

1 Adam E. Polk (SBN 273000)
2 Simon S. Grille (SBN 294914)
3 Kimberly Macey (SBN 342019)
4 Reid Gaa (SBN 330141)
5 **GIRARD SHARP LLP**
6 601 California Street, Suite 1400
7 San Francisco, CA 94108
8 Telephone: (415) 981-4800
9 apolk@girardsharp.com
10 sgrille@girardsharp.com
11 kmacey@girardsharp.com
12 rgaa@girardsharp.com

13 *Attorneys for Plaintiffs*

John J. Nelson (SBN 317598)
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@milberg.com

Gary M. Klinger (*pro hac vice* forthcoming)
Alexandra M. Honeycutt (*pro hac vice* forthcoming)
Nick Suciu (*pro hac vice* forthcoming)
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
ahoneycutt@milberg.com
nsuciu@milberg.com

14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**

16
17
18 In re Meta Browser Tracking Litigation

Case No. 4:22-cv-05267-JST

JURY DEMAND

**CONSOLIDATED CLASS ACTION
COMPLAINT**

1 Plaintiffs Gabriele Willis, Shelby Cooper, Rama Kolesnikow, Lisa Bush, David Alzate, Mark
2 Letoski, Louis Green, Ed Rennie, Teia Pittman, Raven Johnson, Chanel Robinson, Kevin Zenstein, Mary
3 Thew, and Lisa Evans, on behalf of the Class and Subclasses defined below, bring this action against
4 Meta Platforms, Inc. (“Meta”) and allege as follows:

5 **NATURE OF THE ACTION**

6 1. Plaintiffs are Facebook users whose online activity Meta surreptitiously tracked without
7 their knowledge or consent. Plaintiffs bring this action on behalf of themselves and other Facebook users
8 to recover damages for—and put a stop to—the conduct in question.

9 2. Meta owns and operates Facebook, one of the world’s largest social media platforms,
10 which Plaintiffs and Class Members use. Meta tracked their web-browsing activity on their iPhones and
11 iPads (“Apple Devices”), even on websites displaying or requiring the disclosure of financial and health
12 information, in granular detail, down to the keystroke. No Plaintiff consented to Meta monitoring and
13 profiting from their private browsing activity, messages, and other information they communicated
14 online. Even though each Plaintiff chose *not* to be tracked—and Meta knew of this preference—it
15 nonetheless tracked their activity on and across third-party websites.

16 3. Meta’s lucrative mobile advertising business relies on tracking people through their
17 personal devices and building comprehensive profiles that advertisers use to precisely target desired
18 individuals or demographics with algorithmically placed ads. Meta’s enormous user base and possession
19 of data regarding their online activity has enabled it to reap billions in digital advertising revenue for
20 years.

21 4. Beginning in April 2021, in a change that Apple Inc. touted as protecting user privacy,
22 Apple updated its operating systems for iPhones (“iOS”) and iPads (“iPadOS”).¹ The update required
23 app developers, like Meta, to obtain users’ express consent before tracking their activity on third-party
24 websites for the purposes of advertising or sharing the information with data brokers. Apple presented
25 the choice through a pop-up window asking users if they wanted to opt in to being tracked across other
26 companies’ websites. Unsurprisingly, the overwhelming majority of users chose not to be tracked.

27

¹ As used in this Complaint, iOS means both iOS and iPadOS; the latter is the operating system for Apple
28 iPad devices, and is identical to iOS in all respects material to this Complaint.

1 Almost overnight, Meta lost access to a key source of data derived from observing Apple Device users
2 while they accessed third-party websites and communicated information, including sensitive financial,
3 health, and other private information, by typing into search boxes, forms, and other fields. With its user
4 tracking ability neutralized, Meta lost billions of dollars in potential advertising revenue.

5 5. Confronted with the imperative to regain this data and lost revenue, Meta devised a
6 technical workaround allowing it to track its users' activity and communications on third-party websites
7 opened via the Facebook app, even where users expressed their preference not to be tracked on their
8 Apple Device. When a person using the Facebook app clicks on a link to an ostensibly external third-
9 party website, Meta causes the link to be opened in an in-app browser—i.e., on Facebook's own
10 platform—instead of the smartphone's default browser. Meta never tells users they are being tracked
11 through an in-app browser.

12 6. Meta's surveilling of citizens' private communications and other confidential browsing
13 activity, contrary to their stated preference, violates federal and state privacy and other laws. Plaintiffs
14 and Class Members seek appropriate damages or restitution as well as injunctive relief to halt Meta's
15 undisclosed tracking of Apple users who did not wish to be tracked.

16 **JURISDICTION, VENUE AND CHOICE OF LAW**

17 7. The Court has personal jurisdiction over Meta because it is headquartered in this District.

18 8. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs'
19 claims arise in part under federal law: the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Computer Fraud
20 and Abuse Act, 18 U.S.C. § 1030 *et seq.* The Court also has subject matter jurisdiction under 28 U.S.C.
21 § 1332(d) because there are more than 100 Class Members, the amount in controversy exceeds \$5 million
22 (excluding interest and costs), and at least one Class Member is a citizen of a state different from Meta's
23 state of domicile. The Court has supplemental jurisdiction over Plaintiffs' state-law claims under 28
24 U.S.C. § 1367.

25 9. Venue is proper under 28 U.S.C. § 1391 because Meta is headquartered in his District.

26 10. There is a significant aggregation of contacts between Meta's conduct and California.
27 Meta is headquartered and does substantial business in California. Further, a significant percentage of
28 Class Members are located in, and Meta aimed a significant portion of its illicit conduct at, California.

1 The conduct that forms the basis for each Class Member’s claims against Meta emanated from its
2 headquarters in Menlo Park, California. Numerous communications that Meta illegally intercepted were
3 between Class Members and third-party websites controlled and maintained and with servers based in
4 California. Moreover, Meta devised and executed its wrongful conduct, wrote the software code at issue,
5 planned its communications with Class Members, and set its relevant policies and practices at its Menlo
6 Park headquarters. California thus has a greater interest than any other state in applying its law to the
7 claims in this case.

8 11. California has a very strong interest in preventing its resident corporations, such as Meta,
9 from deceiving and invading the privacy of consumers and in ensuring that the harm inflicted on such
10 consumers is adequately redressed. California’s interest in preventing unlawful corporate behavior
11 occurring in California substantially outweighs any interest of any other state in denying recovery to its
12 residents injured by an out-of-state defendant or in applying its laws to business decisions and practices
13 occurring outside its borders. If other states’ laws were applied to Class Members’ claims, California’s
14 strong interest in deterring resident corporations from committing unfair or deceptive trade practices
15 would be significantly impaired.

16 **DIVISIONAL ASSIGNMENT**

17 12. Pursuant to Civil Local Rule 3-2(c), a substantial part of the events giving rise to the claims
18 brought in this Complaint occurred in San Mateo County, California. Consequently, assignment of this
19 action to San Francisco or Oakland Division is appropriate.

20 **PARTIES**

21 **Gabriele Willis**

22 13. Plaintiff Gabriele Willis is an adult citizen of the state of California who resides in El
23 Cajon, California. Ms. Willis has had an active Facebook account since approximately 2007. She has
24 used her iPhone to access the Facebook app since approximately 2008. Her device has run on iOS version
25 14.5 or later since approximately May 2021.

26 14. Ms. Willis did not consent to Facebook tracking her activity. She configured the settings
27 on her iPhone to not allow the Facebook app to track her.
28

1 iPhone to access the Facebook app since 2012. His device has run on iOS version 14.5 or later since April
2 2021.

3 26. Mr. Alzate did not consent to Facebook tracking his activity. He configured the settings
4 on his iPhone to not allow the Facebook app to track him.

5 27. Using the systematic process described below, Meta tracked and intercepted Mr. Alzate's
6 specific electronic activity and private communications with third-party websites opened within
7 Facebook's in-app browser without his knowledge or consent. Mr. Alzate reasonably expected that his
8 communications with third-party websites were confidential, solely between himself and those websites,
9 and that such communications—which include text entries, passwords, personally identifiable
10 information, and other sensitive, confidential and private information—would not be intercepted or
11 tracked by Meta.
12

13 **Mark Letoski**

14 28. Plaintiff Mark Letoski is an adult citizen of the state of Illinois who resides in Chicago,
15 Illinois. Mr. Letoski has had an active Facebook account since approximately December 2005. He has
16 used his iPhone to access the Facebook app since approximately 2008. His device has run on iOS version
17 14.5 or later since approximately April 2021.

18 29. Mr. Letoski did not consent to Facebook tracking his activity. He configured the settings
19 on his iPhone to not allow the Facebook app to track him.

20 30. Using the systematic process described below, Meta tracked and intercepted Mr. Letoski's
21 specific electronic activity and private communications with third-party websites opened within
22 Facebook's in-app browser without his knowledge or consent. Mr. Letoski reasonably expected that his
23 communications with third-party websites were confidential, solely between himself and those websites,
24 and that such communications—which include text entries, passwords, personally identifiable
25 information, and other sensitive, confidential and private information—would not be intercepted or
26 tracked by Meta.
27
28

Louis Green

1
2 31. Plaintiff Louis Green is an adult citizen of the state of Illinois who resides in Hazel Crest,
3 Illinois. Mr. Green has had an active Facebook account since approximately March 2010. He has used
4 his iPhone to access the Facebook app since approximately March 2010. His device has run on iOS
5 version 14.5 or later since approximately April 2021.

6 32. Mr. Green did not consent to Facebook tracking his activity. He configured the settings
7 on his iPhone to not allow the Facebook app to track him.

8 33. Using the systematic process described below, Meta tracked and intercepted Mr. Green’s
9 specific electronic activity and private communications with third-party websites opened within
10 Facebook’s in-app browser without his knowledge or consent. Mr. Green reasonably expected that his
11 communications with third-party websites were confidential, solely between himself and those websites,
12 and that such communications—which include text entries, passwords, personally identifiable
13 information, and other sensitive, confidential and private information—would not be intercepted or
14 tracked by Meta.
15

Ed Rennie

16 34. Plaintiff Ed Rennie is an adult citizen of the state of Massachusetts who resides Salem,
17 Massachusetts. Mr. Rennie has had an active Facebook account since approximately 2009. He has used
18 his iPhone to access the Facebook app since approximately 2011. His device has run on iOS version 14.5
19 or later since approximately April 2021.
20

21 35. Mr. Rennie did not consent to Facebook tracking his activity. He configured the settings
22 on his iPhone to not allow the Facebook app to track him.

23 36. Using the systematic process described below, Meta tracked and intercepted Mr. Rennie’s
24 specific electronic activity and private communications with third-party websites opened within
25 Facebook’s in-app browser without his knowledge or consent. Mr. Rennie reasonably expected that his
26 communications with third-party websites were confidential, solely between himself and those websites,
27 and that such communications—which include text entries, passwords, personally identifiable
28

1 information, and other sensitive, confidential and private information—would not be intercepted or
2 tracked by Meta.

3 **Teia Pittman**

4 37. Plaintiff Teia Pittman is an adult citizen of the state of Maryland who resides in Baltimore,
5 Maryland. Ms. Pittman has had an active Facebook account since approximately 2008. She has used her
6 iPhone to access the Facebook app since approximately 2011. Her device has run on iOS version 14.5 or
7 later since April 2021.

8 38. Ms. Pittman did not consent to Facebook tracking her activity. She configured the settings
9 on her iPhone to not allow the Facebook app to track her.

10 39. Using the systematic process described below, Meta tracked and intercepted Ms.
11 Pittman’s specific electronic activity and private communications with third-party websites opened
12 within Facebook’s in-app browser without her knowledge or consent. Ms. Pittman reasonably expected
13 that her communications with third-party websites were confidential, solely between herself and those
14 websites, and that such communications—which include text entries, passwords, personally identifiable
15 information, and other sensitive, confidential and private information—would not be intercepted or
16 tracked by Meta.
17

18 **Raven Johnson**

19 40. Plaintiff Raven Johnson is an adult citizen of the state of Missouri who resides in Cape
20 Girardeau, Missouri. Ms. Johnson has had an active Facebook account since approximately 2010. She
21 has used her iPhone to access the Facebook app since approximately 2012. Her device has run on iOS
22 version 14.5 or later since April 2021.

23 41. Ms. Johnson did not consent to Facebook tracking her activity. She configured the settings
24 on her iPhone to not allow the Facebook app to track her.

