Adam E. Polk (SBN 273000)
Jordan Elias (SBN 228731)
Simon S. Grille (SBN 294914)
Kimberly Macey (SBN 342019)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

GABRIELE WILLIS and KERREISHA DAVIS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No.

JURY DEMAND

CLASS ACTION COMPLAINT FOR:

1. Violation of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*;
2. Violation of the Invasion of Privacy Act, Cal. Penal Code § 630 *et seq.*;
3. Invasion of Privacy (Intrusion Upon Seclusion);
4. Violation of the Unfair Competition Law, Cal. Bus & Prof. Code § 17200 *et seq.*;
5. Unjust Enrichment.

Plaintiffs Gabriele Willis and Kerreisha Davis, on behalf of the Class defined below, bring this action against Meta Platforms, Inc. and allege as follows:

NATURE OF THE ACTION

1. This class action seeks relief for all persons who used Meta's Facebook app and whose private browsing activity and communications were intercepted, monitored and recorded while using Facebook's in-app browser without their consent.

2. Beginning in April 2021, Apple's iOS 14.5 update required Meta to obtain its users' consent before tracking their internet activity on apps and third-party websites. As a result, Meta lost access to its primary stream of revenue, derived from the user data it extracted from this surveillance. Now, even when users do not consent to being tracked, Meta tracks Facebook users' online activity and communications with external third-party websites by injecting JavaScript code into those sites. When users click on a link within the Facebook app, Meta automatically directs them to the in-app browser it is monitoring instead of the smartphone's default browser, without telling users that this is happening or they are being tracked. The user information Meta intercepts, monitors and records includes personally identifiable information, private health details, text entries, and other sensitive confidential facts.

3. Meta's undisclosed tracking of citizens' browsing activity and communications violates federal and state privacy and other laws, entitling Plaintiffs and Class members to damages. Plaintiffs also seek through this action to put a stop to Meta's undisclosed tracking of its user base.

JURISDICTION AND VENUE

4. The Court has personal jurisdiction over Defendant Meta Platforms, Inc. because it is headquartered in this District.

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises in part under federal law—the Wiretap Act, 18 U.S.C. § 2510 *et seq*.—and pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, the amount in controversy exceeds $5 million (excluding interest and costs), and at least one Class member is a citizen of a state different from the state in which Meta is domiciled.

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

DIVISIONAL ASSIGNMENT

7. Pursuant to Civil Local Rule 3-2(c), a substantial part of the events giving rise to the claims brought in this Complaint occurred in San Mateo County, California. Consequently, this action should be assigned to the San Francisco Division or the Oakland Division.

PARTIES

8. Plaintiff Gabriele Willis is an adult citizen of the state of California who resides in El Cajon, California. Ms. Willis had an active Facebook account during the Class period. Ms. Willis did not consent to Facebook tracking her activity. Using the systematic process described below, Meta tracked and intercepted her specific electronic activity and private communications with external third-party websites without her knowledge or consent. Ms. Willis reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

9. Plaintiff Kerreisha Davis is an adult citizen of the state of Louisiana who resides in Monroe, Louisiana. Ms. Davis had an active Facebook account during the relevant time period. Ms. Davis did not consent to Facebook tracking her activity. Using the systematic process described below, Meta tracked and intercepted her specific electronic activity and private communications with external third-party websites without her knowledge or consent. Ms. Davis reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

10. Meta Platforms Inc., d/b/a as Meta, formerly known as Facebook, Inc., is a Delaware Corporation headquartered in Menlo Park, California.

FACTUAL ALLEGATIONS

A. Meta has a track record of pursuing profit at the expense of its users' privacy.

11. Meta is the owner and operator of, among other businesses, Facebook, a large social media platform.

12. Meta's core business entails collecting revenue for advertisements in conjunction with its data mining practices. Although Meta does not require Facebook members to pay a monetary subscription fee, membership is not actually free. Meta conditions the use of Facebook upon users disclosing sensitive and valuable personal information when they register, including birthdates and email addresses.

13. The personal information Meta collects has substantial economic value. One study valued users' web-browsing histories at $52 per year.

14. Meta primarily makes money by selling advertising space on its various social media and messaging platforms. Meta's business model is based on offering its services to billions of users and earning revenue from sales of digital ads that other businesses purchase from Meta to display to users of Facebook and other Meta properties on a targeted basis. Advertising sales accounted for 97% of Meta's 2021 revenue.

