

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

9 -and-

10 **KESSLER TOPAZ**
11 **MELTZER & CHECK, LLP**
12 Joseph H. Meltzer (*pro hac vice* forthcoming)
13 jmeltzer@ktmc.com
14 Melissa L Yeates (*pro hac vice* forthcoming)
15 myeates@ktmc.com
16 Tyler S. Graden (*pro hac vice* forthcoming)
17 tgraden@ktmc.com
18 Jordan E. Jacobson (Bar No. 302543)
19 jjacobson@ktmc.com
20 Daniel S. Dicce (*pro hac vice* forthcoming)
21 ddicce@ktmc.com
22 280 King of Prussia Road
23 Radnor, PA 19087
24 Telephone: (610) 667-7706
25 Facsimile: (610) 667-7056

26 *Counsel for Plaintiffs and the putative Classes*

27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

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

Plaintiffs,

v.

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

Defendants.

Case No. 26-cv-2615

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

I. INTRODUCTION..... 1

II. JURISDICTION AND VENUE..... 3

III. PARTIES..... 4

 A. Plaintiffs 4

 B. Defendants..... 5

IV. FACTUAL ALLEGATIONS..... 5

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

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

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

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

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

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

 G. Meta Consistently Fails to Protect Users’ Privacy 20

 H. Tolling 22

V. CLASS ACTION ALLEGATIONS..... 23

VI. CLAIMS FOR RELIEF..... 26

VII. PRAYER FOR RELIEF 50

VIII. DEMAND FOR JURY TRIAL..... 51

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

5 I. INTRODUCTION

6 1. As any reasonable user would, Plaintiffs trusted WhatsApp, a popular messaging
 7 service, to abide by its foundational, years-long promises to keep users’ messages private between
 8 senders and recipients. Since its inception in 2009, WhatsApp has consistently branded and marketed
 9 itself as a private and secure messaging service, explicitly stating that: “[w]ith end-to-end encryption
 10 on WhatsApp, your personal messages and calls are secured with a lock. **Only you and the person**
 11 **you’re talking to can read or listen to them**, and no one else, **not even WhatsApp.**”³ WhatsApp
 12 further markets its platform as allowing users to “[m]essage privately.”⁴ And, reinforcing its supposed
 13 commitment to private messaging, WhatsApp also tells users: “[y]our privacy is our priority. With
 14 end-to-end encryption on WhatsApp, your personal messages, photos, calls and more stay between
 15 you and the people you choose, meaning not even WhatsApp can see them.”⁵

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

21
 22 ¹ Meta, WhatsApp, and the Accenture Defendants are collectively referred to herein as “Defendants.”

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

25 ³ WhatsApp, <https://www.whatsapp.com/> (last visited Mar. 24, 2026).

26 ⁴ *Id.*

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

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

1 testified, “we do not see any of the content in WhatsApp; it is fully encrypted . . . Facebook systems
2 do not see the content of messages being transferred over WhatsApp.”⁷

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



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

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

22 5. Notwithstanding Plaintiffs’ and other WhatsApp users’ reasonable expectation that
23 their messages sent on the WhatsApp platform would not be viewed by, shared, seen, or stored by
24 individuals who were not intended recipients of the messages, in truth, WhatsApp and its parent
25 company Meta secretly intercept, read, store, access, and/or view the supposedly private messages
26

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

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

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

11 7. WhatsApp's secret interception, reading, storing, accessing, and/or viewing of the
12 messages it ensured Plaintiffs and similarly situated Class members were private, including without
13 adequate disclosure to Plaintiffs and Class members, constitutes a serious invasion of Plaintiffs' and
14 Class members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510,
15 *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; the Pennsylvania
16 Wiretapping and Electronic Surveillance Act, 18 Pa. Cons. Stat. §§ 5701 *et. seq*; the California
17 Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.*; the Stored
18 Communications Act, 18 U.S.C. §§ 2701, *et seq.*; the California Constitution, Art. 1, § 1; common
19 law intrusion upon seclusion; breach of express and implied contract; Statutory Larceny Through
20 False Pretenses, Cal. Penal Code §§ 484, 496; the California Unfair Competition Law, Cal. Bus. &
21 Prof. Code § 17200, *et seq*; and the California False Advertising Law, Cal. Bus. & Prof. Code §
22 17500, *et seq.*