25 42. Using the systematic process described below, Meta tracked and intercepted Ms.
26 Johnson’s specific electronic activity and private communications with third-party websites opened
27 within Facebook’s in-app browser without her knowledge or consent. Ms. Johnson reasonably expected
28

1 that her communications with third-party websites were confidential, solely between herself and those
2 websites, and that such communications—which include text entries, passwords, personally identifiable
3 information, and other sensitive, confidential and private information—would not be intercepted or
4 tracked by Meta.

5
6 **Chanel Robinson**

7 43. Plaintiff Chanel Robinson is an adult citizen of the state of Pennsylvania who resides in
8 Philadelphia, Pennsylvania. Ms. Robinson has had an active Facebook account since approximately
9 2009. She has used her iPhone to access the Facebook app since 2012. Her device has run on iOS version
10 14.5 or later since April 2021.

11 44. Ms. Robinson did not consent to Facebook tracking her activity. She configured the
12 settings on her iPhone to not allow the Facebook app to track her.

13 45. Using the systematic process described below, Meta tracked and intercepted Ms.
14 Robinson’s specific electronic activity and private communications with third-party websites opened
15 within Facebook’s in-app browser without her knowledge or consent. Ms. Robinson reasonably expected
16 that her communications with third-party websites were confidential, solely between herself and those
17 websites, and that such communications—which include text entries, passwords, personally identifiable
18 information, and other sensitive, confidential and private information—would not be intercepted or
19 tracked by Meta.

20 **Kevin Zenstein**

21 46. Plaintiff Kevin Zenstein is an adult citizen of the state of Pennsylvania who resides in
22 Lafayette Hill, Pennsylvania. Mr. Zenstein has had an active Facebook account since approximately
23 2013. He has used his iPhone to access the Facebook app since approximately 2013. His device has run
24 on iOS version 14.5 or later since approximately April 2021.

25 47. Mr. Zenstein did not consent to Facebook tracking his activity. He configured the settings
26 on his iPhone to not allow the Facebook app to track him.

1 indicate they may take interest in a certain advertised product or service. Meta’s profits thus depend on
2 connecting advertisers with its massive repository of personal data on the users of its platforms. To this
3 end, Meta collects extensive data about its users, attributes users’ data and browsing activity to their
4 individual accounts, continuously aggregates and analyzes this data using advanced algorithms, and
5 deploys the data to sell targeted advertising services.

6 59. The personal information Meta collects has economic value. An older study valued users’
7 web-browsing histories at \$52 per year. The Organization for Economic Cooperation and Development
8 estimated the prices for various individual data points: \$0.50 for an address, \$2 for birthdate, \$8 for a
9 Social Security number, \$3 for a driver’s license number, and \$35 for a military record. More recent
10 estimates suggest the value of personal data continues to be high: a personal email can be worth \$89, a
11 complete health care record is valued at around \$250, and a hacked Facebook account can sell for \$65 on
12 the dark web. Similarly, a 2019 report found that data generated from an adult is worth roughly \$35 per
13 month.

14 60. Between 2009 and 2021 Meta’s annual advertising revenues grew exponentially. In 2021
15 Meta took in over \$114 billion in advertising revenue, which accounted for 97% of Meta’s total revenue
16 in 2021, an approximately 37% year-over-year increase of around \$31 billion.

17 **B. Meta’s tracking of users before Apple’s iOS 14.5 software update**

18 61. In late 2020 Apple announced that its iOS 14.5 software update would change how its
19 Apple Devices handle users’ privacy preferences, requiring apps to obtain users’ affirmative consent to
20 being tracked before tracking them. Apple stated that these changes were intended to provide users of
21 Apple products with greater privacy and control over their mobile app data.

22 62. Before the iOS 14.5 software update, the default settings on Apple Devices required users
23 to opt out of being tracked by apps. As such, app owners and developers could track users by default,
24 unless the user changed their settings. Therefore, apps, including Facebook, on most Apple Devices could
25 access user-level data and the Identifier for Advertising (“IDFA”) without the device owner’s consent.

26 63. The IDFA is a random device identifier assigned by Apple to a user’s Apple Device that
27 allows the app to recognize that specific device and track the user’s activity across third-party websites.
28 IDFAs enable precise targeting and tracking of users within apps on Apple Devices. Using the IDFA,

1 information collected through an app or website can be connected to information about the user gathered
 2 from other online locations.

3 64. Before Apple’s iOS 14.5 software update, Meta used a tool called Facebook Attribution
 4 that enabled advertisers to measure and understand the impact of their ads across multiple publishers,
 5 channels, and devices. This tool helped advertisers understand the true value of their ads and assess which
 6 were most effective. But without the ability to collect IDFAs and monitor users’ activity across third-
 7 party websites, Meta cannot see how users are engaging with ads on the Facebook app and track them as
 8 they progress through various “touchpoints” on different devices. Such attribution is critical to digital
 9 marketing.

10 65. Meta describes attribution as “the process of assigning credit to touchpoints along a
 11 consumer’s conversion path. By understanding which of your ads should get credit for leading a
 12 consumer to take an action you wanted, such as making a purchase, you can better measure the
 13 effectiveness of your ads and make decisions for future planning and optimization.” As Meta further
 14 explains:

[L]et’s say someone saw your ads while browsing the Facebook app on their
 mobile phone, on a website they visited while on their work computer, and
 on a search engine while on their home computer. If the last ad that this
 person clicked on before making their purchase was the ad on the search
 engine from their home computer, it can be tempting to think that this search
 engine ad should get all the credit for making the sale happen, even though
 all of the other ads contributed to building awareness and consideration.

Each of these steps leading up to the conversion are called touchpoints,
 which include any of a consumer’s interactions with an ad. They make up a
 consumer’s conversion path, which may look something like this:



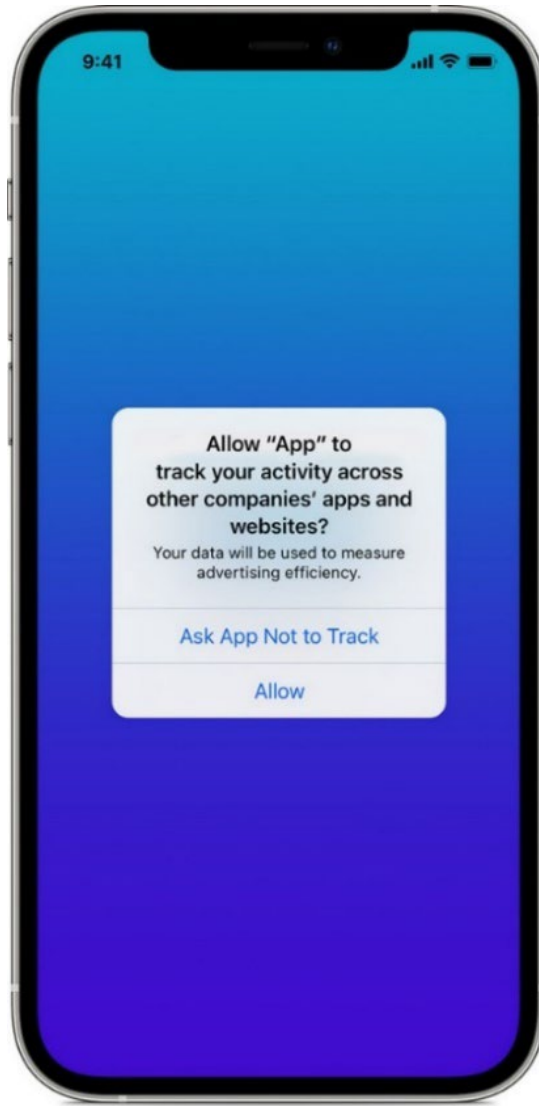
For example, the first touchpoint may introduce someone to a brand or
 product, the middle touchpoints may help increase their consideration of the
 product and the last touchpoint may lead them to take the action of
 converting. Attribution combines the data from the touchpoints in a
 consumer’s conversion path with the model you choose to apply to this data
 to understand which touchpoints should get credit for the conversion.

1 **C. Apple’s iOS 14.5 update**

2 66. Apple’s iOS 14.5 software update, introduced in April 2021, added App Tracking
3 Transparency (“ATT”). ATT converted the “opt out of tracking” framework to an “opt-in” regime.
4 Hence, with iOS 14.5 and later, apps including Facebook must first obtain a user’s permission before
5 accessing their IDFA and tracking their activity across third-party websites. Reasonable consumers
6 understand that by choosing not to “opt in” to tracking, they are denying the app permission to track their
7 keystrokes and other activities as they navigate from the Facebook app to a third-party website.

8 67. For companies like Meta that generate revenue by selling digital ads, Apple’s iOS 14.5
9 software update made it much harder to precisely target ads using existing algorithms and to attribute a
10 user’s online purchase to a specific ad or ad campaign. Because Meta monetizes online activity by
11 converting it to information useful to advertisers, the sudden inability to track consumer browsing
12 activities threatened Meta’s bottom line. Meta continues to confront this challenge as each subsequent
13 iteration of Apple’s iOS, up to and including the current version, iOS 16.3, supports the same ATT
14 functionality.

15 68. With ATT, Apple Device users see a pop-up message when they first launch an app that
16 is generated directly from the app that seeks to track their activity. As shown in Figure 1 below, the
17 bolded message on top asks: “Allow ‘App’ to track your activity across other companies’ apps and
18 websites?” Below, in blue text, the user is prompted to tap either “Ask App Not to Track” or “Allow.”
19 The user must make a selection or cannot proceed into the app; the choice is a mandatory step in the
20 navigation.



(Figure 1 – Image of the pop-up message that appears on Apple devices)

69. If a user selects “Ask App Not to Track,” the app is not able to access the IDFA or track the user’s activity using other information that identifies the user or their device. If a user selects “Allow,” the app is able to access the IDFA and may track the user in the manner it did prior to iOS 14.5 and ATT. Accordingly, Meta is aware of the user’s response to this prompt, as this decision dictates whether Meta can access the IDFA or gather data as it traditionally has.

70. Apple Device users also can configure their settings to *automatically* decline every app’s request to track their activity, by turning off the “Allow Apps to Request to Track” option in the device’s privacy settings. When this option is de-selected, no message prompt appears when an app requests to track the user across third-party websites; the technology treats any such request as if the user had selected

1 “Ask App Not to Track,” thereby preventing IDFA access and other tracking.

2 71. Thus, Apple Device users can indicate whether they consent to being tracked in one of
3 two ways: (1) via the tracking request pop-up message received from a particular app; or (2) by
4 configuring their setting to automatically reject all tracking requests. Accordingly, tracking by an app
5 after the iOS 14.5 software update requires the user’s express permission. Absent such permission,
6 tracking by an app overrides and disregards the user’s denial of consent.

7 72. Apple’s policy shift fundamentally altered—and enhanced—the degree of control the
8 individual user has over the information they share with the apps on their Apple Devices. By requiring
9 apps to obtain permission *before* tracking users, Apple changed its mobile device privacy framework so
10 as to obtain clear, advance user consent or declination to being tracked. Users were thus empowered to
11 decide whether they want to be tracked by the Facebook app at all, putting the onus on Meta to obtain
12 users’ affirmative consent.

13 73. When presented with this privacy choice, Plaintiffs and Class Member explicitly declined
14 to be tracked by Meta, either by (a) tapping “Ask App Not to Track” when prompted by the pop-up
15 message from the Facebook app, or (b) configuring their Apple Device settings to automatically decline
16 requests to track their activity across websites. Their clearly expressed privacy preference, therefore, was
17 *not* to be tracked by Meta when navigating to third-party websites from the Facebook app.

18 74. Through the ATT framework, Meta knows whether users have consented to tracking by
19 the Facebook app. Without this consent, Meta is not permitted to link together user or device data
20 (a) collected from the Facebook app with (b) such data collected from third-party websites—a linkage
21 critical for targeted advertising and related analytics. Thus, in addition to being a mandatory element of
22 the ATT framework, whether Apple Device users permit tracking is bound up with Meta’s digital
23 advertising business. Yet despite knowing that Plaintiffs and Class Members did not consent to being
24 tracked by the Facebook app, Meta tracked them anyway.

25 **D. Meta’s lost profits and P.R. effort in response to Apple’s iOS 14.5 update**

26 75. As noted above, following Apple’s privacy policy change and implementation of ATT,
27 Meta’s digital advertising revenue sharply declined: “According to [Meta], empowering Apple’s users to
28 opt out of tracking cost the company \$10,000,000,000 in the first year, with more losses to come after

1 that,” according to the Electronic Frontier Foundation. In Q2 2022, Meta’s ad revenue decreased by 1%
2 compared to the same period in 2021, and in Q3 2022, Meta’s revenue decreased by 4% compared to the
3 same period the year before.

