr. 9, 2025), *available at* https://www.nbcnews.com/tech/social-media/facebook-meta-whistleblower-senate-video-book-careless-people-rcna200517 (last accessed Jan. 19, 2026).

[85] *Id.*

in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

73. Numerosity (Rule 23(a)(1)): Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of members of the Class is unknown to Plaintiffs at this time. However, it is estimated that there are at least three billion individual members of the class. The identity of such membership is readily ascertainable from Defendants' records, including from Meta's and WhatsApp's records of WhatsApp account holders.

74. Typicality (Rule 23(a)(3)): Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all Class Members, each have used WhatsApp on one or more occasions between April 5, 2016 and the present, and had their private encrypted communications subjected to access by WhatsApp and Meta.

75. Adequacy (Rule 23(a)(4)): Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of other Class Members. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the field of digital privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of all Class Members.

76. Commonality (Rule 23(a)(2)): Questions of law and fact are common to the members of the Class because Defendants have acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Class include, *inter alia*:

- Whether Defendants intercepted users' WhatsApp communications;
- Whether Defendants' interception of users' WhatsApp communications was intentional;
- Whether Defendants' interception of users' WhatsApp communications occurred while those communications were in transit;
- Whether Defendants store users' WhatsApp communications;

- Whether Defendants' interception and storage of users' WhatsApp communications was contrary to its privacy promises;
- Whether Defendants can access the contents of users' WhatsApp communications;
- Whether Defendants used the contents of users' WhatsApp communications;
- Whether Plaintiffs and Class Members had a reasonable expectation of privacy in their WhatsApp communications;
- Whether Defendants' interception and storage of users' WhatsApp communications was highly offensive to a reasonable person;
- Whether Defendants' interception and storage of users' WhatsApp communications was unfair;
- Whether and to what extent Defendants were unjustly enriched through their unlawful conduct;
- Whether Plaintiffs and Class Members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

77. Predominance & Superiority (Rule 23(b)(3)): In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class Members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to individual Plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and court systems around the world. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

78. Injunctive Relief (Rule 23(b)(2)): Defendants have acted on grounds that apply generally to the Class as a whole, such that class certification, injunctive relief, and declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Wiretap Act: Unauthorized Interception of Electronic Communications 18 U.S.C. § 2510, *et seq.*

79. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

80. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. §§ 2510, 2511.

81. The Wiretap Act protects both the sending and receipt of communications.

82. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

83. Defendants intentionally intercepted the electronic communications of Plaintiffs and other WhatsApp users by intercepting their WhatsApp messages. On information and belief, Defendants are aware that they are intercepting WhatsApp messages and have taken no remedial action.

84. The transmission of WhatsApp messages between Plaintiffs and other WhatsApp users were "transfer[s] of signs, signals, writing, images, sounds, data, or intelligence . . . transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[,]" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

85. Defendants' interception of Plaintiffs' communications was done contemporaneously with the Plaintiffs' sending and receipt of those communications. On information and belief, Plaintiffs' and other WhatsApp users' WhatsApp messages were intercepted by Defendants essentially in real time, as soon as they were sent.

86. The intercepted communications include substantially all WhatsApp messages for substantially all WhatsApp users.

87. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' electronic devices on which the WhatsApp application was installed;

b. The WhatsApp application;

c. Defendants' web servers;

d. The computer code deployed by Defendants to effectuate their interception of Plaintiffs' and Class Members' WhatsApp messages.

88. Defendants are not parties to Plaintiffs' communications with other WhatsApp users.

89. Defendants received the "contents" of Plaintiffs' electronic communications with other WhatsApp users because they received the full text of Plaintiffs' WhatsApp messages, which constitute the "substance, purport or meaning of th[ose] communication[s]" within the meaning of 18 U.S.C. § 2510(8).