15. Meta's financial success is the result of connecting advertisers with its massive repository of personal data on users of its platforms. Meta maximizes its profits by targeting ads to individuals who its algorithms have determined may be personally interested in a certain advertised product or service. Meta thus collects extensive data about its users, continuously aggregates and analyzes this data, and deploys it to offer targeted advertising services.

16. This business model, which depends on access to detailed information about its users, has led Meta to violate its users' privacy rights over many years through its use of plug-ins, cookies, Facebook Beacon, the Facebook Like Button, Facebook Pixel, and other data mining tactics.

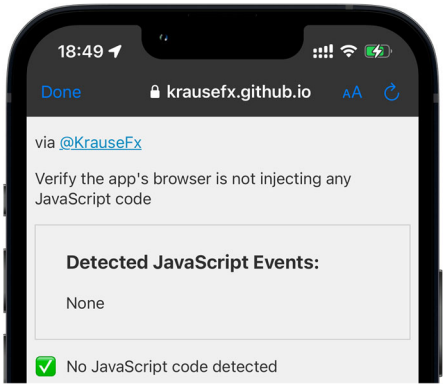
17. Meta has also shared its users' private messages and the details relating to their personal contacts without the users' consent. From 2010 to 2018, Facebook allowed more than 150 third parties, including Amazon, Microsoft, Netflix, and Spotify, to access this private information.

18. In 2019, Facebook agreed to pay a $5 billion penalty and submit to new restrictions and a modified corporate structure to settle Federal Trade Commission charges that Facebook violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.

B. Meta tracks its users without their knowledge or consent by manipulating third-party websites and injecting JavaScript into its in-app browsers.

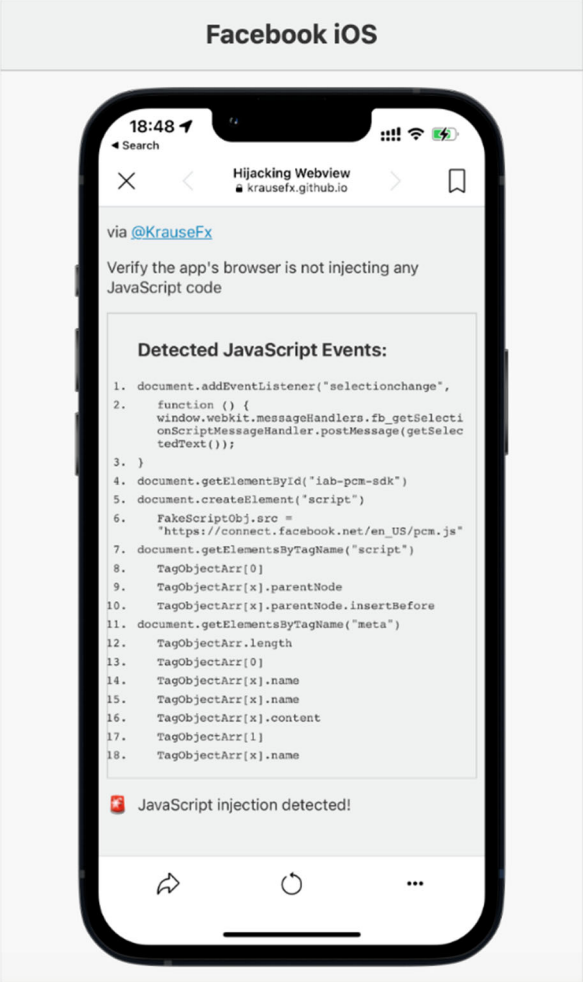
19. A recent report by Felix Krause, a data privacy researcher and former Google engineer, revealed that Meta has been injecting code into third-party websites, a practice that allows Meta to track users and intercept data that would otherwise be unavailable to it. For example, if a user accessed the same third-party website directly through their web browser, instead of Facebook's in-app browser, the user's browser would actively block and prevent Meta's ability to intercept and track the user's activity on the third-party website. But Meta tracks the same activity if the user engages on its in-app browser.