4 76. Meta attributed the large declines in part to Apple’s changes to its iOS operating system
5 in April 2021. In its Q2 2022 Form 10-Q quarterly report, Meta stated, “[o]ur advertising revenue
6 continues to be adversely affected by reduced marketer spending as a result of limitations on our ad
7 targeting and measurement tools arising from changes to the iOS operating system beginning in 2021.”
8 Meta acknowledged that Apple’s “changes to iOS . . . limit our ability to target and measure ads
9 effectively.” In its Q3 2022 Form 10-Q quarterly report, Meta stated that “in 2021, Apple made certain
10 changes to its products and data use policies in connection with changes to its iOS operating system that
11 reduce our and other iOS developers’ ability to target and measure advertising, which has negatively
12 impacted, and we expect will continue to negatively impact, the size of the budgets marketers are willing
13 to commit to us and other advertising platforms.”

14 77. Recognizing that most iOS users would not consent to tracking if given the choice, Meta
15 vehemently criticized and opposed Apple’s privacy shift and attempted to sway public opinion against
16 it. As reported by CNN, after Apple’s announcement of iOS 14.5, Meta began “waging a public relations
17 effort to attack Apple ahead of new iOS data privacy changes that would make it harder for advertisers
18 to track users, in a possible sign of just how much the social network views the move as a threat to its
19 core business.” Meta held press conferences and ran advertisements critical of Apple’s decision to require
20 affirmative user consent to being tracked. In ads in The New York Times, Wall Street Journal and
21 Washington Post, Facebook disparaged Apple’s upcoming requirement for users to give explicit
22 permission for apps to track them, arguing the move would impair targeted advertising and therefore
23 could be “devastating” to millions of small business advertisers. Meta-owned WhatsApp also joined in,
24 “criticiz[ing] Apple over its move to display a summary of an app’s privacy practices before a user
25 downloads it from the App Store, almost like a nutrition label for data collection.”

26 78. Apple responded in part, “We believe that this is a simple matter of standing up for our
27 users. Users should know when their data is being collected and shared across other apps and websites—
28 and they should have the choice to allow that or not.” Apple further noted that “App Tracking

1 Transparency in iOS 14 does not require Facebook to change its approach to tracking users and creating
2 targeted advertising, it simply requires they give users a choice.”

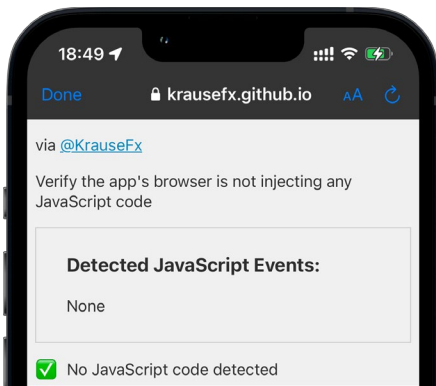
3 79. As of May 2021, shortly after Apple introduced iOS 14.5, 96% of Apple users in the
4 United States had *not* consented to being tracked by apps on their iPhone. In response Meta began
5 showing its users a screen that described its view of the consequences of iOS 14.5, including potential
6 long-term harm to Meta’s ability to provide apps and software. Through these and related
7 communications strategies, contemporaneous reports noted, Meta was “threatening that users will need
8 to pay for their services. But only if users don’t allow [Meta] to track them from app to app after installing
9 iOS 14.5.”

10 80. Meta could not stop the iOS 14.5 change and ATT framework from going into effect.
11 To reverse the ensuing steep drop in revenue, Meta covertly deployed hidden code into third-party
12 websites via its in-app browser to track and monitor its users—and maintain access to their data—in
13 contravention of their stated preference not to be tracked by the Facebook app.

14 **E. How Meta secretly overrides users’ privacy settings**

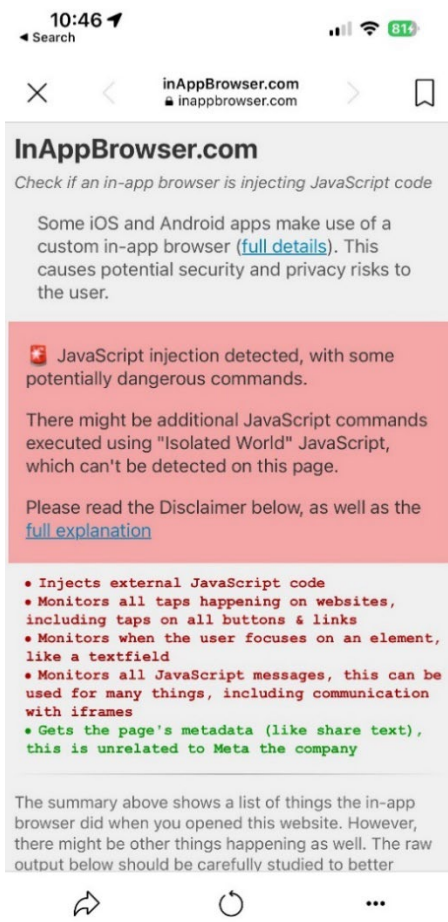
15 81. By injecting code into third-party websites, Meta is able to track users and intercept data
16 that would otherwise be unavailable to it. When a Meta user clicks on a link to an external website from
17 the Facebook app (e.g., from a friend’s post on their profile), Meta *automatically* reroutes the user to its
18 own in-app web browser instead of the users’ built-in web browser (such as Apple’s Safari app that is
19 preloaded onto iPhones). When this occurs, Meta injects a type of programming code known as
20 JavaScript into third-party websites so that it can track users’ activities on those websites. Third-party
21 websites are rendered *inside* the app—enabling Meta to monitor everything happening on external
22 websites, without consent from the user or from the website itself.

23 82. A computer science expert, Felix Krause, helped develop www.InAppBrowser.com, a
24 website that allows users to detect whether a particular in-app browser is injecting code into third-party
25 websites. Figure 2 below shows what happens when a user clicks on a web link they received in the
26 Telegram app, a messaging platform that does not inject JavaScript into third-party websites, but which
27 openly prompts users to use Telegram’s own in-app browser instead of a default browser:
28



(Figure 2) Hence, as demonstrated by the image above, not all in-app browsers disregard users' privacy or override their devices' privacy settings. Telegram, in other words, does not track users' activity on or communications with third-party web pages.

83. Compare the Telegram image in Figure 2 above with the image shown in Figure 3 below, displaying what happens when a user clicks on a web link in the iOS Facebook app:



1 (Figure 3) Thus, when the same HTML file (website) is opened from the iOS Facebook app,
2 www.InAppBrowser.com detects and identifies several different JavaScript events.

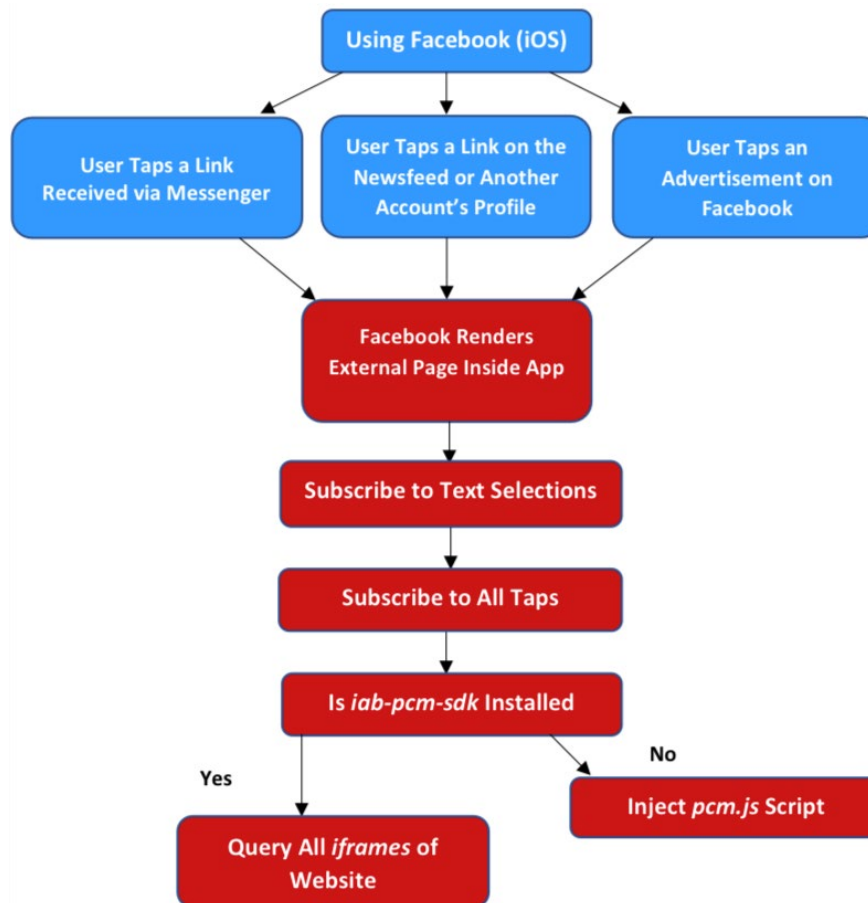
3 84. Krause’s report, entitled “*iOS Privacy: Instagram and Facebook can Track Anything you*
4 *do on any Website in their In-App Browser,*” describes how Meta uses JavaScript to alter websites and
5 override its users’ default privacy settings by sending users to Facebook’s in-app browser instead of their
6 default web browser.

7 85. Meta’s practice of injecting its JavaScript code into the code of third-party websites is
8 similar to actions taken by malicious actors seeking to intercept confidential information communicated
9 to a website. As one data security company described:

10 **What is a JavaScript Injection Attack?**

11 A JavaScript injection attack is a type of attack in which a threat actor
12 injects malicious code directly into the client-side JavaScript. This allows
13 the threat actor to manipulate the website or web application and collect
14 sensitive data, such as personally identifiable information (PII) or payment
information.

15 86. When the Facebook app injects Meta’s JavaScript code (“pcm.js”) into a third-party
16 website accessed from within Facebook’s in-app browser, it creates a bridge to communicate between
17 the Facebook app and the third-party website. This allows Meta to intercept and record users’ interactions
18 and communications with third parties, providing data that Meta analyzes and uses to boost its advertising
19 revenue. As illustrated in Figure 4 below, this systematic process occurs whenever a user clicks on a link
20 they received in their inbox (through the private messaging feature), or when they click on a link
21 displayed on their “news feed” or on another Facebook account’s “profile” or post, or when they tap a
22 link within Facebook that is a digital ad.



17 (Figure 4) The image above depicts the systematic manner in which Meta injects its JavaScript code into
18 third-party webpages for the purpose of intercepting, tracking, monitoring, and collecting data about its
19 users' interactions with those webpages.

20 87. After causing the third-party website to be rendered in Facebook's in-app browser, Meta
21 adds JavaScript "event listeners" to the third-party website. As the name suggests, "event listeners" are
22 pieces of JavaScript code that "listen" and trigger every time an "event" occurs. For the Facebook in-app
23 browser, Meta has implemented JavaScript event listeners that listen for (or "subscribe to"): any tap on
24 a button or link; any time a user focuses on an element (such as selecting a text field); and all JavaScript
25 messages.

26 88. When users engage with any of these "events" on the third-party website rendered within
27 Facebook's in-app browser, an event listener contemporaneously captures and transmits the information
28 to the Facebook app. Hence the event listeners operate like a keystroke logger, allowing Meta to acquire,

1 in real time, information a user transmits to a third-party website in real time, before that information is
2 electronically stored. In this way, Meta accesses and intercepts this information while it is in transit to
3 the third-party site.

4 89. These event listeners are critical to Meta’s ability to intercept, view, monitor, and record
5 all user interactions with third parties—every button and link users tap, text selections, screenshots, form
6 inputs (including passwords, addresses, and payment card numbers), personally identifiable information,
7 protected health details, and other private and confidential communications and data. In the context of an
8 online purchase, Facebook’s in-app browser collects and records all details of the purchase, including the
9 item purchased; name and address of purchaser; their telephone number, credit card or bank information,
10 usernames, passwords and birthdate; and the purchase price. Similarly, Facebook’s in-app browser
11 acquires and records details about certain users’ physical and mental health when they click on a link to
12 a medical provider’s website. Once there, HIPAA-protected health information provided by the user also
13 can be intercepted and captured by Meta.

14 90. At no point while communicating with a third-party website did Plaintiffs or Class
15 Members intend to transmit any information to Meta or the Facebook app. On the contrary, all Plaintiffs
16 and Class Members expressly denied Meta permission to monitor their online activity.

17 91. Meta’s surreptitious conduct precludes a reasonable user from knowing the Facebook app
18 receives any information once they tap a link to a third-party website.