23 **II. JURISDICTION AND VENUE**

24 8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C.
25 § 1331 because this suit is brought under the laws of the United States, specifically the Electronic

26 ⁸ Jake Bleiberg, *US Has Investigated Claims WhatsApp Chats Aren't Private*, Bloomberg (Jan. 29,
27 2026, 17:22 ET), <https://www.bloomberg.com/news/articles/2026-01-29/us-has-investigated-claims-that-whatsapp-chats-aren-t-private>.

28 ⁹ *Id.*

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

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

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

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

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

18 **III. PARTIES**

19 **A. Plaintiffs**

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

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

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

27 16. Plaintiff Nida Samson is a citizen of Pennsylvania and resides in Media, Pennsylvania.
28

1 17. Plaintiff Samson downloaded the WhatsApp mobile application in or about March
2 2018 and created a WhatsApp account contemporaneously.

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

6 **B. Defendants**

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

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

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

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

25 **IV. FACTUAL ALLEGATIONS**

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

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

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

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

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

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

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

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

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

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

27 _____
28 ¹⁰ *How to get started on WhatsApp Messenger*, WhatsApp, <https://www.whatsapp.com/coronavirus/get-started> (last visited Mar. 24, 2026).

1 31. WhatsApp’s Terms of Service begin with a clause detailing “Privacy and Security
2 Principles” which asserts: “Since we started WhatsApp, we’ve built our Services with strong privacy
3 and security principles in mind.”¹¹

4 32. The WhatsApp Terms of Service also state that the “laws of the State of California
5 govern our Terms, as well as any Disputes . . . in court.”¹²

6 33. WhatsApp’s Privacy Policy states that: “We do not retain your messages in the
7 ordinary course of providing our Services to you. Instead, your messages are stored on your device
8 and not typically stored on our servers. Once your messages are delivered, they are deleted from our
9 servers.”¹³

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

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

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

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

21 37. From its inception, WhatsApp has held itself out to users as a secure platform where
22 users can send entirely private messages. Indeed, a 2009 blog post by WhatsApp co-founder Jan
23 Koum stated: “We have not, we do not and we will not ever sell your personal information to anyone.
24

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

26 ¹² *Id.*

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

28 ¹⁴ *Id.*

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

3 38. When Meta acquired WhatsApp in 2014, the companies’ co-founders publicly
4 disclaimed concerns that this acquisition would compromise WhatsApp’s commitment to privacy
5 with Mr. Koum again writing a blog post regarding WhatsApp’s supposed continued focus on
6 privacy. Mr. Koum stated: “[r]espect for your privacy is coded into our DNA, and we built WhatsApp
7 around the goal of knowing as little about you as possible.”¹⁷ Mr. Koum emphasized that WhatsApp
8 had historically not collected private information and said “we really have no plans to change that”¹⁸
9 and “[i]f partnering with Facebook meant that we had to change our values, we wouldn’t have done
10 it.”¹⁹ Mr. Koum then concluded, “[o]ur focus remains on delivering the promise of WhatsApp far and
11 wide, so that people around the world have the freedom to speak their mind without fear.”²⁰

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

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

20
21 _____
22 ¹⁵ *Just wanted to say a few things*, WhatsApp Blog, (Nov. 19, 2009), <https://blog.whatsapp.com/just-wanted-to-say-a-few-things>.

23 ¹⁶ *Why we don’t sell ads*, WhatsApp Blog, (June 18, 2012), <https://blog.whatsapp.com/why-we-don-t-sell-ads>.