20. Krause helped develop www.InAppBrowser.com, a website that allows users to detect whether a particular in-app browser is injecting code into third-party websites. Figure 1 below shows what happens when a user clicks on a web link they received in the Telegram app, a messaging platform that does not inject JavaScript onto third-party websites but which openly prompts users to use its own in-app browser instead of a default browser:



(Figure 1.) As demonstrated by the image above, not all in-app browsers violate users' privacy rights or override their devices' privacy settings. Telegram, in other words, does not track users' activity on or communications with third-party web pages.

21. Compare that Telegram image and situation with Figure 2 below concerning the iOS Facebook app:



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

22. Krause's report, entitled "*iOS Privacy: Instagram and Facebook can Track Anything you do on any Website in their In-App Browser*," describes how Meta uses JavaScript to alter websites and override its users' default privacy settings by directing users to Facebook's in-app browser instead of their pre-programmed default web browser.[1]

23. Injecting JavaScript into the code of third-party websites can allow a malicious actor to intercept confidential information communicated to those sites:

[1] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last accessed Sept. 6, 2022).

> **What is a JavaScript Injection Attack?**
>
> A JavaScript injection attack is a type of attack in which a threat actor injects malicious code directly into the client-side JavaScript. This allows the threat actor to manipulate the website or web application and collect sensitive data, such as personally identifiable information (PII) or payment information.[2]

24. Meta now is using this coding tool to gain an advantage over its competitors and, in relation to iOS users, preserve its ability to intercept and track their communications. Meta inserts code to track its users' in-app browsing activity without their knowledge or consent, even when users have declined to "opt in" to Meta's tracking and set their devices to block third-party tracking cookies.

C. Meta intercepts and tracks its users' private interactions and communications with third-party websites, overriding users' privacy settings.

25. When a Meta user, while visiting the Facebook app, clicks on a link to an external website (e.g., from a friend's wall post on their profile), Meta *automatically* reroutes the user to its own in-app web browser instead of the users' built-in web browser (such as Apple's Safari app that is preloaded onto iPhones). As a result, third-party websites are rendered *inside* the app—enabling Meta "to monitor everything happening on external websites, without the consent [of] the user" or from the website itself.[3]

26. The Facebook app injects Meta's JavaScript code into every third-party website a user visits from within Facebook's in-app browser. This allows to Meta to intercept, monitor and record its users' interactions and communications with third parties, providing data to Meta that it aggregates, analyzes, and uses to boost its advertising revenue.

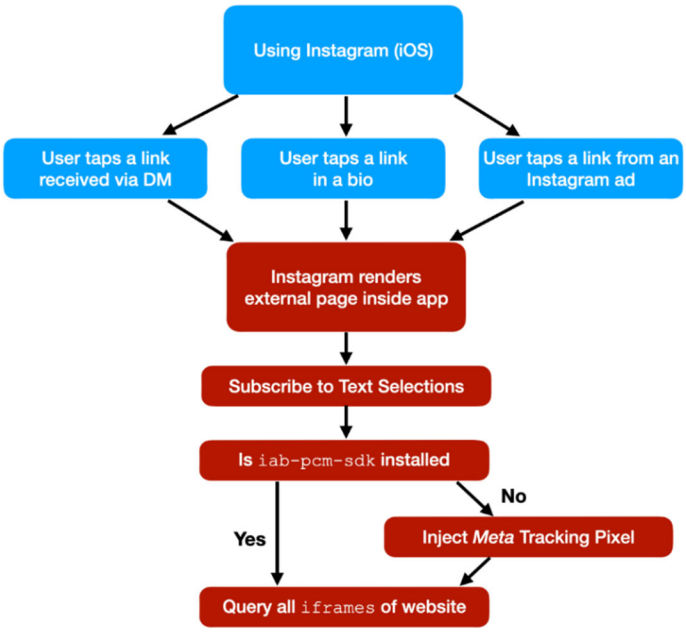
27. There was never any pop-up window or other prominent notice given to Facebook users of Meta's tracking practice. The relevant "Off-Facebook activity" settings tab within the Facebook app does not disclose the practice. At no point did Meta fairly or reasonably disclose to users its practice of intercepting, monitoring, and selling their activities and communications while using its in-app browser, even after they have opted out of being tracked.

---

[2] https://www.feroot.com/education-center/what-is-a-javascript-injection-attack/ (last accessed Sept. 6, 2022).