19 92. Additionally, Meta’s pcm.js scans the third-party website rendered within Facebook’s in-
20 app browser to detect whether the Meta Pixel is present on the website. The Meta Pixel is a snippet of
21 programming code that, once installed on a website, allows website owners to track visitor actions to
22 target products and services to those visitors on Facebook. Meta tells website owners that the Meta Pixel
23 allows it “to match your website visitors to their respective Facebook User accounts.”

24 93. If the Meta Pixel is present on the third-party website, Meta’s JavaScript code will
25 exfiltrate the Meta Pixel data from the website to the Facebook app in real time. This data includes
26 personally identifiable information and information about the content users viewed on the third-party
27 website. For example, if a user on a financial services website interacts with a button corresponding to
28 their credit score, that personal information would be included in the data that Meta acquires.

1 94. Meta is therefore able to surveil and extract details about users’ texting, selections, and
2 other communications with third-party websites. Krause further described technical elements of this
3 process:

4 [Event listeners], in combination with listening to screenshots, gives Meta full
5 insight over what specific piece of information was selected & shared. The
6 [Meta] app checks if there is an element with the ID iab-pcm-sdk: According
7 to this tweet, the iab likely refers to “In App Browser”. If no element with the
8 ID iab-pcm-sdk was found, [Meta] creates a new script element, sets its
9 source to https://connect.facebook.net/en_US/pcm.js. It then finds the first
10 script element on [the] website to insert the pcm JavaScript file right before.
11 [Meta] also queries for iframes on [the] website.

12 95. For users of iOS 14.5 or later, Meta’s tracking occurs even if those users—like all
13 Plaintiffs and Class Members—*declined* to consent by tapping “Ask App Not to Track” or their device
14 settings were configured to decline all requests to track. If a user accessed the same third-party website
15 directly through Apple’s Safari web browser, instead of Facebook’s in-app browser, Safari would
16 actively block and prevent Meta’s ability to intercept and track the user’s activity on the third-party
17 website. But, through the mechanisms detailed above, Meta tracks this same activity when the user
18 engages in activity through Facebook’s in-app browser.

19 96. Meta knowingly tracks users across the web in a manner that circumvents users’ privacy
20 preferences and ATT settings on their Apple devices. Further, the technical nature and complexity of
21 Meta’s conduct, in sending users to its own undisclosed in-app browser that is invisibly configured to
22 intercept and redirect users’ communications to Meta, makes it impossible for ordinary users to realize
23 what Meta is doing.

24 **F. Meta’s conduct harmed Plaintiffs and Class Members**

25 97. Meta does not inform Facebook users that clicking on links to third-party websites from
26 within Facebook will automatically send the user to Facebook’s in-app browser, as opposed to the user’s
27 default web browser, or that Meta will monitor the user’s activity and communications while browsing
28 on those sites. Because nothing alerts users to these facts, they are unaware of the tracking. Users freely
engage with these sites, sharing all manner of personal facts and preferences, without having reason to
suspect they are being tracked or are still within Facebook’s app.

1 98. Meta fails to disclose the consequences of browsing, navigating, and communicating with
2 third-party websites from within Facebook’s in-app browser—namely, that doing so may override the
3 privacy settings and preferences of users intended to block and prevent tracking. Meta also conceals that
4 it injects JavaScript that alters external third-party websites so that it can intercept, track, and record data
5 it otherwise could not access. There was never any pop-up window or other conspicuous notice to users
6 regarding Meta’s tracking practice. The relevant “Off-Facebook activity” settings tab within the
7 Facebook app did not disclose the practice. At no point did Meta fairly or reasonably disclose to users its
8 practice of intercepting, monitoring, and selling information gleaned from their online activities and
9 communications even after they declined consent to being tracked.

10 99. Even users who may realize they are visiting websites from within Facebook’s in-app
11 browser are not informed that the browser ignores, rejects, and overrides their pop-up response or privacy
12 settings and enables Meta to track, intercept, and monitor their activities on third-party websites. A
13 reasonable consumer has no way of detecting Meta’s JavaScript injection; a website viewed within
14 Facebook’s in-app browser functions no differently than otherwise. Nor would a reasonable consumer
15 expect Meta to disregard and override their clearly communicated refusal to be tracked by embedding
16 JavaScript code on the third-party websites accessed through the Facebook app.

17 100. Most users of Apple Devices running iOS 14.5 and above also reasonably expect that their
18 communications with external third-party websites are not being intercepted and tracked because Apple’s
19 default browser for its devices, Safari, disables and blocks third-party cookies. Meta does not inform
20 users that its in-app browser differs from Safari and other browsers regarding such privacy settings.

21 101. Plaintiffs reasonably believed that their communications and interactions with third-party
22 websites were solely with those sites. Had Plaintiffs known that Meta could and would use its in-app
23 browser to nullify Plaintiffs’ ATT settings and other privacy choices, Plaintiffs would have avoided
24 navigating to third-party websites from within Facebook. Instead, they would have copied and pasted
25 hyperlinks into their standard browser to avoid being tracked, and ensured that their communications
26 with third-party websites were made outside of any Meta platform, particularly when the communications
27 involved sensitive or other personally identifiable information, such as private health information.

28

1 **Class:** All persons in the United States with active Facebook accounts who (i) visited a
2 third-party external website on Facebook’s in-app browser while using an Apple Device
3 running iOS 14.5 or higher, and (ii) did not allow the Facebook app to track them.

4 **California Subclass:** All persons with active Facebook accounts who (i) visited a third-
5 party external website on Facebook’s in-app browser while using an Apple Device
6 running iOS 14.5 or higher in California, and (ii) did not allow the Facebook app to
7 track them.

8 **Florida Subclass:** All persons with active Facebook accounts who (i) visited a third-
9 party external website on Facebook’s in-app browser while using an Apple Device
10 running iOS 14.5 or higher in Florida, and (ii) did not allow the Facebook app to track
11 them.

12 **Illinois Subclass:** All persons with active Facebook accounts who (i) visited a third-
13 party external website on Facebook’s in-app browser while using an Apple Device
14 running iOS 14.5 or higher in Illinois, and (ii) did not allow the Facebook app to track
15 them.

16 **Maryland Subclass:** All persons with active Facebook accounts who (i) visited a third-
17 party external website on Facebook’s in-app browser while using an Apple Device
18 running iOS 14.5 or higher in Maryland, and (ii) did not allow the Facebook app to track
19 them.

20 **Massachusetts Subclass:** All persons with active Facebook accounts who (i) visited a
21 third-party external website on Facebook’s in-app browser while using an Apple Device
22 running iOS 14.5 or higher in Massachusetts, and (ii) did not allow the Facebook app to
23 track them.

24 **Missouri Subclass:** All persons with active Facebook accounts who (i) visited a third-
25 party external website on Facebook’s in-app browser while using an Apple Device
26 running iOS 14.5 or higher in Missouri, and (ii) did not allow the Facebook app to track
27 them.

28

1 **Pennsylvania Subclass:** All persons with active Facebook accounts who (i) visited a
2 third-party external website on Facebook’s in-app browser while using an Apple Device
3 running iOS 14.5 or higher in Pennsylvania, and (ii) did not allow the Facebook app to
4 track them.

5 **Washington Subclass:** All persons with active Facebook accounts who (i) visited a
6 third-party external website on Facebook’s in-app browser while using an Apple Device
7 running iOS 14.5 or higher in Washington, and (ii) did not allow the Facebook app to
8 track them.

9 105. Excluded from the Class are all Facebook users who tapped “Allow” on Apple’s “Allow
10 App to Track?” pop-up window or configured their Apple Device settings to permit apps to track their
11 activity. Also excluded from the Class are Meta and its officers, directors, employees, affiliates, legal
12 representatives, predecessors, successors and assigns, and any entity in which any of them has a
13 controlling interest, as well as all persons employed by counsel in this action and any judge to whom this
14 case is assigned, his or her spouse and immediate family members, and members of the judge’s staff.

15 106. The Class Period extends from the date that Meta began implementing the practices
16 described in the Complaint to the date of entry of judgment. Plaintiffs may modify the Class and Subclass
17 definitions or propose additional subclasses as appropriate based on further investigation and discovery.

18 107. Numerosity. The members of the Class are so numerous that joinder of all members would
19 be impracticable. While the number of Class Members is unknown to Plaintiffs at this time, it is estimated
20 to number in the millions. The identity of Class Members is readily ascertainable from Meta’s records.

21 108. Typicality. Plaintiffs’ claims are typical of the claims of the Class because Plaintiffs used
22 Meta’s platforms to view third-party websites that were embedded as URLs within the respective Meta
23 applications, and all Class Members were subjected to Meta’s wrongful and invasive tracking practices.

24 109. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests
25 of the Class Members. Plaintiffs’ interests are coincident with, and not antagonistic to, those of the Class
26 Members. Plaintiffs are represented by attorneys experienced in the prosecution of class action litigation,
27 including digital privacy protection litigation, who will vigorously prosecute this action for the Class.

1 110. Common Questions of Law and Fact Predominate. Questions of law and fact common to
2 the Class Members predominate over questions that may affect only individual Class Members because
3 Meta has acted on grounds generally applicable to the Class. The following questions of law and fact are
4 common to the Class and predominate over any individual issues:

- 5 a. Whether Meta intentionally tapped the lines of electronic communication between
6 Class Members and third-party websites they visited;
- 7 b. Whether Meta intentionally intercepted the private information of Class Members
8 in transit without their consent;
- 9 c. Whether Facebook’s in-app web browser secretly monitored and recorded Class
10 Members’ private communications and personally identifiable information;
- 11 d. Whether Meta violated state and federal laws by tracking its users’ online activities
12 and intercepting their communications when they visited third-party websites, even
13 when they expressly indicated that they did not wish to be tracked;
- 14 e. Whether Class Members have a reasonable expectation of privacy with respect to
15 such information;
- 16 f. Whether Meta’s invasion of Class Members’ privacy rights is highly offensive to a
17 reasonable person;
- 18 g. Whether Meta’s statements and omissions misled Class Members as to the level of
19 control they had over their private communications derived from activity on the
20 Facebook app;
- 21 h. Whether Meta was unjustly enriched as a result of its wrongful and invasive
22 practices; and
- 23 i. Whether Class Members are entitled to damages, restitution and/or injunctive relief
24 in view of Meta’s conduct.
25

26 111. Superiority. A class action will permit numerous similarly situated persons to prosecute
27 their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication
28

1 of evidence, effort, or expense. A class action will provide injured persons a method for obtaining redress
2 on claims that could not practicably be pursued individually. Plaintiffs know of no manageability or other
3 issue that would preclude maintenance of this case as a class action.

4 112. Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- 5 • The prosecution of separate actions by the individual members of the Class would
6 create a risk of inconsistent or varying adjudications establishing incompatible
7 standards of conduct for Meta;
- 8 • The prosecution of separate actions by individual Class Members would create a risk
9 of adjudications that would, as a practical matter, be dispositive of the interests of
10 other Class Members not parties to the adjudications, or would substantially impair or
11 impede their ability to protect their interests;
- 12 • Meta has acted or refused to act on grounds generally applicable to the Class, making
13 injunctive and corresponding declaratory relief appropriate with respect to the Class
14 as a whole; and
- 15 • The claims of Class Members are comprised of common issues whose resolution in a
16 class trial would materially advance this litigation.

17 **TOLLING OF THE STATUTES OF LIMITATIONS**

18 113. All applicable statute(s) of limitations have been tolled by Meta's knowing and active
19 concealment and denial of the facts alleged herein. Plaintiffs and Class Members could not have
20 reasonably discovered Meta's practice of tracking and intercepting their activities and communications
21 while they have an in-app browser open, even after they declined to consent to being tracked, until shortly
22 before this class action litigation commenced.

23 114. Meta was and remains under a continuing duty to disclose to Plaintiffs and Class Members
24 its practice of tracking and intercepting their activities and communications while they have an in-app
25 browser open. As a result of the active concealment by Meta, any and all applicable statutes of limitations
26 otherwise applicable to the allegations herein have been tolled.

FIRST CLAIM FOR RELIEF

VIOLATION OF THE WIRETAP ACT

18 U.S.C. § 2510 *et seq.*

(On Behalf of the Class)

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

115. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class.

116. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986 (“ECPA”), prohibits the intentional interception of any wire, oral, or electronic communication.

117. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

118. **Electronic Communications.** The communications between Plaintiffs and Class Members and third-party websites are “transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce” and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

119. **Content.** The ECPA defines content, when used with respect to electronic communications, to “include[] *any* information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (emphasis added).

