BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ehorne@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEVIN ROSE, individually and on behalf of all others similarly situated, Plaintiff, v. META PLATFORMS, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

PAGE

Plaintiff Devin Rose ("Plaintiff") brings this action on behalf of himself and all others similarly situated against Meta Platforms, Inc. ("Meta" or "Defendant"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. When a user visits a website where one of Meta's tracking technologies is installed, Meta acquires certain browsing information of the user (*e.g.*, what webpages they visit that have embedded Meta's trackers, what items they search for, etc.) and their Facebook ID—an identifier that ties the user's browsing information to their Facebook profile.

2. For Android users, however, this is just the tip of the iceberg. As a breaking news report and study found,[1] between September 2024 and at least June 2, 2025, Meta was exploiting a communication channel—typically "used for making audio or video calls"—in the Android ecosystem to tie users' browsing information to their persistent Facebook and Instagram profiles, rendering that browsing information *completely non-anonymous and identifiable*. Thus, when an Android user with the Facebook or Instagram app installed on their phone visited a webpage where the Meta Tracking Pixel was installed, Meta linked the browsing information to the information on the Facebook and Instagram profiles, making such users non-anonymous and identifiable.

3. If it seems like technology should not work this way, that is a correct assumption. Defendant's conduct not only violates general Android security protocols like "sandboxing" (keeping app and website data separate) and browsers' Incognito Mode, but also *Google's own "security and privacy principles*."[2] The breach was so egregious, in fact, that Google and other web browser developers like Mozilla and DuckDuckGo are actively trying to mitigate these techniques.

4. Of course, Meta had every incentive to exploit typical Android communication capabilities. Meta traffics in amassing as much information about users as possible. The less anonymous users are, the more they can be targeted with advertisements on Facebook and Instagram,

[1] Dan Goodin, *Meta And Yandex Are De-Anonymizing Android Users' Web Browsing Identifiers*, ARSTECHNICA (June 3, 2025), https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/.

[2] *Id.*

and the more the opportunity to target such users will be worth to advertisers. So, by exploiting this channel, Meta rendered Android users completely de-anonymous and exponentially increased the value of the data it collects. However, Meta did this not only in violation of federal and California privacy laws, but without either users *or* websites' knowledge or consent.

5. Plaintiff Devin Rose is a California Android user with a Facebook and Instagram account who, like other members of the Classes, was affected by Meta's pervasive tracking practices. Plaintiff now bring this action to enforce his privacy rights and to seek damages for the harm Defendant caused him and others by the collection and sale of his personal information.

THE PARTIES

6. Plaintiff Devin Rose is a natural person and citizen of California, residing in Los Angeles County, California.

7. Defendant Meta Platforms, Inc. is a Delaware corporation with its principal place of business at 1 Meta Way, Menlo Park, California 94025.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

9. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in California.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District.

FACTUAL ALLEGATIONS

I. META'S ADVERTISING PLATFORM AND THE META PIXEL

11. Meta describes itself as a "real identity platform,"[3]

[3] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021), https://tinyurl.com/m5d2hmbv.

12. This means that users are allowed only one account and must share "the name they go by in everyday life."[4]

13. To that end, when creating an account, users must provide their first and last name, along with their e-mail address, birthday, and gender.[5]

14. Meta sells advertising space by highlighting its ability to target users.[6] Meta can target users so effectively because it surveils user activity both on and off its site.[7]This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behaviors," and "demographics."[8]

15. Meta compiles the information it collects into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[9]

16. Meta operates what is known in the ad-tech space as a "walled garden." "A walled garden is a closed platform where the publisher or technology provider controls access to hardware, applications, content, and user data. In this environment, all advertising activities—from ad buying and serving to measurement and reporting—take place exclusively within the platform's ecosystem."[10]

17. "Walled gardens emerged as a strategy by major tech companies such as Google, Meta, and Amazon to monetize their vast amounts of first-party data by charging advertisers for access. The combined ad revenue of these three companies exceeds the total ad revenue generated by all other ad tech firms."[11]

[4] META, COMMUNITY STANDARDS: ACCOUNT INTEGRITY AND AUTHENTIC IDENTITY, https://tinyurl.com/37rrzynp.