[3] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last accessed Sept. 6, 2022).

28. As demonstrated in Figure 3 below, this systematic process occurs whenever a user clicks on a link they received in their inbox (through the private messaging feature) or when they click on a link displayed on another Facebook account's "bio" or post. (While this flowchart refers to "Instagram," the same process occurs on Facebook.)



(Figure 3.) The image above depicts the systematic manner in which Meta injects JavaScript into external third-party webpages for the purpose of intercepting, tracking, monitoring, and collecting data about its users' interactions with external third-party webpages.

29. Though the process shown in Figure 3, Meta is able to surveil and extract details about its users' text selections and other communications with third-party websites:

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

[4] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last accessed Sept. 6, 2022).

30. Stated less technically, by running custom scripts on third-party websites, Meta can and does intercept, view, monitor, and record all user interactions—every button and link they tap, as well as text selections, screenshots, form inputs (including passwords, addresses, and payment card numbers), other personally identifiable information, protected health details, and other private and confidential communications and data.

D. Further details on Meta's in-app tracking process and business.

31. Meta acknowledged that it tracks Facebook users' in-app browsing activity within hours after the practice was reported to Meta in connection with its "Bug Bounty Program." Meta later stated that the data obtained through this practice assists in "aggregating events" before such "events" are deployed in targeted advertising.

32. In contrast, Meta has not added this JavaScript code to the in-app browser of another of its properties, WhatsApp. This disparity in business conduct confirms that injecting JavaScript is not necessary for users' security or for any other legitimate purpose. Instead, this practice deployed on Facebook serves only to benefit Meta and increase its revenue from ad impressions sold for display to Facebook users.

33. Meta's injection of JavaScript coincides with recent privacy updates for iPhones and other iOS devices. In 2020, Apple announced that beginning in 2021, it would change how its iOS mobile operating systems handle users' privacy preferences, by requiring apps to obtain users' affirmative consent to being tracked before doing so. After this Apple announcement, Meta began "waging a public relations effort to attack Apple ahead of new iOS data privacy changes that would make it harder for advertisers to track users, in a possible sign of just how much the social network views the move as a threat to its core business."[5]

34. Facebook held press conferences and ran advertisements critical of Apple's decision to require affirmative user consent to being tracked: "In ads featured in The New York Times, Wall Street Journal and Washington Post, Facebook slammed Apple's upcoming requirement for users to give

[5] https://edition.cnn.com/2020/12/16/tech/facebook-apple-ios-privacy-rules/index.html (last accessed Sept. 6, 2022).

explicit permission for apps to track them across the internet. Facebook said the move could be 'devastating' to millions of small businesses that advertise on its platform."[6] WhatsApp likewise "criticized Apple over its move to display a summary of an app's privacy practices before a user downloads it from the App Store, almost like a nutrition label for data collection."[7]

35. In response, Apple stated in part, "We believe that this is a simple matter of standing up for our users. Users should know when their data is being collected and shared across other apps and websites—and they should have the choice to allow that or not."[8] Apple also noted that "App Tracking Transparency in iOS 14 does not require Facebook to change its approach to tracking users and creating targeted advertising, it simply requires they give users a choice."[9]

36. As of May 2021, shortly after Apple introduced iOS 14.5, 96% of Apple users in the United States had *not* consented to being tracked by apps on their iPhone. And, "[a]ccording to [Meta], empowering Apple's users to opt out of tracking cost the company $10,000,000,000 in the first year, with more losses to come after that."[10] Hence "[w]ith web browsers and iOS adding more and more privacy controls into the users' hands, it becomes clear why [Meta] is interested in monitoring all web traffic of external websites."[11]

37. Meta began showing its users a screen that described the consequences of iOS 14.5 and the long-term impact it could have on Meta's ability to provide apps and software. Through these and related communications strategies, Meta was "threatening that users will need to pay for their services. But only if users don't allow [Meta] to track them from app to app after installing iOS 14.5."[12]

---

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] https://www.eff.org/deeplinks/2022/06/facebook-says-apple-too-powerful-theyre-right (last accessed Aug. 24, 2022).

[11] https://krausefx.com/blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser (last accessed Sept. 6, 2022).

[12] https://www.imore.com/facebook-and-instagram-threaten-charge-access-ios-145-unless-you-give-it-your-data (accessed Aug.24, 2022).