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

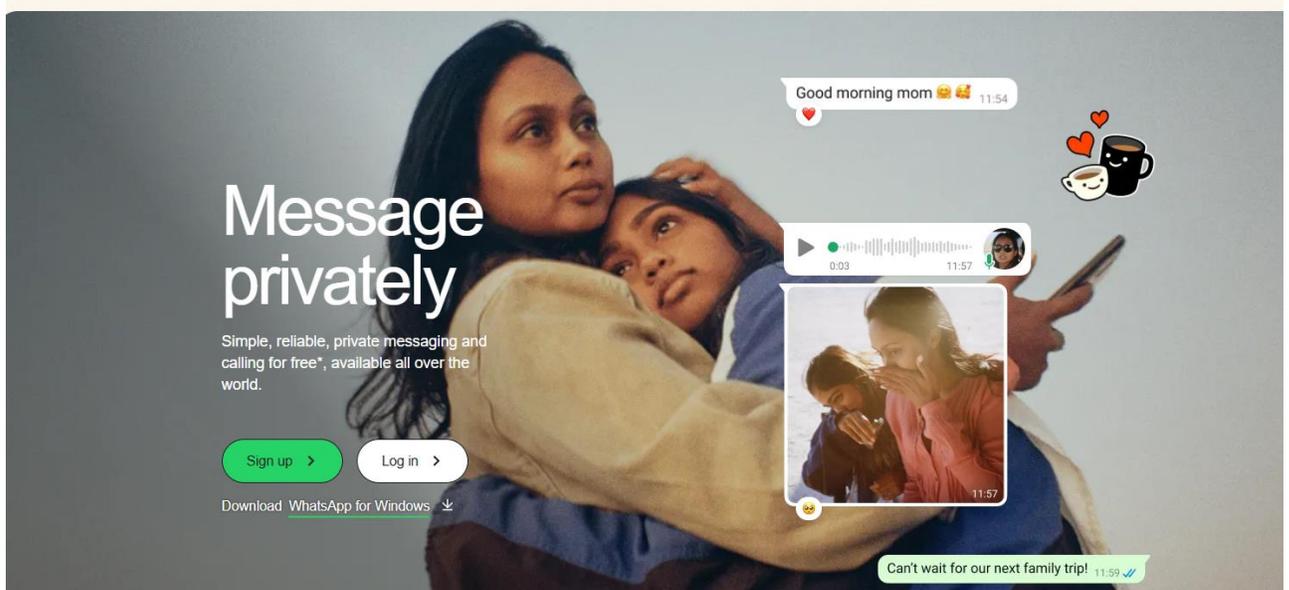
25 ¹⁸ *Id.*

26 ¹⁹ *Id.*

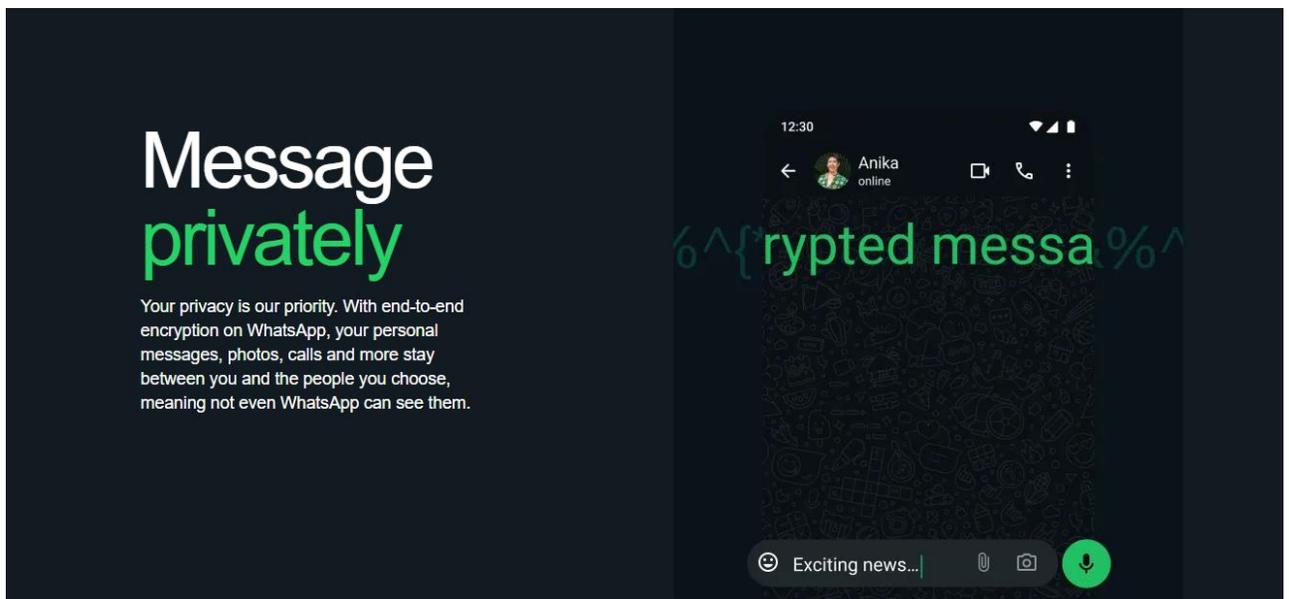
27 ²⁰ *Id.*

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

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



13 42. Moreover, the “Privacy” page on WhatsApp’s website, which is listed second only
14 following the websites’ “Features” section, states “[y]our privacy is our priority. With end-to-end
15 encryption on WhatsApp, your personal messages, photos, calls and more stay between you and the
16 people you choose, meaning not even WhatsApp can see them.”²³



27 ²² WhatsApp, <https://www.whatsapp.com/> (last visited Mar. 24, 2026).

28 ²³ Privacy, WhatsApp, <https://www.whatsapp.com/privacy> (last visited Mar. 24, 2026).