90. Defendants' interception of Plaintiffs' WhatsApp messages occurred in the United States.

91. Plaintiffs did not consent to Defendants' acquisition of the contents of their WhatsApp messages with other WhatsApp users. For example, WhatsApp expressly promised in its Privacy Policy that "[w]e offer end-to-end encryption for our Services[,]" which "means that your messages are encrypted to protect against us and third parties from reading them."[86] It also claimed on its website that "all your personal messages stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them."[87]

92. The surreptitious interception of Plaintiffs' WhatsApp messages was not done in the "ordinary course" of Defendants' business within the meaning of 18 U.S.C. § 2510(5)(a). As

[86] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

[87] WhatsApp, "Does WhatsApp collect or sell your data?", *available at* https://faq.whatsapp.com/2779769622225319/?helpref=hc_fnav (last accessed Jan. 19, 2026).

explained, this interception was directly contrary to Defendants' representations about their treatment of WhatsApp users' messages.

93. The surreptitious interception of Plaintiffs' WhatsApp messages was not done in the "normal course" of Defendants' officers', employees', or agents' employment, was not a "necessary incident to the rendition" of WhatsApp's electronic communications service, and was not done for the purpose of "mechanical or service quality control checks" within the meaning of 18 U.S.C. § 2511(2)(a)(i). Defendants' interceptions are contrary to their representations about their treatment of WhatsApp users' messages, are for their own benefit, and are unrelated to providing WhatsApp users with the ability to send and receive WhatsApp messages.

94. The surreptitious interception of Plaintiffs' WhatsApp messages was not done for "the protection of the rights or property" of Defendants within the meaning of 18 U.S.C. § 2511(2)(a)(i).

95. As a result of the above actions and pursuant to 18 U.S.C. § 2520(b), the Court may provide injunctive and declaratory relief; assess as damages the greater of the sum of the actual damages suffered by Plaintiffs and any profits made by Defendants as a result of the violation, or statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the future; and reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CAUSE OF ACTION

Violation of the California Comprehensive Computer Data Access and Fraud Act Cal. Penal Code § 502, *et seq.*

96. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

97. Cal. Penal Code § 502(j) provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

Smart phone devices with the capability of using web browsers are "computers" within the meaning of the statute.

98. Defendants violated Cal. Penal Code § 502(c)(1) by knowingly and without permission accessing and using Plaintiffs' and Class Members' private WhatsApp messages in order to execute a scheme to deceive or defraud consumers by claiming that Defendants cannot read and do not store users' WhatsApp messages, when in fact Defendants have intercepted and made copies of substantially all WhatsApp users' private messages.

99. Defendants violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, and using Plaintiffs' and the Class Members' private WhatsApp messages.

100. Defendants violated Cal. Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' computer systems and/or computer networks.

101. Defendants violated Cal. Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' computer systems and/or computer networks.

102. Pursuant to Cal. Penal Code § 502(b)(12) a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information."

103. Defendants violated Cal. Penal Code § 502(c)(8) by knowingly introducing a computer contaminant into Plaintiffs' and the Class Members' mobile devices; specifically, the code used in the WhatsApp application that Defendants deployed to effectuate their interception, copying, and storage of Plaintiffs' and the Class Members' WhatsApp messages.

104. Defendants accessed, copied, took, analyzed, and used data from Plaintiffs' and Class Members' computers in and from the State of California, where Defendants: (1) have their principal place of business; (2) used servers that provided communication links between Plaintiffs' and Class Members' computers and Defendants, which allowed Defendants to access and obtain

Plaintiffs' and Class Members' data; and (3) designed and contrived their scheme to deploy computer code to effectuate their interception of Plaintiffs' WhatsApp messages. Accordingly, Defendants caused the access of Plaintiffs' and Class Members' computers from California, and are therefore deemed to have accessed Plaintiffs' and Class Members' computers in California. In addition, Defendants have adopted California substantive law to govern their relationship with WhatsApp users.