E. Meta's conduct harmed Plaintiffs and Class members.

38. Meta does not inform Facebook users that clicking on links to third-party websites from within Facebook will automatically send the user to Facebook's in-app browser, as opposed to the user's default web browser, or that Meta will monitor the user's activity and communications while on those sites. Because nothing alerts users as to these facts, they are unaware of the tracking; most do not even realize they are browsing the third-party website from within Facebook's in-app browser. Therefore users freely engage with these sites, sharing all manner of personal facts and preferences, without having reason to know they are being tracked or are actually still within Facebook's app.

39. Even users who may realize they are visiting websites from within Facebook's in-app browser do not realize that this activity overrides their privacy settings and enables Meta to track, intercept, and monitor their activities on the websites as a consequence of Meta's undisclosed injection of code. Meta's JavaScript injection cannot be detected by a lay person, and a website when viewed on Facebook's in-app browser functions no differently than otherwise.

40. Users also reasonably expect that their communications with external third-party websites are not being intercepted and tracked because their default browser disables and blocks third-party cookies. Meta does not inform users that its in-app browser differs from Safari and other default browsers in regard to such privacy settings.

41. Moreover, Meta fails to disclose the consequences of browsing, navigating, and communicating with third-party websites from within Facebook's in-app browser—namely, that doing so overrides their default browser's privacy settings, which users rely on to block and prevent tracking. Similarly, Meta conceals the fact that it injects JavaScript that alters external third-party websites so that it can intercept, track, and record data that it otherwise could not access.

42. Plaintiffs reasonably believed that their communications and interactions with third-party websites were confidential—solely between themselves and external websites. Had Plaintiffs known that Meta could and would use its in-app browser to overcome Plaintiffs' default browser settings and override their privacy choices, Plaintiffs would have avoided navigating to third-party websites from within Facebook. Instead, they would have copied and pasted links into their standard browser to avoid being tracked, and ensured that their communications with third-party websites were made outside of

Facebook's in-app browser, particularly when the communications involved sensitive or other personally identifiable information, such as private health information and other confidential facts.

CLASS ACTION ALLEGATIONS

43. Plaintiffs bring this lawsuit under Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3) as representatives of the following Class and constituent Subclasses:

> **Class:** All persons in the United States with active Facebook accounts who visited a third-party external website on Facebook's in-app browser during the Class Period.
>
> **California Subclass:** All persons with active Facebook accounts who visited a third-party external website on Facebook's in-app browser during the Class Period in California.

Plaintiffs reserve the right to modify these definitions and/or to propose additional subclasses as appropriate based on further investigation and discovery.

44. The "Class Period" is the time period beginning on the date that Meta began implementing on Facebook the practices described in the Complaint, and ending on the date of entry of judgement.

45. Meta and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling are excluded from the Class. Additionally, Facebook users who assented to Facebook tracking their activity by tapping "yes" upon Apple's launch of iOS 14.5 are excluded from the Class. Also excluded are persons employed by counsel in this action and any judge to whom this case is assigned, his or her spouse and immediate family members, and members of the judge's staff.

46. Numerosity. The members of the Class are so numerous that joinder of all members would be impracticable. The exact number of Class members is unknown to Plaintiffs at this time, but it is estimated to number in the millions. The identity of Class members is readily ascertainable from Meta's records.

47. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used Meta's platforms to view third-party websites that were embedded as URLs within the respective Meta applications, and all Class members were similarly affected by Meta's wrongful conduct related thereto.

48. Adequacy. Plaintiffs will fairly and adequately represent the interests of the Class members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the Class members. Plaintiffs are represented by attorneys experienced in the prosecution of class action litigation generally, and in digital privacy litigation specifically, who will vigorously prosecute this action on behalf of the Class.

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

a. Whether Meta intentionally tapped the lines of electronic communication between Class members and third-party websites they visited;

b. Whether Facebook's in-app web browser surreptitiously records Class members' private communications and personally identifiable information;

c. Whether Class members have a reasonable expectation of privacy with respect to such information;

d. Whether Meta's invasion of Class members' privacy rights is highly offensive to a reasonable person;

e. Whether Meta violated state and federal laws by tracking Internet use and intercepting its users' communications when they visited third-party websites;

f. Whether Meta's conduct resulted in a breach of confidentiality;

g. Whether Meta's statements and omissions misled Class members as to the level of control they had over their private communications derived from activity on the Facebook app; and

h. Whether Class members are entitled to damages, restitution and/or injunctive relief.