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



44. WhatsApp also makes assurances of privacy on its “Help Center” page which includes a “Safety and Security” section stating: “Your privacy and security are important to us, which is why we built end-to-end encryption into our app.”²⁴ The Help Center also includes a page “[a]bout end-to-end encryption” which asserts: “End-to-end encryption keeps your personal messages and calls between you and the person you’re communicating with. No one outside of the chat, not even WhatsApp, can read, listen to, or share them.”²⁵

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

About end-to-end encryption

[Copy link](#)

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

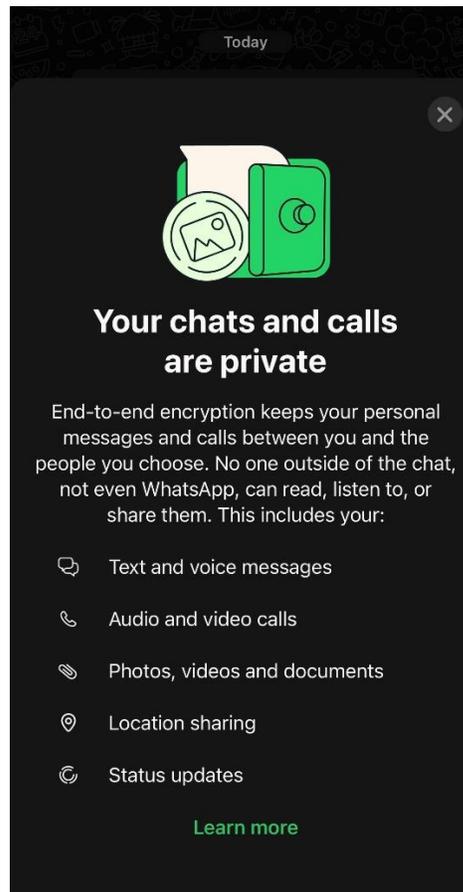
How does WhatsApp work?