105. As a direct and proximate result of Defendants' unlawful conduct under California Penal Code § 502, Defendants have caused loss to Plaintiffs and Class Members and have been unjustly enriched in an amount to be proven at trial. Despite Defendants' false representations to the contrary, Defendants effectively charged Plaintiffs, Class Members, and other consumers, and Defendants were unjustly enriched, by acquiring their sensitive, private, and valuable WhatsApp messages without permission and using them for Defendants' own commercial benefit.

106. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and declaratory or other equitable relief, pursuant to Cal. Penal Code § 502(e)(1).

107. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendants' violations were willful and, upon information and belief, Defendants are guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

108. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e)(2).

THIRD CAUSE OF ACTION

Violation of the California Invasion of Privacy Act Cal. Penal Code § 630, *et seq.*

109. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

110. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology 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.

Cal. Penal Code § 630.

111. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally 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 who willfully 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 who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

112. California Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

113. Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

114. Defendants have their principal place of business in California and designed and contrived their scheme to deploy computer code to effectuate their interception of Plaintiffs' WhatsApp messages in California. Defendants have adopted California substantive law to govern their relationship with WhatsApp users.

115. At all relevant times, Defendants' interception of the Plaintiffs' and Class Members' private WhatsApp messages was without authorization and consent from the Plaintiffs (and Class Members). The interceptions by Defendants in the aforementioned circumstances were unlawful and tortious.

116. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Defendants' scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. Plaintiffs' and Class Members' electronic devices on which the WhatsApp application was installed;

b. The WhatsApp application;

c. Defendants' web servers;

d. The computer code deployed by Defendants to effectuate their interception of Plaintiffs' and Class Members' WhatsApp messages.

117. Defendants tapped or made an unauthorized connection with Plaintiffs' and Class Members' telephones through Defendants' use of computer code within the WhatsApp application, which secretly intercepted Plaintiffs' and Class Members' private WhatsApp messages. The WhatsApp application requires that users enter a cellular telephone number in order to register to use the application.

118. Defendants' non-consensual interception of Plaintiffs' and Class Members' WhatsApp messages was designed to learn the contents of those communications, and occurred while Plaintiffs' and Class Members' communications were in transit. Plaintiffs' and Class Members' private WhatsApp messages were available for Defendants and their agents to read or review essentially in real time.

119. The data collected by Defendants constituted "confidential communications," as that term is used in Section 632, because Plaintiffs and Class Members had objectively reasonable expectations of privacy in their private WhatsApp messages. WhatsApp expressly promised in its Privacy Policy that "[w]e offer end-to-end encryption for our Services[,]" which "means that your messages are encrypted to protect against us and third parties from reading them."[88] It also claimed

[88] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

on its website that "all your personal messages stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them."[89]

120. Plaintiffs and Class Members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

121. Pursuant to California Penal Code § 637.2, Plaintiffs and Class Members have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 per violation or three times the amount of actual damages, as well as injunctive relief.

FOURTH CAUSE OF ACTION

Invasion of Privacy
Cal. Constitution, Article 1, Section 1

122. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

123. The right to privacy in California's Constitution creates a right of action against private entities such as Defendants.

124. Plaintiffs' and Class Members' expectation of privacy is deeply enshrined in California's Constitution. 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."

125. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone… It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control

[89] WhatsApp, "Does WhatsApp collect or sell your data?", *available at* https://faq.whatsapp.com/2779769622225319/?helpref=hc_fnav (last accessed Jan. 19, 2026).

> circulation of personal information. This is essential to social relationships and personal freedom.[90]

126. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendants.

127. To plead a California constitutional privacy claim, a plaintiff must show (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

128. As described herein, Defendants have intruded upon the following legally protected privacy interests:

a. The Federal Wiretap Act as alleged herein;

b. The California Invasion of Privacy Act as alleged herein;

c. The California Constitution, which guarantees the right to privacy;

d. WhatsApp's Privacy Policy and policies referenced therein and other public promises it made not to intercept or store the Plaintiffs' and Class Members' WhatsApp messages.

129. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class Members could not reasonably expect Defendants would commit acts in violation of federal and state civil and criminal laws; and WhatsApp affirmatively promised users (including Plaintiffs and Class Members) that their messages were end-to-end encrypted, which "means that your messages are encrypted to protect against us and third parties from reading them."[91] It also claimed on its website that "all your personal messages stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them."[92] WhatsApp's website also asserted that WhatsApp "does not store messages once they

---

[90] UC Law SF Scholarship Repository, 1972 "Right of Privacy" Ballot Proposition, *available at* https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props (last accessed Jan. 19, 2026).

[91] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

[92] WhatsApp, Does WhatsApp collect or sell your data?, *available at* https://faq.whatsapp.com/2779769622225319/?helpref=hc_fnav (last accessed Jan. 19, 2026).

are delivered" and that "undelivered messages are deleted from [its] servers after 30 days."[93] In reality, Defendants' intercepted substantially all WhatsApp users' private messages such that they were available for Defendants' review in real time, and stored those messages for an unlimited time.

130. Defendants' actions constituted a serious invasion of privacy in that they:

a. Invaded the privacy of billions of WhatsApp users worldwide (including Plaintiffs and Class Members) without their consent;

b. Violated federal and California state laws on wiretapping and invasion of privacy, as set forth herein;

c. Constituted the unauthorized taking of valuable information from billions of WhatsApp users worldwide through deceit; and

d. Further violated Plaintiffs' and Class Members' reasonable expectation of privacy via Defendants' storage, review, analysis, and subsequent uses of Plaintiffs' and Class Members' private messages that Plaintiffs and Class Members considered sensitive and confidential.

131. Committing criminal acts against billions of WhatsApp users worldwide constitutes an egregious breach of social norms that is highly offensive.

132. The surreptitious and unauthorized interception and storage of the private messages of billions of worldwide WhatsApp users, contrary to Defendants' express promises that the messages would not be stored or accessible to Defendants, constitutes an egregious breach of social norms that is highly offensive.

133. Defendants' intentional intrusion into Plaintiffs' and Class Members' private messages and cellular telephones was highly offensive to a reasonable person. Defendants are well aware that billions of users rely on their promises that WhatsApp messages are not stored or accessible to anyone, including Defendants themselves, and that these promises induce users to share their most sensitive and personal information on WhatsApp. Anyone who learned that

[93] WhatsApp, "Information for Law Enforcement Authorities," *available at* https://faq.whatsapp.com/444002211197967 (last accessed Jan. 19, 2026).

Defendants' promises are false, and that Defendants are in fact storing and accessing WhatsApp users' messages every day, would find Defendants' conduct highly offensive.

134. Secret monitoring of private messages is highly offensive behavior, especially given that Defendants expressly and falsely represent that no one—not even Defendants—can read users' messages.

135. Wiretapping and surreptitious recording of communications is highly offensive behavior.

136. Defendants lacked a legitimate business interest in intercepting and storing users' private messages without their consent and contrary to Defendants' privacy promises.

137. Plaintiffs and Class Members have been damaged by Defendants' invasion of their privacy and are entitled to just compensation and injunctive relief.

FIFTH CAUSE OF ACTION

Intrusion Upon Seclusion

138. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

139. To state a claim for intrusion upon seclusion in California, a plaintiff must plead that (1) the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy, and (2) the intrusion occurred in a manner highly offensive to a reasonable person.

140. In carrying out their scheme to intercept and store Plaintiffs' and Class Members' private WhatsApp messages in violation of their own privacy promises, Defendants intentionally intruded upon the Plaintiffs' and Class Members' solitude or seclusion in that they effectively placed themselves in the middle of private conversations to which they were not authorized parties.

141. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class Members could not reasonably expect Defendants would commit acts in violation of federal and state civil and criminal laws; and WhatsApp affirmatively promised users (including Plaintiffs and Class Members) that their messages were end-to-end encrypted, which "means that your messages are encrypted to protect against us and third parties

from reading them."[94] It also claimed on its website that "all your personal messages stay between you and who you send them to—no one else, not even WhatsApp (or Meta), can read, listen to, or share them."[95] WhatsApp's website also asserted that WhatsApp "does not store messages once they are delivered" and that "undelivered messages are deleted from [its] servers after 30 days."[96] In reality, Defendants' intercepted substantially all WhatsApp users' private messages such that they were available for Defendants' review in real time, and stored those messages for an unlimited time.

142. Defendants' interception and storage of Plaintiffs' and Class Members' WhatsApp messages was not authorized by the Plaintiffs and Class Members or the WhatsApp users with whom they were communicating.

143. The surreptitious and unauthorized interception and storage of the private messages of billions of worldwide WhatsApp users constitutes an egregious breach of social norms that is highly offensive.

144. Defendants' intentional intrusion into Plaintiffs' and Class Members' private messages and cellular telephones was highly offensive to a reasonable person. Defendants are well aware that billions of users rely on their promises that WhatsApp messages are not stored or accessible to anyone, including Defendants themselves, and that these promises induce users to share their most sensitive and personal information on WhatsApp. Anyone who learned that Defendants' promises are false, and that Defendants are in fact storing and accessing WhatsApp users' messages every day, would find Defendants' conduct highly offensive.

145. Secret monitoring of private messages is highly offensive behavior, especially given that Defendants expressly and falsely represent that no one—not even Defendants—can read users' messages.

146. Wiretapping and surreptitious recording of communications is highly offensive behavior.

---

[94] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

[95] WhatsApp, Does WhatsApp collect or sell your data?, *available at* https://faq.whatsapp.com/2779769622225319/?helpref=hc_fnav (last accessed Jan. 19, 2026).

[96] WhatsApp, "Information for Law Enforcement Authorities," *available at* https://faq.whatsapp.com/444002211197967 (last accessed Jan. 19, 2026).

147. Defendants lacked a legitimate business interest in intercepting and storing users' private messages without their consent.

148. Plaintiffs and the Class Members have been damaged by Defendants' invasion of their privacy and are entitled to reasonable compensation, including but not limited to disgorgement of profits related to the unlawful interception, use, and storage of their messages.

SIXTH CAUSE OF ACTION

Breach of Contract

149. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

150. Defendants' relationship with WhatsApp users is governed by the WhatsApp Terms of Service, which incorporates the WhatsApp Privacy Policy.

151. The WhatsApp Privacy Policy asserts that "[r]espect for your privacy is coded into our DNA. Since we started WhatsApp, we've built our services with a set of strong privacy principles in mind."[97] It promises 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."[98]

152. Defendants breached these promises; in fact, WhatsApp, Meta, and their agents have access to and can read substantially all users' private WhatsApp messages.

153. WhatsApp also promises in its Privacy Policy 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."[99]

154. Defendants breached these promises; in fact, Defendants stored substantially all users' private WhatsApp messages and could review them at any time.

155. Plaintiffs and Class Members performed their obligations under the relevant contracts and are not in breach of any such obligations.

---

[97] WhatsApp, "WhatsApp Privacy Policy" (effective Jan. 4, 2021), *available at* https://www.whatsapp.com/legal/privacy-policy (last accessed Jan. 19, 2026).

[98] *Id.*

[99] *Id.*

156. As a result of Defendants' breach(es), Defendants were able to obtain the personal property of Plaintiffs and Class Members and earn unjust profits.

157. Plaintiffs and Class Members also did not receive the benefit of the bargain for which they contracted and for which they provided valuable consideration in the form of their use of the WhatsApp app, which has ascertainable value to be proven at trial, including but not limited to its growth of the WhatsApp and broader Meta Companies user network.

158. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages, consequential damages, and/or non-restitutionary disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

SEVENTH CAUSE OF ACTION

Breach of the Implied Covenant of Good Faith and Fair Dealing

159. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

160. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement.

161. In dealings between Defendants and WhatsApp users, Defendants are invested with discretionary power affecting the rights of WhatsApp users.

162. Defendants purport to respect and protect WhatsApp users' privacy. For instance, the WhatsApp Privacy Policy asserts that "[r]espect for your privacy is coded into our DNA." Both the WhatsApp Privacy Policy and WhatsApp Terms of Service state that "[s]ince we started WhatsApp, we've built our services with a set of strong privacy principles in mind."

163. Despite Defendants' contractual privacy promises to keep WhatsApp users' messages end-to-end encrypted such that Defendants and third parties could not read them, and its promises not to store WhatsApp users' messages, Defendants took actions outside those contractual promises to deprive Plaintiffs and Class Members of the benefits of their contract with Defendants.

164. Defendants' interception, storage, and use of WhatsApp users' (including Plaintiffs' and Class Members') messages was objectively unreasonable given Defendants' privacy promises, and evaded the spirit of the bargain made between Defendants and Plaintiffs.

165. Defendants' conduct in this case abused their power to specify terms—in particular, Defendants failed to accurately disclose their interception, storage, and use of WhatsApp users' messages.

166. As a result of Defendants' misconduct and breach of their duty of good faith and fair dealing, Plaintiffs and Class Members suffered damages. Plaintiffs and Class Members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their use of the WhatsApp app, which, as alleged above, has ascertainable value to be proven at trial, including but not limited to its growth of the WhatsApp and broader Meta Companies user network.

EIGHTH CAUSE OF ACTION

Quasi-Contract (Restitution and Unjust Enrichment) (In Alternative to Contract Claims)

167. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

168. Defendants, intentionally and without consent or other legal justification, violated the privacy, property, and statutory rights of Plaintiffs, Class Members, and other WhatsApp users.

169. As a result of Defendants' tortious acts, Defendants received and unjustly retained a benefit at the expense of Plaintiffs, Class Members, and other WhatsApp users.

170. It would be unjust for Defendants to retain the value of the Plaintiffs' property and any profits earned thereon.

171. If Plaintiffs' contract claims fail, they have no adequate remedy at law to force the disgorgement of Defendants' unjustly earned profits. This count is therefore pled in the alternative to the contract claims.

NINTH CAUSE OF ACTION

Statutory Larceny Cal. Penal Code §§ 484 and 496

172. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

173. California Penal Code section 496(a) prohibits the obtaining of property "in any manner constituting theft."

174. California Penal Code section 484 defines theft, and provides:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall 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 money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

175. Section 484 thus defines "theft" to include obtaining property by false pretense.

176. Defendants intentionally designed a program that would operate in a manner unbeknownst to WhatsApp users, including Plaintiffs and Class Members, who were thus deceived into providing their personal information (private WhatsApp messages) to Defendants.

177. Defendants acted in a manner constituting theft and/or false pretense.

178. Defendants stole, took, and/or fraudulently appropriated Plaintiffs' and Class Members' personal information without Plaintiffs' and Class Members' consent.

179. Defendants concealed, aided in the concealing, and/or utilized Plaintiffs' and Class Members' personal information that was obtained by Defendants for Defendants' commercial purposes and the financial benefit of Defendants.

180. Defendants knew that Plaintiffs' and Class Members' personal information was stolen and/or obtained because Defendants designed the code that intercepted and stored Plaintiffs' and Class Members' private WhatsApp messages and operated it in a manner that was concealed and/or withheld from Plaintiffs.

181. The reasonable and fair market value of the unlawfully obtained personal data can be determined in the marketplace.

TENTH CAUSE OF ACTION

Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*

182. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

183. The California Unfair Competition Law prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal.

Bus. & Prof. Code § 17200 ("UCL"). By engaging in the practices aforementioned, Defendants have violated the UCL.