50. Superiority. A class action will permit numerous similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication of evidence, effort, or expense. A class action will provide injured persons a method for obtaining redress

on claims that could not practicably be pursued individually. Plaintiffs know of no manageability or other issue that would preclude maintenance of this case as a class action.

51. Rule 23(b)(1) and (b)(2) Certification. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Meta;
- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impeded their ability to protect their interests; and
- Meta has acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole.

FIRST CLAIM FOR RELIEF

VIOLATION OF THE WIRETAP ACT
18 U.S.C. § 2510 *et seq*.
(On Behalf of the Class)

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

53. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986, prohibits the intentional interception of any wire, oral, or electronic communication.

54. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

55. Without Plaintiffs', Class members', or third-party websites' knowledge or consent, Meta intercepted the contents of their electronic communications when they navigated from Facebook to third-party websites.

56. Meta intentionally used technology—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiffs' and Class members' electronic communications, in violation of the Wiretap Act.

57. Plaintiffs, Class members, and operators of third-party websites were unaware that Facebook was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites.

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

SECOND CLAIM FOR RELIEF

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

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

60. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630-638. The Act contains the following statement of purpose:

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

Cal. Penal Code § 630.

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

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or

> who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

62. At all relevant times, Meta's business practice of injecting JavaScript allowed it to access, intercept, learn the contents of and collect Plaintiffs' and Class members' personally identifiable information and other data, including information concerning their interactions with third-party websites, even when Plaintiffs' and Class members' default internet browsers and devices were set to block such actions.

63. Plaintiffs, and each Class Member, during one or more of their interactions on the internet during the Class period, communicated with one or more third-party websites owned by entities based in California, or with one or more entities whose servers were located in California. Communications from the California web-based entities to Plaintiffs and Class members, and from Plaintiffs and Class members to the California web-based entities, were sent to California.

64. Plaintiffs and Class members did not consent to any of Meta's actions in intercepting, reading, and learning the contents of their communications with such California-based entities. Meta read and learned the contents of Plaintiffs and Class members' communications in transit and in an unauthorized manner. Meta failed to disclose that it was intercepting, tracking and learning the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

65. Meta's conduct was intentional in that it purposefully installed code which allows it to eavesdrop and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta without engaging in this practice. Meta directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiffs, Class members and California-based web entities.

66. The information Meta intercepts while Plaintiffs and Class members are using its in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the

user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on the website.

67. Plaintiffs and Class members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

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

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

THIRD CLAIM FOR RELIEF

INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Class)

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

71. Plaintiffs and Class members had a reasonable expectation of privacy when communicating with third-party website, and, as a result of Meta's actions, they have suffered harm and injury, including from the invasion of their privacy rights.

72. By intercepting Plaintiffs' and Class members' wire and electronic communications on the internet, Meta intentionally intruded upon their solitude or seclusion.

73. Meta's intentional intrusion on Plaintiffs' and Class members' solitude or seclusion is highly offensive to a reasonable person, especially considering the highly personal, sensitive, and confidential information and data that Meta monitored, intercepted, transmitted and recorded.

74. Meta's conduct infringed Plaintiffs' and Class members' privacy interests in, among other things, (1) preventing the dissemination and/or misuse of their sensitive, confidential personally

identifiable information; (2) maintaining control over the type of information that Meta tracks and/or records; and (3) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including being able visit and interact with various internet sites without that information being intercepted by Meta without Plaintiffs' and Class members' knowledge or consent.

75. Plaintiffs and Class members have been damaged as a direct and proximate result of Meta's invasion of their privacy rights and are entitled to just compensation, including monetary damages.

FOURTH CLAIM FOR RELIEF

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

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

77. By engaging in the acts and practices described herein, Meta has committed one or more acts of unfair competition within the meaning of the UCL, and as a result, Plaintiffs and the Class members have suffered injury in fact and lost money and/or property, namely, as described herein, the insertion of JavaScript on their devices and the invasion and lost value of their personally identifiable information and other data.