120. **Interception.** The ECPA defines interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents ... include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

121. **Electronic, Mechanical, or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- (a) Plaintiffs’ and Class Members’ browsers;
- (b) Plaintiffs’ and Class Members’ Apple Devices;

- 1 (c) Defendant’s mobile applications including the Facebook app;
- 2 (d) Defendant’s in-app browser;
- 3 (e) Defendant’s electronic servers; and
- 4 (f) The code deployed by Defendant to circumvent users’ privacy controls and
- 5 transmit their communications to Defendant.

6 122. Without Plaintiffs’, Class Members’, or third-party websites’ knowledge or consent, Meta
7 intercepted the contents of their electronic communications when they navigated from Facebook to third-
8 party websites.

9 123. Meta intentionally used technology, including the JavaScript code it injected into third-
10 party websites, as a means of intercepting and acquiring the contents of Plaintiffs’ and Class Members’
11 electronic communications, in violation of the Wiretap Act.

12 124. Meta intentionally intercepted Plaintiffs’ and Class Members’ information in transit. Meta
13 intercepted Plaintiff’s and Class Members’ website communications, whenever they used Facebook’s in-
14 app browser to communicate with third-party websites, using the JavaScript code inserted by Meta,
15 including every click, keystroke (e.g., text being entered into an information field or text box), URL
16 visited, and other electronic communication. These website communications—which comprise the
17 transfer of signs, signals, writing, images, sounds, data, and/or intelligence transmitted in whole or in
18 party by wire, radio, electromagnetic, photoelectric, or photo-optical system—constitute “electronic
19 communications” under the Wiretap Act and were contemporaneously copied by Meta in real time.

20 125. The personal information was content as defined by the Wiretap Act as it involves the
21 substance and import of Plaintiffs’ communications with third-party websites and not simply routine
22 identifiers or metadata. Meta configured and implemented code to surreptitiously capture user
23 information such as keystrokes, search queries, and information entered into forms or text boxes.

24 126. Plaintiffs and Class Members were not aware that Meta was intercepting its users’
25 electronic communications and tracking their communications and interactions with third-party websites.
26 Plaintiffs and Class Members did not consent to Meta’s tracking and collection of their personal
27 communications, and in fact they affirmatively opted out of such tracking on their Apple Devices.
28

1 Additionally, the nature of the tracking and collection of information at issue goes beyond what a
2 reasonable consumer would anticipate when using the internet or mobile applications.

3 127. By intentionally disclosing or endeavoring to disclose the electronic communications of
4 Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to
5 know that the information was obtained through the interception of an electronic communication in
6 violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

7 128. By intentionally using, or endeavoring to use, the contents of the electronic
8 communications of Plaintiffs and Class Members, while knowing or having reason to know that the
9 information was obtained through the interception of an electronic communication in violation of 18
10 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

11 129. Plaintiffs and Class Members are persons whose electronic communications were
12 intercepted within the meaning of Section 2520. As such, they are entitled to preliminary, equitable and
13 declaratory relief, in addition to statutory damages of the greater of \$10,000 or \$100 per day for each day
14 of violation, actual damages, punitive damages, and reasonable attorneys' fees and costs of suit.

15 **SECOND CLAIM FOR RELIEF**

16 **VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT**
17 **18 U.S.C. § 1030 *et seq.* ("CFAA")**
18 **(On Behalf of the Class)**

19 130. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and
20 bring this count individually and on behalf of the Class.

21 131. The Consumer Fraud and Abuse Act establishes a private cause of action against a
22 person who "knowingly accessed a computer without authorization or exceeding authorized access," and
23 whose prohibited access results in damage or loss in excess of \$5,000. 18 U.S.C. § 1030(g) (referencing
24 § 1030(c)(4)(A)(i)(I)); *see also* § 1030(a).

25 132. The CFAA establishes liability against whomever:

26 (a) "knowingly causes the transmission of a program, information, code, or
27 command, and as a result of such conduct, intentionally causes damage without authorization, to a
28 protected computer" (§ 1030(a)(5)(A));

1 (b) “intentionally accesses a protected computer without authorization, and as a
2 result of such conduct, recklessly causes damage” (§ 1030(a)(5)(B)); or

3 (c) “intentionally accesses a protected computer without authorization, and as a
4 result of such conduct, causes damage and loss” (§ 1030(a)(5)(C)).

5 133. The term “computer” means “an electronic, magnetic, optical, electrochemical, or other
6 high speed data processing device performing logical, arithmetic, or storage functions, and includes any
7 data storage facility or communications facility directly related to or operating in conjunction with such
8 device[.]” 18 U.S.C. § 1030(e)(1).

9 134. A “protected computer” is defined, in relevant part, as a computer “which is used in or
10 affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B).

11 135. “[E]xceeds authorized access” means “access[ing] a computer with authorization and
12 . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so
13 to obtain or alter.” 18 U.S.C. § 1030(e)(6).

14 136. “Loss” means “any reasonable cost to any victim, including the cost of responding to
15 an offense, conducting a damage assessment, and restoring the data, program, system, or information to
16 its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages
17 incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11).

18 137. Damage means “any impairment to the integrity or availability of data, a program, a
19 system, or information.” 18 U.S.C. § 1030(e)(8).

20 138. Plaintiffs’ and Class Members’ Apple Devices are “computers” under the CFAA by
21 virtue of their data processing and storage functions and their operation in conjunction with other similar
22 devices.

23 139. Plaintiffs’ and Class Members’ Apple Devices are “protected computers” under the CFAA
24 because, at all relevant times, they are and were used in and affect interstate and foreign commerce and
25 communication, including through contact and communication with remote servers and through personal
26 and business usages that affect interstate and foreign commerce.
27
28

1 140. Defendant exceeded, and continues to exceed, its authorized access to Plaintiffs’ and Class
2 Members’ protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2).

3 141. Defendant knowingly and intentionally exceeded its authorized access to Plaintiffs’ and
4 Class Members’ Apple Devices. Plaintiffs and Class Members did not consent to be tracked by the
5 Facebook app across third-party websites and configured their devices to reject such requests.

6 142. By exceeding its authorized access, Defendant obtained Plaintiffs’ and Class Members’
7 private and personally identifiable data and communications—including their clicks, keystrokes (such as
8 text being entered into an information field or text box), URLs of web pages visited, and/or other
9 electronic communications. Defendant’s injection of code into third-party websites rendered within
10 Facebook’s in-app browser allowed it to access information that it could not otherwise obtain.

11 143. By injecting code into third-party websites rendered within Facebook’s in-app browser,
12 Defendant knowingly caused the transmission of “a program, information, code, or command ... to a
13 protected computer” and, as a result of that conduct, intentionally caused damage in violation of 18 U.S.C.
14 § 1030(a)(5)(A).

15 144. By injecting code into third-party websites rendered within Facebook’s in-app browser,
16 Defendant intentionally accessed Plaintiffs’ and Class Members’ Apple Devices without authorization,
17 and as a result of that conduct, caused or recklessly caused damage or loss to those protected computers,
18 in violation of 18 U.S.C. §§ 1030(a)(5)(B) and (a)(5)(C).

19 145. Defendant’s injection of code into third-party websites rendered within Facebook’s in-app
20 browser was a single act by which Defendant intentionally accessed Plaintiffs’ and Class Members’
21 protected computers without authorization and exceeding authorization. As a direct and proximate result
22 of Defendant’s CFAA violations, Defendant caused damages and loss to Plaintiffs and Class Members
23 during a one-year period that exceed \$5,000 in value.

24 146. Defendant’s injection of code into third-party websites rendered within Facebook’s in-app
25 browser caused damage and loss to Plaintiffs and Class Members, including by decreasing the value of
26 their private and personally identifiable information and communications, and by impeding their ability
27 to control the dissemination and use of such information and communications, which they reasonably
28

1 believed would be protected from tracking and disclosure by result of the privacy controls they
2 implemented on their devices.

3 147. Defendant’s conduct also represents “a threat to public health or safety” under 18 U.S.C.
4 § 1030(c)(4)(A)(i)(IV) due to the sensitive, confidential information, including protected health
5 information, that Meta collects and disseminates to its advertising partners and/or other third parties
6 without adequate legal privacy protections.

7 148. Accordingly, Plaintiffs and Class Members may “maintain a civil action against the
8 violator to obtain compensatory damages and injunctive relief or other equitable relief” and hereby seek
9 recovery of economic damages and all other relief provided for under 18 U.S.C. § 1030(g).

10 **THIRD CLAIM FOR RELIEF**

11 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT**
12 **Cal. Penal Code § 630 *et seq.* (“CIPA”)**
13 **(On Behalf of the Class or, Alternatively, the California Subclass)**

14 149. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and
15 bring this count individually and on behalf of the Class or, alternatively, the California Subclass.

16 150. The California Invasion of Privacy Act , codified at Cal. Penal Code §§ 630-638, contains
17 the following statement of purpose:

18 The Legislature hereby declares that advances in science and technology
19 have led to the development of new devices and techniques for the purpose
20 of eavesdropping upon private communications and that the invasion of
21 privacy resulting from the continual and increasing use of such devices and
22 techniques has created a serious threat to the free exercise of personal
23 liberties and cannot be tolerated in a free and civilized society.

24 Cal. Penal Code § 630.

25 151. California Penal Code § 631(a) accordingly provides, in pertinent part:

26 Any person who, by means of any machine, instrument, or contrivance, or
27 in any other manner . . . willfully and without the consent of all parties to
28 the communication, or in any unauthorized manner, reads, or attempts to
read, or to learn the contents or meaning of any message, report, or
communication while the same is in transit or passing over any wire, line,
or cable, or is being sent from, or received at any place within this state; or
who uses, or attempts to use, in any manner, or for any purpose, or to
communicate in any way, any information so obtained, or who aids, agrees
with, employs, or conspires with any person or persons to unlawfully do, or

1 permit, or cause to be done any of the acts or things mentioned above in this
2 section, is punishable by a fine not exceeding two thousand five hundred
dollars (\$2,500).

3 152. At all relevant times, Meta's business practices described herein allowed it to access,
4 intercept, learn the contents of and collect Plaintiffs' and Class Members' personally identifiable
5 information and other data, including information concerning their interactions with third-party websites,
6 even when Plaintiffs' and Class Members' devices were set to block such actions.

7 153. Plaintiffs and Class Members, during one or more of their relevant interactions on the
8 internet during the Class Period, communicated with one or more third-party websites owned by entities
9 based in California, and whose servers were located in California, and also communicated with Meta's
10 servers located in California. Communications from the California web-based entities to Plaintiffs and
11 Class Members, and from Plaintiffs and Class Members to the California web-based entities, were sent
12 to California and illegally intercepted by Meta.

13 154. Plaintiffs and Class Members did not consent to any of Meta's actions in intercepting,
14 reading, and learning the contents of their communications with such California-based entities. Meta read
15 and learned the contents of Plaintiffs' and Class Members' communications in transit and without
16 authorization. Meta failed to disclose that it was intercepting, tracking and learning the contents of such
17 private conversations and activities when it directed users, without their knowledge or consent, to external
18 third-party websites from within the Facebook app.

19 155. Meta's conduct was intentional in that it purposefully diverted users to its in-app browser
20 and installed code which allows it to monitor and learn the content of its users' communications and other
21 browsing activities that would otherwise be unavailable to Meta. Meta directly participated in the
22 interception, reading, and/or learning of the contents of the communications between Plaintiffs and Class
23 Members and California-based web entities.

24 156. The information Meta intercepted while Plaintiffs and Class Members used the Facebook
25 in-app browser includes personally identifiable information and other highly specific information and
26 communications, including, without limitation, every button, keystroke and link a user taps, whether the
27 user has taken any screenshots, text entries (including passwords, birthdates, and payment card
28 information), and how much time a user spent on which websites.

1 157. Meta intentionally intercepted Plaintiffs’ and Class Members’ information in transit. Meta
2 intercepted Plaintiffs’ and Class Members’ website communications whenever they used Facebook’s in-
3 app browser to communicate with third-party websites using the JavaScript code inserted by Meta,
4 including every mouse movement, click, keystroke (e.g., text being entered into an information field or
5 text box), URL visited, and other electronic communication. These website communications constitute
6 electronic communications and were contemporaneously copied by Meta in real time.

7 158. Plaintiffs and Class Members have experienced damage and loss by reason of these
8 violations, including but not limited to, violation of their right to privacy. Unless restrained and enjoined,
9 Meta will continue to commit such acts.