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

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



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



5
6
7
8
9
10
11 **D. Unbeknownst to Plaintiffs and Other Users, WhatsApp, Meta, Their
12 Employees, and Third-Party Contractors, Including those Employed by
13 Accenture, Have Access to Users’ Communications**

14 47. End-to-end encryption is a means of securing digital communications whereby data is
15 encrypted on a sender’s device and is only decrypted once it reaches the recipient’s device. The use
16 of this method of transmission, in theory, means that while a sender’s encrypted communication may
17 pass through a service provider’s servers on way to the intended recipient, the communication is
18 unreadable to everyone but the intended recipient because only the sender and recipient have the
19 necessary “key” to unlock the communication on their respective devices.
20
21
22
23
24
25
26
27
28

1 48. After Meta acquired WhatsApp in 2014, WhatsApp partnered with Open Whisper
2 Systems to integrate the Signal Protocol, which is an end-to-end encryption cryptographic protocol,
3 into the WhatsApp platform.²⁶ The integration of the Signal Protocol onto the WhatsApp platform
4 was completed by April 5, 2016.²⁷

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

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

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

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

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

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

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

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

22
23 ²⁸ Jyoti Panday, *Encryption Under Siege in India: National Security & the Erosion of Digital Privacy*,
24 Internet Governance Project (Oct. 20, 2024), [https://www.internetgovernance.org/2024/10/20/
encryption-under-siege-in-india-national-security-the-erosion-of-digital-privacy/](https://www.internetgovernance.org/2024/10/20/encryption-under-siege-in-india-national-security-the-erosion-of-digital-privacy/).

25 ²⁹ *Id.*

26 ³⁰ *Id.*

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

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

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

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

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

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

25 58. Recent reporting has confirmed that WhatsApp's numerous promises that no one other
26 than intended recipients has access to users' communications is false. Indeed, contrary to WhatsApp's
27
28

1 repeated assurances otherwise, Meta, WhatsApp, their employees, contractors, and/or third-parties’
2 personnel have access to users’ WhatsApp messages.³²

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

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

13 61. Moreover, these whistleblowers have “outlined much broader access” by Meta
14 employees and third-party contractors than the limited access described in WhatsApp’s Privacy
15 Policy and website.³⁶

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

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

22 ³² *E.g.*, Jake Bleiberg, *US Has Investigated Claims WhatsApp Chats Aren’t Private*, Bloomberg (Jan.
23 29, 2026, at 16:22 ET), <https://www.bloomberg.com/news/articles/2026-01-29/us-has-investigated-claims-that-whatsapp-chats-aren-t-private>.

24 ³³ *Id.*

25 ³⁴ *Id.*

26 ³⁵ *Id.*

27 ³⁶ *Id.*

27 ³⁷ *Id.*

28 ³⁸ *Id.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28 ⁴³ *Id.*

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

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

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

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

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

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

- 21 a. Defendants' common law obligations to not intrude on private
22 communications;
- 23 b. State and federal laws and regulations protecting the confidentiality of
24 communications and computer data;
- 25 c. Defendants' express promises of privacy; and

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

1 d. Defendants' implied promises of privacy.

2 **G. Meta Consistently Fails to Protect Users' Privacy**

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

5 79. This history dates back to, at least, November 29, 2011, when Facebook entered into
6 a 20-year consent order with the United States Federal Trade Commission ("FTC") to settle the FTC's
7 eight-count complaint alleging that Facebook "deceived consumers by telling them they could keep
8 their information on Facebook private, and then repeatedly allowing [that information] to be shared
9 and made public."⁴⁵

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

14 81. This renewed FTC investigation eventually led to the FTC announcing a historic \$5
15 billion penalty against Facebook for violations of the 2012 consent order, which was "the largest ever
16 imposed on any company for violating consumers' privacy and almost 20 times greater than the
17 largest privacy or data security penalty ever imposed worldwide" and "one of the largest penalties
18 ever assessed by the U.S. government for any violation."⁴⁷ Notably, even though Facebook had
19 entered into the 2012 consent order, in the intervening years, Facebook nonetheless "repeatedly used
20

21
22 ⁴⁵ Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers By Failing To
23 Keep Privacy Promises (Nov. 29, 2011), [https://www.ftc.gov/news-events/news/press-releases/
24 2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises](https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises);
25 Agreement Containing Consent Order, *In the Matter of Facebook, Inc.*, No. 092 3184, (FTC Nov. 11,
26 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>.

⁴⁶ Tony Romm and Craig Timberg, *FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information*, Washington Post (Mar. 20, 2018, at 11:50 ET), <https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/>.