184. Defendants' "unlawful" acts and practices include their violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq*.; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq*.; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*.; Invasion of Privacy; Intrusion Upon Seclusion; Breach of Contract; Breach of the Implied Covenant of Good Faith and Fair Dealing; Quasi-Contract; Statutory Larceny, Cal. Penal Code §§ 484 and 496; and California Bus. & Prof. Code § 22576.

185. Defendants' conduct violated the spirit and letter of these laws, which protect property, economic, and privacy interests and prohibit unauthorized collection of private communications and personal information.

186. Defendants' "unfair" acts and practices include its violation of property, economic, and privacy interests protected by the statutes identified above. To establish liability under the unfair prong, Plaintiffs and Class Members need not establish that these statutes were actually violated, although the claims pleaded herein do so.

187. Defendants promised that Plaintiffs', Class Members', and other WhatsApp users' messages would be end-to-end encrypted such that they could not be read by Defendants or third parties, and that Defendants would not store those messages. Plaintiffs thus had no reason to know and could not have anticipated this intrusion into their privacy by Defendants' interception and storage of their WhatsApp messages. Defendants' conduct was immoral, unethical, oppressive, unscrupulous, and substantially injurious to Plaintiffs, Class Members, and other WhatsApp users. Further, Defendants' conduct narrowly benefitted their own business interests at the expense of Plaintiffs' and Class Members' fundamental privacy interests protected by the California Constitution and the common law.

188. Plaintiffs and Class Members have suffered injury-in-fact, including the loss of money and/or property as a result of Defendants' unfair and/or unlawful practices, to wit, the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use by Defendants. Plaintiffs and Class Members have suffered harm in the form of diminution

of the value of their private and personally identifiable data and content. Plaintiffs and Class Members have also suffered harm in the form of loss of the benefit of their bargain with Defendants.

189. Defendants' actions caused damage to and loss of Plaintiffs' and Class Members' property right to control the dissemination and use of their personal information and communications.

190. Defendants reaped unjust profits and revenues in violation of the UCL. Plaintiffs and Class Members seek restitution and disgorgement of these unjust profits and revenues.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an order:

1. certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as class counsel;

2. awarding damages, including nominal, statutory, and punitive damages where applicable, to Plaintiffs and the Class in an amount to be determined at trial;

3. awarding Plaintiffs and the Class reasonable attorneys' fees and costs of suit incurred herein;

4. awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

5. awarding such injunctive and declaratory relief as is necessary to protect the interests of Plaintiffs and the Class; and

6. awarding such other and further relief as the Court deems just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs hereby demand trial by jury of all issues properly triable thereby.

DATED: January 23, 2026

Respectfully submitted,

By */s/ Adam Wolfson*

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Adam Wolfson (Bar No. 262125)
adamwolfson@quinnemanuel.com
Stephen A. Broome (Bar No. 314605)
stephenbroome@quinnemanuel.com
Kevin Teruya (Bar No. 235916)
kevinteruya@quinnemanuel.com
Valerie Roddy (Bar No. 235163)
valerieroddy@quinnemanuel.com
Lauren B. Lindsay (Bar No. 280516)
laurenlindsay@quinnemanuel.com
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

KELLER POSTMAN, LLC
Warren Postman (Bar No. 330869)
wdp@kellerpostman.com
Ashley Keller (*pro hac vice forthcoming*)
ack@kellerpostman.com
J.J. Snidow (*pro hac vice forthcoming*)
jj.snidow@kellerpostman.com
1101 Connecticut Avenue, N.W., Suite 1100
Washington, D.C. 20036
Telephone: (833) 633-0118

BARNETT LEGAL, PLLC
Jay W. Barnett (*pro hac vice forthcoming*)
jay@barnettlegal.net
3404 NW 135th Street
Oklahoma City, OK 73120
Telephone: (405) 456-9343

Attorneys for Plaintiffs