10 159. As a result of the above violations and pursuant to CIPA section 637.2, Meta is liable to
11 Plaintiffs and Class Members for the greater of treble actual damages related to their loss of privacy in
12 an amount to be determined at trial, or statutory damages in the amount of \$5,000 per violation. Section
13 637.2 provides “[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs
14 has suffered, or be threatened with, actual damages.”

15 160. Plaintiffs further request, as provided under CIPA, reasonable attorneys’ fees and costs of
16 suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury
17 sufficient to prevent or deter the same or similar conduct by Meta.

18 **FOURTH CLAIM FOR RELIEF**

19 **VIOLATION OF THE UNFAIR COMPETITION LAW**
20 **Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”)**
21 **(On Behalf of the Class or, Alternatively, the California Subclass)**

22 161. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and
23 bring this count individually and on behalf of the Class or, alternatively, the California Subclass.

24 162. The UCL proscribes “any unlawful, unfair or fraudulent business act or practice and
25 unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof. Code § 17200.

26 163. Meta is a “person” as defined by Cal. Bus. & Prof. Code § 17201.

27 164. The acts and omissions complained of herein were conceived of and directed from, and
28 emanated from, California.

1 benefit. The information and data Meta intercepted includes highly sensitive and valuable personal
2 information, including but not limited to personally identifiable information, confidential medical facts,
3 and other privileged communications and private details.

4 169. Plaintiffs interacted with various third-party websites reasonably believing that their
5 browsing activities—and any facts and information communicated to third-party websites—were secure
6 and confidential (i.e., solely between themselves and the third-party website).

7 170. There is no justification for Meta’s conduct other than to increase, beyond what it would
8 have otherwise realized, its profit from fees from third parties and the value of its information assets by
9 acquisition of Plaintiffs’ and Class Members’ personal information. Meta’s conduct lacks justification in
10 that Meta has benefited from such conduct and practices while Plaintiffs and Class Members were misled
11 as to the nature and integrity of Meta’s services and were materially disadvantaged in regard to their
12 interests in the privacy and confidentiality of their personal information.

13 **Fraudulent**

14 171. Meta’s acts and practices were fraudulent in violation of the UCL because they were likely
15 to, and did, in fact, mislead the members of the public to whom they were directed. Meta actively
16 concealed its tracking practice at issue and had exclusive knowledge of it, creating a duty to disclose.

17 172. Meta failed to disclose this tracking practice. Its disclosure would have been a material
18 and important factor in Plaintiffs’ and Class Members’ actions related to visiting third-party websites
19 through Facebook’s in-app browser or another browser.

20 173. Meta’s secret, undisclosed, and deceptive tracking practice caused Plaintiffs and Class
21 Members to surrender more in their transaction with Meta than they otherwise would have. Had Plaintiffs
22 and Class Members known that Meta could and would use its in-app browser in the manner described,
23 directly counter to their stated preference known to Meta, they would have avoided navigating to third-
24 party websites from within Facebook, and instead would have copied and pasted links into their standard
25 browser to avoid being tracked, thereby avoiding this injury.

26 174. Meta’s conduct was unethical, deceptive and unscrupulous in part because it acted against
27 the express, known wish of Plaintiffs and Class Members not to be tracked without communicating to
28 them the material fact that Meta would, in fact, track their private browsing activities and

1 communications. Further, Meta’s deceptive conduct narrowly benefitted its own business interests at the
2 expense of Plaintiffs’ and Class Members’ fundamental privacy rights and interests protected by
3 California’s Constitution and common law.

4 175. Plaintiffs’ and Class Members’ loss of their personal information constitutes an economic
5 injury. Plaintiffs and Class Members have a property right in their personal information, which has value
6 to themselves as well as Meta, and lost money or property as a result of Defendant’s violations of the
7 UCL. Plaintiffs and Class Members have suffered harm in the form of lost property value, specifically
8 the diminution of the value of their private and personally identifiable data and content, of which they
9 lost control against their wishes. Meta’s actions also caused damage to and loss of Plaintiffs’ and Class
10 Members’ property right to control the dissemination and use of their personal information and
11 communications.

12 176. Plaintiffs and Class Members accordingly seek appropriate relief, including (1) restitution
13 under the UCL; and (2) such orders or judgments as may be necessary to enjoin Meta from continuing
14 its unfair, unlawful, and fraudulent practices. There is no adequate remedy at law that would provide
15 redress to Plaintiffs and Class Members or ensure that Meta, a serial privacy offender, will not continue
16 engaging in the same practices. Plaintiffs also seek reasonable attorneys’ fees and costs under applicable
17 law, including under California Code of Civil Procedure section 1021.5.

18 **FIFTH CLAIM FOR RELIEF**

19 **VIOLATION OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT**
20 **Fla. Stat. Ann. § 934.01 *et seq.* (“FSCA”)**
21 **(On Behalf of the Florida Subclass)**

22 177. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

23 178. Plaintiffs Lisa Bush and David Alzate bring this count individually and on behalf of the
24 Florida Subclass.

25 179. The Florida Security of Communications Act is codified at Florida Statutes Annotated
26 §§ 934.01–934.50. Florida Statutes Annotated § 934.03(1)(a) punishes, in pertinent part, any person who
27 “[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor
28 to intercept any wire, oral, or electronic communication.”

1 180. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
2 third-party websites allowed it to intercept the contents of Plaintiffs Lisa Bush’s and David Alzate’s and
3 Florida Subclass Members’ electronic communications with third-party websites.

4 181. Without Plaintiffs Lisa Bush’s and David Alzate’s, Florida Subclass Members’, or third-
5 party websites’ knowledge or consent, Meta intercepted the contents of Plaintiffs Lisa Bush’s and David
6 Alzate’s and Florida Subclass Members’ electronic communications when they navigated to third-party
7 websites within Facebook’s in-app browser.

8 182. Meta contemporaneously intercepted the contents of Plaintiffs Lisa Bush’s and David
9 Alzate’s and Florida Subclass Members’ electronic communications while they were in transit and
10 without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such
11 private conversations and activities when users visit external third-party websites from within the
12 Facebook app.

13 183. Meta intentionally used an electronic, mechanical, or other device—the JavaScript code
14 it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiffs
15 Lisa Bush’s and David Alzate’s and Florida Subclass Members’ electronic communications, in violation
16 of the FSCA.

17 184. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members were unaware that
18 Facebook was intercepting its users’ electronic communications and tracking their communications and
19 interactions with third-party websites.

20 185. Meta’s conduct was intentional in that it purposefully installed code which allows it to
21 intercept and learn the content of its users’ communications and other browsing activities that would
22 otherwise be unavailable to Meta.

23 186. The information Meta intercepted while Plaintiffs Lisa Bush and David Alzate and Florida
24 Subclass Members were using the Facebook in-app browser includes personally identifiable information
25 and other highly specific information and communications, including, without limitation, every button,
26 keystroke and link a user taps, whether the user has taken any screenshots, text entries (including
27 passwords and credit card information), and how much time a user spent on which websites.

1 187. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members intended and
2 believed that the information they provided to third-party websites while using Facebook’s in-app
3 browser would remain private and would not be transmitted to Meta.

4 188. Meta intentionally intercepted Plaintiffs Lisa Bush’s and David Alzate’s and Florida
5 Subclass Members’ information in transit. Meta intercepted their website communications whenever they
6 used Facebook’s in-app browser to communicate with third-party websites using the JavaScript code
7 inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an
8 information field or text box), URL visited, and other electronic communication. These website
9 communications constitute electronic communications and were contemporaneously copied by Meta in
10 real time.

11 189. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members have experienced
12 damage and loss by reason of these violations, including but not limited to, violation of the right to
13 privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

14 190. As a result of the above violations and pursuant to Florida Statutes Annotated § 934.10,
15 Meta is liable to the Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members for the greater
16 of their actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each
17 day of violation, or \$1,000.

18 191. Plaintiffs Lisa Bush and David Alzate further request, as provided under Florida Statutes
19 Annotated § 934.10, reasonable attorneys’ fees and costs of suit, injunctive and declaratory relief, and
20 punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or
21 similar conduct by Meta.

22 **SIXTH CLAIM FOR RELIEF**

23 **VIOLATION OF THE ILLINOIS EAVESDROPPING ACT**

24 **720 ILCS 5/14-1 *et seq.***

25 **(On Behalf of the Illinois Subclass)**

26 192. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

27 193. Plaintiffs Mark Letoski and Louis Green bring this count individually and on behalf of the
28 Illinois Subclass.

1 194. A person violates the Illinois Eavesdropping Act where he or she “knowingly and
2 intentionally . . . [i]ntercepts, records, or transcribes, in a surreptitious manner, any private electronic
3 communication to which he or she is not a party unless he or she does so with the consent of all parties
4 to the private electronic communication” 720 ILCS 5/14-2(a).

5 195. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
6 third-party websites allowed it to intercept, record, or transcribe the contents of Plaintiffs Mark Letoski’s
7 and Louis Green’s and Illinois Subclass Members’ private electronic communications with third-party
8 websites.

9 196. Without Plaintiffs Mark Letoski’s, Louis Green’s and Illinois Subclass Members’, or
10 third-party websites’ knowledge or consent, Meta intercepted, recorded, or transcribed the contents of
11 Plaintiffs Mark Letoski’s and Louis Green’s and Illinois Subclass Members’ electronic communications
12 when they navigated to third-party websites within Facebook’s in-app browser.

13 197. Meta contemporaneously intercepted the contents of Plaintiffs Mark Letoski’s and Louis
14 Green’s and Illinois Subclass Members’ electronic communications while they were in transit and
15 without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such
16 private conversations and activities when users visit external third-party websites from within the
17 Facebook app.

18 198. Meta failed to disclose that it was intercepting and tracking the contents of such private
19 conversations and activities when users visit external third-party websites from within the Facebook app.

20 199. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members were unaware
21 that Facebook was intercepting its users’ electronic communications and tracking their communications
22 and interactions with third-party websites.

23 200. Meta’s conduct was intentional in that it purposefully installed code which allows it to
24 intercept and learn the content of its users’ communications and other browsing activities that would
25 otherwise be unavailable to Meta.

26 201. The information Meta intercepted while Plaintiffs Mark Letoski and Louis Green and
27 Illinois Subclass Members were using the Facebook in-app browser includes personally identifiable
28 information and other highly specific information and communications, including, without limitation,

1 every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries
2 (including passwords and credit card information), and how much time a user spent on which websites.

3 202. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members intended and
4 believed that the information they provided to third-party websites while using Facebook’s in-app
5 browser would remain private and would not be transmitted to Meta.

6 203. Meta intentionally intercepted Plaintiffs Mark Letoski’s and Louis Green’s and Illinois
7 Subclass Members’ information in transit. Meta intercepted their website communications whenever they
8 used Facebook’s in-app browser to communicate with third-party websites using the JavaScript code
9 inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an
10 information field or text box), URL visited, and other electronic communication. These website
11 communications constitute electronic communications and were contemporaneously copied by Meta in
12 real time.

13 204. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members have experienced
14 damage and loss by reason of these violations, including but not limited to, violation of the right to
15 privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

16 205. As a result of the above violations and pursuant to 720 ILCS 5/14-6, Meta is liable to the
17 Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members for actual damages. Plaintiffs
18 Mark Letoski and Louis Green further request, as provided under 720 ILCS 5/14-6 injunctive and
19 declaratory relief and punitive damages in an amount to be determined by a jury sufficient to prevent or
20 deter the same or similar conduct by Meta.

21 **SEVENTH CLAIM FOR RELIEF**

22 **VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC**
23 **SURVEILLANCE CONTROL ACT**

24 **18 Pa. Stat. and Cons. Stat. Ann. § 5701 *et seq.* (“WESCA”)**

25 **(On Behalf of the Pennsylvania Subclass)**

26 206. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

27 207. Plaintiffs Chanel Robinson and Kevin bring this count individually and on behalf of the
28 Pennsylvania Subclass.

1 208. The Pennsylvania Wiretapping and Electronic Surveillance Control Act makes it unlawful
2 to “intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or
3 endeavor to intercept any wire, electronic or oral communication.” 18 Pa. Stat. and Cons. Stat. Ann. §
4 5703(1).

5 209. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
6 third-party websites allowed it to intercept the contents of Plaintiffs Chanel Robinson’s and Kevin
7 Zenstein’s and Pennsylvania Subclass Members’ electronic communications with third-party websites.

8 210. Without Plaintiffs Chanel Robinson’s and Kevin Zenstein’s, Pennsylvania Subclass
9 Members’, or third-party websites’ knowledge or consent, Meta intercepted the contents of Plaintiffs
10 Chanel Robinson’s and Kevin Zenstein’s and Pennsylvania Subclass Members’ electronic
11 communications when they navigated to third-party websites within Facebook’s in-app browser.