⁴⁷ Press Release, FTC, FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook: FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency" (July 24, 2019), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>.

1 deceptive disclosures and settings to undermine users’ privacy preferences” and “share[d] users’
2 personal information with third party-apps that were downloaded by the user’s Facebook ‘friends.’”⁴⁸

3 82. Then, in May 2023, the FTC alleged that Meta “misled parents about their ability to
4 control with whom their children communicated through its Messenger Kids app” and
5 “misrepresented the access it provided some app developers to private user data.”⁴⁹

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

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

12 85. Yet, even as Meta continually comes under scrutiny from regulators for failing to
13 protect user privacy, Meta has chosen to downsize its internal departments tasked with safeguarding
14 user information in what employees described as “as a ‘gutting’ of the workers in the department who
15 review projects at Meta for privacy and integrity risks.”⁵¹

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

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

21
22 ⁴⁹ Press Release, FTC, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing
23 Youth Data: FTC says that the company violated 2020 privacy order; proposes new protections for
children and teens (May 3, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data>.

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

28 ⁵¹ Mike Isaac and Eli Tan, *Meta Layoffs Included Employees Who Monitored Risks to User Privacy*,
N.Y. Times (Oct. 23, 2025), <https://www.nytimes.com/2025/10/23/technology/meta-layoffs-user-privacy.html>.

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

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

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

10 **H. Tolling**

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

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

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

19
20 ⁵² Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for*
21 *Teen Girls, Company Documents Show*, Wall St. J. (Sep. 14, 2021, at 7:59 ET),
22 [https://www.wsj.com/tech/personal-tech/facebook-knows-instagram-is-toxic-for-teen-girls-](https://www.wsj.com/tech/personal-tech/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739)
company-documents-show-11631620739; Vanessa Romo, *Whistleblower’s testimony has resurfaced*
23 *Facebook’s Instagram problem*, NPR (Oct. 5, 2021, at 18:00 ET),
24 <https://www.npr.org/2021/10/05/1043194385/whistleblowerstestimony-facebook-instagram>; J.
Wakefield, *Facebook under fire over secret teen research*, BBC (Sep. 15, 2021),
<https://www.bbc.com/news/technology-58570353>.

25 ⁵³ Press Release, Dick Durbin, Senator, Durbin, Blumenthal, Bipartisan Group of Senators Demand
26 Documents from Mark Zuckerberg After Newly Unsealed Court Filing Alleges Meta Hid Evidence
27 of Harms to Kids: Newly unsealed disclosures suggest Meta executives’ direct knowledge of the
28 harms of its product & concealment from Congress and the public, supporting whistleblower Arturo
Béjar’s testimony to the Senate Judiciary Committee (Nov. 15, 2023),
[https://www.durbin.senate.gov/newsroom/press-releases/durbin-blumenthal-bipartisan-group-of-](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)
senators-demand-documents-from-mark-zuckerberg-after-newly-unsealed-court-filing-alleges-
meta-hid-evidence-of-harms-to-kids.

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

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

5 **V. CLASS ACTION ALLEGATIONS**

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

8 **Nationwide Class:** All WhatsApp users residing in the United States who, between
9 April 5, 2016 and the present, sent or received communications via the WhatsApp
platform.

10 **California Sub-Class:** All WhatsApp users residing in the State of California who,
11 between April 5, 2016 and the present, sent or received communications via the
WhatsApp platform.

12 **Pennsylvania Sub-Class:** All WhatsApp users residing in the Commonwealth of
13 Pennsylvania who, between April 5, 2016 and the present, sent or received
communications via the WhatsApp platform.