78. Meta's conduct violates federal and state statutes and, therefore, the unlawful prong of the UCL. Further, Meta's conduct is substantially unfair, predatory and contrary to California's legislatively declared public policy in favor of protecting the privacy and security of personal confidential information.

79. Plaintiffs interacted with various third-party websites reasonably believing that their browsing activities—and any facts and information communicated to third-party websites—were secure and confidential (i.e., solely between themselves and the third-party website). In actuality, without Plaintiffs' or Class members' knowledge or consent, Meta injected code into every web URL embedded within its Facebook app, which was capable of overriding security and privacy settings previously set by Plaintiffs and Class members. Through this conduct, Meta actively intercepted, viewed, and collected Plaintiffs' and Class members' personally identifiable information so that it could be used for advertising

and other purposes for Meta's financial benefit. The information and data Meta intercepted includes highly sensitive and valuable personal information, including but not limited to personally identifiable information, confidential medical information, and other privileged communications and facts.

80. There is no justification for Meta's conduct other than to increase, beyond what it would have otherwise realized, its profit from fees from third parties and the value of its information assets through the acquisition of Plaintiffs' and Class members' personal information. Meta's conduct lacks justification in that Meta has benefited from such conduct and practices while Plaintiffs and Class members have been misled as to the nature and integrity of Meta's services and have, in fact, suffered material disadvantage with regard to their interests in the privacy and confidentiality of their personal information. Meta's conduct offends public policy in California as embodied in the Consumers Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them safeguard their privacy interests, such as Cal. Civ. Code § 1798.80.

81. Meta's acts and practices were fraudulent in violation of the UCL because they were likely to, and did, in fact, mislead the members of the public to whom they were directed. Meta actively concealed its tracking practice at issue and had exclusive knowledge of it, creating a duty to disclose. Meta failed to disclose this practice and its disclosure would have been a material and important factor in Plaintiffs' and Class members' actions related to visiting third-party websites through Facebook's in-app browser or another browser. Meta's secret, undisclosed, and deceptive tracking practice to profit from Plaintiffs' and Class members' data caused the data to lose value. Had Plaintiffs and Class members known that Meta could and would use its in-app browser in the manner described, they would have avoided navigating to third-party websites from within Facebook, and instead would have copied and pasted links into their standard browser to avoid being tracked, thereby avoiding this injury.

82. Plaintiffs, on behalf of themselves and the Class, accordingly seek restitution, injunctive relief, and such other relief that is warranted under the UCL.

FIFTH CLAIM FOR RELIEF

UNJUST ENRICHMENT
(On Behalf of the Class)

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

84. Plaintiffs and Class members conferred benefits on Meta by using Facebook and as a result of Meta's receipt of their personal and confidential information, including through the tracking practices at issue in this case.

85. As set forth herein, Meta secretly intercepts, monitors, and records Facebook users' online activity and communications with external third-party websites by injecting code into those sites. When users click on a link within the Facebook app, Meta automatically directs them to the in-app browser that it is monitoring, rather than to their default browser, without telling the users this is happening or they are being tracked, even where users have not consented to being tracked and their other relevant settings would block such tracking.

86. Under these circumstances, equity and good conscience militate against permitting Meta to retain the profits and benefits from its wrongful conduct. They should accordingly be disgorged or placed in a constructive trust so that Plaintiffs and Class members can obtain restitution.

PRAYER FOR RELIEF

87. WHEREFORE, Plaintiffs, on behalf of themselves and the Class defined herein, respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs and their attorneys to represent the Class;

B. Award compensatory damages, including statutory damages where available, and/or restitution to Plaintiffs and the Class against Meta in an amount to be proven at trial, including interest thereon;

C. Permanently restrain Meta, and its officers, agents, servants, employees and attorneys, from injecting JavaScript onto its users' devices in a manner that allows Meta to intercept users' private communications and track users' internet activity on third-party websites in a manner that is inconsistent with their privacy settings;

D. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

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

DEMAND FOR JURY TRIAL

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

Dated: September 21, 2022

Respectfully submitted,

By: */s/ Adam E. Polk*

Adam E. Polk (SBN 273000)
Jordan Elias (SBN 228731)
Simon S. Grille (SBN 294914)
Kimberly Macey (SBN 342019)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com