12 211. Meta contemporaneously intercepted the contents of Plaintiffs Chanel Robinson’s and
13 Kevin Zenstein’s and Pennsylvania Subclass Members’ electronic communications while they were in
14 transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents
15 of such private conversations and activities when users visit external third-party websites from within the
16 Facebook app.

17 212. Meta intentionally used an electronic, mechanical, or other device—the JavaScript code
18 it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiffs
19 Chanel Robinson’s and Kevin Zenstein’s and Pennsylvania Subclass Members’ electronic
20 communications, in violation of the WESCA.

21 213. Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members were
22 unaware that Facebook was intercepting its users’ electronic communications and tracking their
23 communications and interactions with third-party websites.

24 214. Meta’s conduct was intentional in that it purposefully installed code which allows it to
25 intercept and learn the content of its users’ communications and other browsing activities that would
26 otherwise be unavailable to Meta.

27 215. The information Meta intercepted while Plaintiffs Chanel Robinson and Kevin Zenstein
28 and Pennsylvania Subclass Members were using Facebook’s in-app browser includes personally

1 identifiable information and other highly specific information and communications, including, without
2 limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text
3 entries (including passwords and credit card information), and how much time a user spent on which
4 website.

5 216. Meta intentionally intercepted Plaintiffs Chanel Robinson's and Kevin Zenstein's and
6 Pennsylvania Subclass Members' information in transit. Meta intercepted their website communications
7 whenever they used Facebook's in-app browser to communicate with third-party websites using the
8 JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being
9 entered into an information field or text box), URL visited, and other electronic communication. These
10 website communications constitute electronic communications and were contemporaneously copied by
11 Meta in real time.

12 217. Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members
13 intended and believed that the information they provided to third-party websites while using Facebook's
14 in-app browser would remain private and would not be transmitted to Meta.

15 218. As a result of the above violations and pursuant to 18 Pennsylvania Statutes and
16 Consolidated Statutes Annotated § 5725(a), Meta is liable to Plaintiffs Chanel Robinson and Kevin
17 Zenstein and Pennsylvania Subclass Members for the greater of their actual damages, but not less than
18 liquidated damages computed at the rate of \$100 a day for each day of violation, or \$1,000. Plaintiffs
19 Chanel Robinson and Kevin Zenstein further request, as provided under 18 Pennsylvania Statutes and
20 Consolidated Statutes Annotated § 5725(a), reasonable attorneys' fees and costs of suit and punitive
21 damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct
22 by Meta.

23 **EIGHTH CLAIM FOR RELIEF**

24 **VIOLATION OF WASHINGTON'S PRIVACY ACT**

25 **Wash. Rev. Code Ann. § 9.73.030**

26 **(On Behalf of the Washington Subclass)**

27 219. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.
28

1 220. Plaintiffs Mary Thew and Lisa Evans bring this count individually and on behalf of the
2 Washington Subclass.

3 221. Washington Revised Code Annotated § 9.73.030(1) provides, in pertinent part:

4 [I]t shall be unlawful for any individual, partnership, corporation, [or]
5 association . . . to intercept, or record any: (a) Private communication
6 transmitted by telephone, telegraph, radio, or other device between two or
7 more individuals between points within or without the state by any device
8 electronic or otherwise designed to record and/or transmit said
communication regardless how such device is powered or actuated, without
first obtaining the consent of all the participants in the communication.

9 222. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
10 third-party websites allowed it to intercept or record the contents of Plaintiffs Mary Thew’s and Lisa
11 Evans’s and Washington Subclass Members’ private communications with third-party websites.

12 223. Without Plaintiffs Mary Thew’s and Lisa Evans’s, Washington Subclass Members’, or
13 third-party websites’ knowledge or consent, Meta intercepted the contents of Plaintiffs Mary Thew’s and
14 Lisa Evans’s and Washington Subclass Members’ private communications when they navigated to third-
15 party websites within Facebook’s in-app browser.

16 224. Plaintiffs Mary Thew’s and Lisa Evans’s and Washington Subclass Members’ private
17 communications were transmitted to third-party websites via a device.

18 225. Meta contemporaneously intercepted the contents of Plaintiffs Mary Thew’s and Lisa
19 Evans’s and Washington Subclass Members’ private communications while they were in transit and
20 without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such
21 private conversations and activities when users visit external third-party websites from within the
22 Facebook app.

23 226. Meta intentionally used a device—the JavaScript code it injected into third-party
24 websites—designed as a means of intercepting and acquiring the contents of Plaintiffs Mary Thew’s and
25 Lisa Evans’s and Washington Subclass Members’ private communications, in violation of Washington
26 Revised Code Annotated § 9.73.030(1).

1 227. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members were unaware
2 that Facebook was intercepting its users' private communications and tracking their communications and
3 interactions with third-party websites.

4 228. Meta's conduct was intentional in that it purposefully installed code which allows it to
5 intercept and learn the content of its users' communications and other browsing activities that would
6 otherwise be unavailable to Meta.

7 229. The information Meta intercepted while Plaintiffs Mary Thew and Lisa Evans and
8 Washington Subclass Members were using the Facebook in-app browser includes personally identifiable
9 information and other highly specific information and communications, including, without limitation,
10 every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries
11 (including passwords and credit card information), and how much time a user spent on which websites.

12 230. Meta intentionally intercepted Plaintiffs Mary Thew's and Lisa Evans's and Washington
13 Subclass Members' information in transit. Meta intercepted their website communications whenever they
14 used Facebook's in-app browser to communicate with third-party websites using the JavaScript code
15 inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an
16 information field or text box), URL visited, and other private communication. These communications
17 constitute private communications and were contemporaneously copied by Meta in real time.

18 231. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members intended and
19 believed that the information they provided to third-party websites while using Facebook's in-app
20 browser would remain private and would not be transmitted to Meta.

21 232. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members have
22 experienced damage and loss by reason of these violations, including but not limited to, violation of the
23 right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

24 233. As a result of the above violations and pursuant to Washington Revised Code Annotated
25 § 9.73.060, Meta is liable to the Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members
26 for actual damages, liquidated damages computed at the rate of \$100 a day for each violation. Plaintiffs
27 Mary Thew and Lisa Evans further request, as provided under Washington Revised Code Annotated §
28 9.73.060, reasonable attorneys' fees and costs of suit.

NINTH CLAIM FOR RELIEF

VIOLATION OF THE MISSOURI WIRETAP ACT

Mo. Stat. § 542.400 *et seq.*

(On Behalf of the Missouri Subclass)

234. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

235. Plaintiff Raven Johnson brings this count individually and on behalf of the Missouri Subclass.

236. The Missouri Wiretap Act is codified at Missouri Annotated Statutes §§ 542.400–542.424. Missouri Annotated Statutes § 542.402 punishes, in pertinent part, any person who “[k]nowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire communication.”

237. “Person” includes “any individual, partnership, association, joint stock company, trust, or corporation.” *Id.* § 542.400(9).

238. Defendant, as a corporation, is a “person” under the Missouri Act.

239. “Intercept” is defined as the “acquisition of the contents of any wire communication through the use of any electronic or mechanical device.” *Id.* § 542.400(6).

240. “Contents” is defined as either “any information concerning the identity of the parties, the substance, purport, or meaning of that communication.” *Id.* § 542.400(3).

241. “Wire communication” is defined as “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications.” *Id.* § 542.400(12).

242. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiff Raven Johnson’s and Missouri Subclass Members’ wire communications with third-party websites.

1 243. Without Plaintiff Raven Johnson’s, Missouri Subclass Members’, or third-party websites’
2 knowledge or consent, Meta intercepted the contents of Plaintiff Raven Johnson’s and Missouri Subclass
3 Members’ wire communications when they navigated to third-party websites within Facebook’s in-app
4 browser.

5 244. Meta contemporaneously intercepted the contents of Plaintiff Raven Johnson’s and
6 Missouri Subclass Members’ wire communications while they were in transit and without authorization.
7 Meta failed to disclose that it was intercepting and tracking the contents of such private conversations
8 and activities when users visit external third-party websites from within the Facebook app.

9 245. Meta intentionally used an electronic or mechanical device—the JavaScript code it
10 injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff
11 Raven Johnson’s and Missouri Subclass Members’ wire communications, in violation of the Missouri
12 Wiretap Act.

13 246. Plaintiff Raven Johnson and Missouri Subclass Members were unaware that Facebook
14 was intercepting its users’ wire communications and tracking their communications and interactions with
15 third-party websites.

16 247. Meta’s conduct was intentional in that it purposefully installed code which allows it to
17 intercept and learn the content of its users’ communications and other browsing activities that would
18 otherwise be unavailable to Meta.

19 248. The information Meta intercepted while Plaintiff Raven Johnson and Missouri Subclass
20 Members were using the Facebook in-app browser includes personally identifiable information and other
21 highly specific information and communications, including, without limitation, every button, keystroke
22 and link a user taps, whether the user has taken any screenshots, text entries (including passwords and
23 credit card information), and how much time a user spent on which websites.

24 249. Plaintiff Raven Johnson and Missouri Subclass Members intended and believed that the
25 information they provided to third-party websites while using Facebook’s in-app browser would remain
26 private and would not be transmitted to Meta.

27 250. Meta intentionally intercepted Plaintiff Raven Johnson’s and Missouri Subclass
28 Members’ information in transit. Meta intercepted their website communications whenever they used

1 Facebook’s in-app browser to communicate with third-party websites using the JavaScript code inserted
2 by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information
3 field or text box), URL visited, and other electronic communication. These website communications
4 constitute wire communications and were contemporaneously copied by Meta in real time.

5 251. Plaintiff Raven Johnson and Missouri Subclass Members have experienced damage and
6 loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless
7 restrained and enjoined, Meta will continue to commit such acts.

8 252. As a result of the above violations and pursuant to Missouri Annotated Statutes § 542.418,
9 Meta is liable to the Plaintiff Raven Johnson and Missouri Subclass Members for the greater of their
10 actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of
11 violation, or \$10,000.

12 253. Plaintiff Raven Johnson further requests, as provided under Missouri Annotated Statutes
13 § 542.418, reasonable attorneys’ fees and costs of suit, and punitive damages in an amount to be
14 determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

15 **TENTH CLAIM FOR RELIEF**

16 **VIOLATION OF THE MASSACHUSETTS WIRETAP STATUTE**

17 **Mass. Gen. Laws Ann. 272 § 99**

18 **(On Behalf of the Massachusetts Subclass)**

19 254. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

20 255. Plaintiff Ed Rennie brings this count individually and on behalf of the Massachusetts
21 Subclass.

22 256. Massachusetts bars the surreptitious interception and recording of private
23 communications. Mass Gen. Laws Ann. 272 § 99.

24 257. It is a violation of Massachusetts law for any person to willfully commit an interception,
25 attempt to commit an interception, or procure any other person to commit an interception or attempt to
26 commit an interception of any wire communication. *Id.* § 99(C)(1).

27 ///

28 ///

1 258. Further, it is a violation for any person to willfully use, or attempt to use, “the contents
2 of any wire . . . communication, knowing that the information was obtained through interception.” *Id.* §
3 99(C)(3)(b).

4 259. “Person” includes “any individual, partnership, association, joint stock company, trust,
5 or corporation.” *Id.* § 99(B)(13).

6 260. Defendant, as a corporation, is a “person” under Massachusetts law.

7 261. “Interception” is defined as “to secretly record . . . the contents of any wire . . .
8 communications through the use of any intercepting device by any person other than a person given prior
9 authority by all parties to such communication.” *Id.* § 99(B)(4).

10 262. “Wire communication” is defined as “any communication made in whole or in part
11 through the use of facilities for the transmission of communications by the aid of wire, cable, or other
12 like connection between the point of origin and the point of reception.” *Id.* § 99(B)(1).

13 263. “Contents” is defined as either “any information concerning the identity of the parties
14 to such communication,” or any information concerning the “existence, contents, substance, purport, or
15 meaning of that communication.” *Id.* § 99(B)(5).

16 264. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
17 third-party websites allowed it to intercept the contents of Plaintiff Ed Rennie’s and Massachusetts
18 Subclass Members’ wire communications with third-party websites.

19 265. Without Plaintiff Ed Rennie’s, Massachusetts Subclass Members’, or third-party
20 websites’ knowledge or consent, Meta intercepted the contents of Plaintiff Ed Rennie’s and
21 Massachusetts Subclass Members’ wire communications when they navigated to third-party websites
22 within Facebook’s in-app browser.