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

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

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

- 26 a. Whether the Meta and WhatsApp Defendants' acts and practices violated the Electronic
27 Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;
- 28 b. Whether Defendants' acts and practices violated the California Invasion of Privacy Act,
Cal. Penal Code §§ 630, *et seq.*;

- c. Whether the Meta and WhatsApp Defendants' acts and practices violated Pennsylvania's Wiretapping and Electronic Surveillance Act, Pa. Cons. Stat. §§ 5701 *et seq.*;
- d. Whether the Meta and WhatsApp Defendants' acts and practices violated 18 U.S.C. §§ 2701, *et seq.*
- e. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;
- f. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Constitution, art. 1, § 1;
- g. Whether the Meta and WhatsApp Defendants' acts and practices constitute Statutory Larceny, Cal. Penal Code §§ 484, 496;
- h. Whether the Meta and WhatsApp Defendants' acts and practices violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*
- i. Whether the Meta and WhatsApp Defendants' acts and practices violated California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq.*
- j. Whether Defendants' acts and practices violate Plaintiffs' and Class members' common law privacy rights;
- k. Whether the Meta and WhatsApp Defendants breached an express contract;
- l. Whether the Meta and WhatsApp Defendants breached an implied contract; and
- m. Whether damages, restitution, injunctive, equitable, compulsory, or other relief is warranted.

98. Plaintiffs' claims are typical of the claims of the Class that Plaintiffs seeks to represent.

As alleged herein, Plaintiffs and the Class sustained damages arising out of the same unlawful actions and conduct by Defendants.

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

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

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

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

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

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

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

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

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

1 **VI. CLAIMS FOR RELIEF**

2 **COUNT I**

3 **Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.***

4 **On Behalf of the Nationwide Class**

5 **(Against the Meta and WhatsApp Defendants)**

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

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

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

13 111. The ECPA confers a civil cause of action on “any person whose wire, oral, or
14 electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.”
15 18 U.S.C. § 2520(a).

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

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

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

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

1 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”
2 18 U.S.C. § 2510(12).

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

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

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

9 119. Defendants intercept the “contents” of Plaintiffs’ and the Nationwide Class members’
10 communications where they acquire the text or other substance of a communication sent by a user on
11 the WhatsApp platform.

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

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

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

26
27 ⁵⁴ *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), <https://www.whatsapp.com/legal/privacy-policy>.

28 ⁵⁵ *Id.*

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

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

9 125. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Nationwide Class members have been
10 damaged by the interception of their communications in violation of the ECPA and are entitled to:
11 (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial,
12 assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and
13 any profits made as a result of the violation, or (b) statutory damages of whichever is the greater of
14 \$100 per day per violation or \$10,000; and (3) reasonable attorneys’ fees and other litigation costs
15 reasonably incurred.

16 **COUNT II**

17 **Violation of the California Invasion of Privacy Act**

18 **Cal. Penal Code §§ 630, *et. seq.***

19 **On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class**
20 **(Against All Defendants)**

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

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

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

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

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

10 [i] [I]ntentionally taps, or makes any unauthorized connection, whether physically,
11 electrically, acoustically, inductively or otherwise, with any telegraph or telephone
12 wire, line, cable, or instrument, including the wire, line, cable, or instrument of any
13 internal telephonic communication system,

14 Or

15 [ii] [W]illfully and without the consent of all parties to the communication, or in
16 any unauthorized manner, reads, or attempts to read, or to learn the contents or
17 meaning of any message, report, or communication while the same is in transit or
18 passing over any wire, line, or cable, or is being sent from, or received at any place
19 within this state,

20 Or

21 [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to
22 communicate in any way, any information so obtained,

23 Or

24 [iv] [A]ids, agrees with, employs, or conspires with any person or persons to
25 unlawfully do, or permit, or cause to be done any of the acts or things mentioned
26 above in this section.

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

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

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

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

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

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

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

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

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

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

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

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

3 141. Plaintiffs and the Class members seek statutory damages in accordance with §
4 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of
5 damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive
6 or other equitable relief.

7 **COUNT III**

8 **Pennsylvania Wiretapping and Electronic Surveillance Act**

9 **On Behalf of the Pennsylvania Sub-Class**

10 **18 Pa. Cons. Stat. §§ 5701 *et. seq.***

11 **(Against the Meta and WhatsApp Defendants)**

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

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

16 144. The Pennsylvania Wiretap Act prohibits: (1) the interception or endeavoring to
17 intercept any wire, electronic or oral communication; and (2) the intentional disclosure of the contents
18 of any wire, electronic, or oral communication that the discloser knew or should have known was
19 obtained through the interception of a wire, electronic or oral communication. 18 Pa. Cons. Stat. §
20 5703(1)-(2).