23 266. Meta contemporaneously intercepted the contents of Plaintiff Ed Rennie’s and
24 Massachusetts Subclass Members’ wire communications while they were in transit and without
25 authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private
26 conversations and activities when users visit external third-party websites from within the Facebook app.
27
28

1 267. Meta intentionally used an electronic or mechanical device—the JavaScript code it
2 injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff Ed
3 Rennie’s and Massachusetts Subclass Members’ wire communications, in violation of Massachusetts
4 law.

5 268. Plaintiff Ed Rennie and Massachusetts Subclass Members were unaware that Facebook
6 was intercepting its users’ wire communications and tracking their communications and interactions with
7 third-party websites.

8 269. Meta’s conduct was intentional in that it purposefully installed code which allows it to
9 intercept and learn the content of its users’ communications and other browsing activities that would
10 otherwise be unavailable to Meta.

11 270. The information Meta intercepted while Plaintiff Ed Rennie and Massachusetts Subclass
12 Members were using the Facebook in-app browser includes personally identifiable information and other
13 highly specific information and communications, including, without limitation, every button, keystroke
14 and link a user taps, whether the user has taken any screenshots, text entries (including passwords and
15 credit card information), and how much time a user spent on which websites.

16 271. Plaintiff Ed Rennie and Massachusetts Subclass Members intended and believed that the
17 information they provided to third-party websites while using Facebook’s in-app browser would remain
18 private and would not be transmitted to Meta.

19 272. Meta intentionally intercepted Plaintiff Ed Rennie’s and Massachusetts Subclass
20 Members’ information in transit. Meta intercepted Plaintiff Ed Rennie’s and Massachusetts Subclass
21 Members’ website communications whenever they used Facebook’s in-app browser to communicate with
22 third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click,
23 keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic
24 communication. These website communications constitute wire communications and were
25 contemporaneously copied by Meta in real time.

26 273. Plaintiff Ed Rennie and Massachusetts Subclass Members have experienced damage and
27 loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless
28 restrained and enjoined, Meta will continue to commit such acts.

1 274. As a result of the above violations and pursuant to Massachusetts General Laws Annotated
2 Chapter 272, § 99(Q), Meta is liable to the Plaintiff Ed Rennie and Massachusetts Subclass Members for
3 the greater of their actual damages, but not less than liquidated damages computed at the rate of \$100 a
4 day for each day of violation, or \$1,000.

5 275. Plaintiff Ed Rennie further requests, as provided under Massachusetts General Laws
6 Annotated Chapter 272, § 99(Q), reasonable attorneys’ fees and costs of suit, and punitive damages in an
7 amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

8 **ELEVENTH CLAIM FOR RELIEF**

9 **VIOLATION OF THE MARYLAND WIRETAP ACT**
10 **Md. Cts. & Jud. Pro. § 10-401 *et seq.***
11 **(On Behalf of the Maryland Subclass)**

12 276. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

13 277. Plaintiff Teia Pittman brings this count individually and on behalf of the Maryland
14 Subclass.

15 278. The Maryland Wiretap Act bars the surreptitious interception and recording of private
16 communications. Md. Cts. & Jud. Pro. § 10-402.

17 279. It is a violation of the Maryland Wiretap Act for any person to “[w]illfully intercept,
18 endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or
19 electronic communication.” *Id.* § 10-402(a)(1).

20 280. Further, it is a violation for any person to willfully use, or endeavor to use, “the contents
21 of any wire, oral, or electronic communication, knowing or having reason to know that the information
22 was obtained through the interception of a wire, oral, or electronic communication.” *Id.* § 10-402(a)(3).

23 281. “Person” includes “any individual, partnership, association, joint stock company, trust, or
24 corporation.” *Id.* § 10-401(14).

25 282. Defendant, as a corporation, is a “person” under the Maryland Wiretap Act.

26 283. “Intercept” is defined as the “acquisition of the contents of any wire, electronic, or oral
27 communication through the use of any electronic, mechanical, or other device.” *Id.* § 10-401(10).

1 284. “Contents” is defined as either “any information concerning the identity of the parties to
2 such communication,” or any information concerning the “existence, contents, substance, purport, or
3 meaning of that communication.” *Id.* § 10-401(4).

4 285. “Electronic communication” is defined as “any transfer of signs, signals, writing, images,
5 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
6 electromagnetic, photoelectronic, or photooptical system.” *Id.* § 10-401(5)(i).

7 286. At all relevant times, Meta’s business practice of injecting its unique JavaScript code into
8 third-party websites allowed it to intercept the contents of Plaintiff Teia Pittman’s and Maryland Subclass
9 Members’ electronic communications with third-party websites.

10 287. Without Plaintiff Teia Pittman’s, Maryland Subclass Members’, or third-party websites’
11 knowledge or consent, Meta intercepted the contents of Plaintiff Teia Pittman’s and Maryland Subclass
12 Members’ electronic communications when they navigated to third-party websites within Facebook’s in-
13 app browser.

14 288. Meta contemporaneously intercepted the contents of Plaintiff Teia Pittman’s and
15 Maryland Subclass Members’ electronic communications while they were in transit and without
16 authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private
17 conversations and activities when users visit external third-party websites from within the Facebook app.

18 289. Meta intentionally used an electronic or mechanical device—the JavaScript code it
19 injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff Teia
20 Pittman’s and Maryland Subclass Members’ electronic communications, in violation of the Maryland
21 Wiretap Act.

22 290. Plaintiff Teia Pittman and Maryland Subclass Members were unaware that Facebook was
23 intercepting its users’ electronic communications and tracking their communications and interactions
24 with third-party websites.

25 291. Meta’s conduct was intentional in that it purposefully installed code which allows it to
26 intercept and learn the content of its users’ communications and other browsing activities that would
27 otherwise be unavailable to Meta.
28

1 292. The information Meta intercepted while Plaintiff Teia Pittman and Maryland Subclass
2 Members were using the Facebook in-app browser includes personally identifiable information and other
3 highly specific information and communications, including, without limitation, every button, keystroke
4 and link a user taps, whether the user has taken any screenshots, text entries (including passwords and
5 credit card information), and how much time a user spent on which websites.

6 293. Plaintiff Teia Pittman and Maryland Subclass Member intended and believed that the
7 information they provided to third-party websites while using Facebook’s in-app browser would remain
8 private and would not be transmitted to Meta.

9 294. Meta intentionally intercepted Plaintiff Teia Pittman’s and Maryland Subclass Members’
10 information in transit. Meta intercepted their website communications whenever they used Facebook’s
11 in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta,
12 including every mouse movement, click, keystroke (e.g., text being entered into an information field or
13 text box), URL visited, and other electronic communication. These website communications constitute
14 electronic communications and were contemporaneously copied by Meta in real time.

15 295. Plaintiff Teia Pittman and Maryland Subclass Member have experienced damage and loss
16 by reason of these violations, including but not limited to, violation of the right to privacy. Unless
17 restrained and enjoined, Meta will continue to commit such acts.

18 296. As a result of the above violations and pursuant to Maryland Code Annotated, Courts &
19 Judicial Proceedings § 10-410, Meta is liable to Plaintiff Teia Pittman and Maryland Subclass Members
20 for the greater of their actual damages, but not less than liquidated damages computed at the rate of \$100
21 a day for each day of violation, or \$1,000.

22 297. Plaintiff Teia Pittman further requests, as provided under Maryland Code Annotated,
23 Courts & Judicial Proceedings § 10-410, reasonable attorneys’ fees and costs of suit, and punitive
24 damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct
25 by Meta.

26 ///

27 ///

TWELFTH CLAIM FOR RELIEF

**INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Class or, Alternatively, Each State Subclass)**

1
2
3
4 298. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and
5 bring this count individually and on behalf of the Class or, alternatively, each state subclass.

6 299. Plaintiffs and Class Members had a reasonable expectation of privacy when
7 communicating with third-party websites, and, as a result of Meta’s actions, they have suffered harm and
8 injury, including from the invasion of their privacy rights.

9 300. By intercepting Plaintiffs’ and Class Members’ wire and electronic communications on
10 the internet, Meta intentionally intruded upon their solitude or seclusion.

11 301. Meta’s intentional intrusion on Plaintiffs’ and Class Members’ solitude or seclusion is
12 highly offensive to a reasonable person, especially considering the extremely personal, sensitive, and
13 confidential information and data that Meta monitored, intercepted, transmitted and recorded in spite of
14 Plaintiffs’ and Class Members’ known, expressed preference not to have this information tracked.

15 302. Meta’s conduct infringed Plaintiffs’ and Class Members’ privacy interests in, among other
16 things, (1) preventing the dissemination and/or misuse of their sensitive, confidential personally
17 identifiable information; (2) maintaining control over the type of information that Meta tracks and/or
18 records; and (3) making personal decisions and/or conducting personal activities without observation,
19 intrusion, or interference, including being able visit and interact with various internet sites without that
20 information being intercepted by Meta without Plaintiffs’ and Class Members’ knowledge or consent.

21 303. Plaintiffs and Class Members have been damaged as a direct and proximate result of
22 Meta’s invasion of their privacy rights and are entitled to just compensation, including monetary
23 damages, in an amount to be determined at trial.

THIRTEENTH CLAIM FOR RELIEF

**INVASION OF PRIVACY (PUBLICATION OF PRIVATE FACTS)
(On Behalf of the Class or, Alternatively, Each State Subclass)**

24
25
26 304. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring
27 this count individually and on behalf of the Class or, alternatively, each state subclass.
28

1 305. Plaintiffs' and Class Members' personal information, including their Internet
2 communications and sensitive data, are private facts that Meta acquired without the knowledge or consent
3 of Plaintiffs and Class Members.

4 306. Meta gave publicity to Plaintiffs' and Class Members' private facts and the content of
5 their Internet communications by sharing and selling them to its advertising partners. Many of those
6 companies have business models predicated on building massive databases of individual consumer
7 profiles from which to sell, broker or display targeted advertising.

8 307. Plaintiffs and Class Members had no knowledge that Meta was collecting, selling, and
9 publishing to such third parties their private browsing activities and overriding their privacy settings
10 because they had opted out of such tracking and did not otherwise consent to being tracked on third-party
11 websites.

12 308. Meta's surreptitious tracking and commoditization of Plaintiffs' and Class Members'
13 personal information would be highly offensive to a reasonable person, particularly because Plaintiffs
14 chose to opt out of tracking to prevent Meta or its advertising partners from viewing, acquiring, and using
15 their personal information.

16 309. In disseminating Plaintiffs' and Class Members' personal information without their
17 consent in the manner described above, Meta acted with oppression, fraud, or malice.

18 310. Plaintiffs and Class Members have been damaged by the publication of their private
19 information and are entitled to just compensation in the form of actual damages, general damages, unjust
20 enrichment, nominal damages, and punitive damages.

21
22 **FOURTEENTH CLAIM FOR RELIEF**

23 **UNJUST ENRICHMENT**

24 **(On Behalf of the Class or, Alternatively, Each State Subclass)**

25 311. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and
26 bring this count individually and on behalf of the Class or, alternatively, each state Subclass under
27 universal principles in equity.

1 users' private communications and track users' internet activity on third-party websites in a manner that
2 is inconsistent with their privacy settings or preferences;

3 E. Award Plaintiffs and Class Members their reasonable costs and expenses incurred
4 in this action, including counsel fees and expert fees; and

5 F. Grant such other and further relief as the Court deems appropriate.

6 **DEMAND FOR JURY TRIAL**

7 Plaintiffs hereby demand a trial by jury for all claims so triable.

8
9 Dated: February 6, 2023

Respectfully submitted,

10 By: /s/ Adam E. Polk

11 Adam E. Polk (SBN 273000)

12 Simon S. Grille (SBN 294914)

13 Kimberly Macey (SBN 342019)

14 Reid Gaa (SBN 330141)

GIRARD SHARP LLP

601 California Street, Suite 1400

San Francisco, CA 94108

Telephone: (415) 981-4800

apolk@girardsharp.com

sgrille@girardsharp.com

kmacey@girardsharp.com

rgaa@girardsharp.com

19 Gary M. Klinger (*pro hac vice* forthcoming)

20 Nick Suci (*pro hac vice* forthcoming)

21 Alexandra M. Honeycutt (*pro hac vice* forthcoming)

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

22 227 W. Monroe Street, Suite 2100

23 Chicago, IL 60606

Telephone: (866) 252-0878

24 gklinger@milberg.com

25 nsuciu@milberg.com

ahoneycutt@milberg.com

26 John J. Nelson (SBN 317598)

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@milberg.com

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