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

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

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

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

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

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

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

18 **COUNT IV**

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

21 **On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class**
22 **(Against the Meta and WhatsApp Defendants)**

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

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

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

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

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

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

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

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

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

COUNT V

Violations of the Stored Communications Act (“SCA”)

18 U.S.C. §§ 2701, *et seq.*

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

(Against the Meta and WhatsApp Defendants)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT VI

**Invasion of Privacy in Violation of the California Constitution, Art. 1, § 1
On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class
(Against All the Meta and WhatsApp Defendants)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 _____
28 ⁵⁶ *WhatsApp Privacy Policy*, WhatsApp, (effective Jan. 4, 2021), <https://www.whatsapp.com/legal/privacy-policy>.

COUNT VII

**Common Law Invasion of Privacy — Intrusion Upon Seclusion
On Behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class and
Pennsylvania Sub-Class
(Against All Defendants)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18 **COUNT VIII**

Breach of Express Contract

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

21 **(Against the Meta and WhatsApp Defendants)**

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

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

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

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

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

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

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

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

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

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

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

23 **Consent**

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

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

1 **Consideration**

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

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

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

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

17 **Performance**

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

19 **The Meta and WhatsApp Defendants Breached the Express Contract**

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

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

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

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

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

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

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

7 **COUNT IX**

8 **Breach of Implied Contract**

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

11 **(Against the Meta and WhatsApp Defendants)**

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

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

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

24 **Mutual Assent**

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

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

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

6 **Consideration**

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

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

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

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

23 **Performance**

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

25 **The Meta and WhatsApp Defendants’ Breach of the Implied Contract**

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

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

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

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

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

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

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

23 247. Pursuant to Cal. Penal Code § 496(c), Plaintiffs and the Class have been injured by a
24 violation of § 496(a), and are entitled to: (1) treble damages; (2) attorneys’ fees reasonably incurred;
25 and (3) costs of suit.
26
27
28

COUNT XI

**Violations of Cal. Bus. & Prof. Code § 17200, et seq.
Unlawful, Unfair, and Fraudulent Business Practices
On Behalf of Plaintiffs Individually
(Against the Meta and WhatsApp Defendants)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 **COUNT XII**

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

8 **False or Misleading Representations**

9 **On Behalf of Plaintiffs Individually**

10 **(Against the Meta and WhatsApp Defendants)**

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

13 265. Plaintiffs bring this claim individually.

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

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

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

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

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

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

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

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

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

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

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

21 **VII. PRAYER FOR RELIEF**

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

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

- 1 b. An order issuing a public injunction enjoining the Meta and WhatsApp Defendants
2 from continuing the unlawful, deceptive, fraudulent, and unfair business practices
3 alleged in this Complaint, by making untrue, false, deceptive, and/or misleading
4 statements in connection with WhatsApp’s Privacy Policy and other public facing
5 advertisements informing users that WhatsApp does not and cannot intercept, read,
6 store, access, and/or view WhatsApp users’ communications with other users while,
7 in truth, engaging in such conduct;
- 8 c. A declaration that Defendants are financially responsible for all Class notice and the
9 administration of Class relief;
- 10 d. An order awarding costs, restitution, disgorgement, punitive damages, statutory
11 damages, treble damages, and exemplary damages under applicable law, and
12 compensatory damages for economic loss, and out-of-pocket costs in an amount to be
13 determined at trial;
- 14 e. An order requiring Defendants to pay both pre- and post-judgment interest on any
15 amounts awarded;
- 16 f. An award of costs, expenses, and attorneys’ fees as permitted by law; and
- 17 g. Such other or further relief as the Court may deem appropriate, just, and equitable.

18 **VIII. DEMAND FOR JURY TRIAL**

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

21
22 DATED: March 25, 2026

Respectfully submitted,

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

-and-

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

Counsel for Plaintiffs and the Putative Classes