[5] META, SIGN UP, https://www.facebook.com/signup.

[6] META, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.

[7] META, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153.

[8] META, AUDIENCE AD TARGETING, https://www.facebook.com/business/ads/ad-targeting.

[9] META, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[10] WHAT IS A WALLED GARDEN?, Adjust, https://www.adjust.com/glossary/walled-garden/

[11] *Id.*

18. To put this another way, on a typical website, the website controls which advertisements are shown to which users and contracts with various third parties to access the website's data. By contrast, publishers who choose to advertise on Meta do not control "who sees the ads and how the data is used"—Meta does.[12] And while a company "can create a targeted ad campaign on Facebook, it cannot export user data for use on other platforms."[13]

19. The advantage of advertising on a Meta platform is that Facebook and Instagram users provide significant personal information to Meta—their names, their contact information, their interests, etc. This "provid[es] advertisers with detailed insights into user behavior, preferences, and demographics" and "enables highly precise targeting, allowing for personalized and relevant ad campaigns that resonate with the target audience,"[14] more so than an advertiser might be able to accomplish on its own website. But "[a]dvertisers become reliant on the walled garden's tools, algorithms, and reporting, leading to a lack of control over their data and campaign outcomes."[15] And this structure likely incentivized Meta to exploit certain communication channels to collect additional information that it should not have to make its data more valuable, as explained in more detail below.

20. As a result of its advertising efforts, as recently as 2023, Meta generated over $131 billion in annual revenue.[16]

21. Advertisers can also build "Custom Audiences."[17] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[18] With Custom Audiences, advertisers can target existing customers directly, and can also build "Lookalike

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] META, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227.

[18] META, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[19]

22. Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Meta with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Meta's "Business Tools,"[20] including the Meta Tracking Pixel, as described *supra*.

23. As Meta puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Meta, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[21]

24. Put succinctly, Meta's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

25. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user makes a purchase.[22] However, Meta's Business Tools can also track other events. Meta offers a menu of "standard events" from which advertisers can choose, including what content a visitor

[19] META, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531.

[20] META, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568; META, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341.

[21] META, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

[22] *See* META, META PIXEL GUIDE: ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* META, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; META, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

views or purchases.[23] Advertisers can even create their own tracking parameters by building a "custom event."[24]

26. One such Business Tool is the Meta Tracking Pixel. Meta offers this piece of code to advertisers (*e.g.*, website operators) to integrate into their websites. As the name implies, the Meta Tracking Pixel "tracks the people and the types of actions they take."[25]

27. When a user accesses a website hosting the Meta Tracking Pixel, Meta's software surreptitiously directs the user's browser to simultaneously send a separate message to Meta's servers. This second transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by Meta code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and a website in this scenario: the website's own code, and Meta's embedded code.

28. An example illustrates the point. Take an individual who navigates to a website and clicks on a button to browse the website's offerings. Once that button is clicked, the individual's browser sends a GET request to the website's server requesting that server to load the particular webpage. Because the website utilizes the Meta Tracking Pixel, Meta's embedded code, written in JavaScript, sends instructions back to the individual's browser, without alerting the individual that this is happening. Meta causes the browser to secretly and simultaneously duplicate the communication with the website, transmitting it to Meta's servers alongside additional information that transcribes the communication's content and the individual's identity. This entire process occurs within milliseconds.

[23] META, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[24] META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* META, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[25] META, RETARGETING, https://www.facebook.com/business/goals/retargeting.

29. In other words, when a user communicates with a website, those communications are simultaneously and contemporaneously duplicated and sent to Meta at the same time as they are being sent to the website.

30. After collecting and intercepting this information, Meta processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

31. Meta's other Business Tools function the same. For mobile applications, advertisers can utilize the Facebook SDK, which contains components like the App Events API, allowing advertisers to track events on native mobile apps so they can "measure ad performance and build audiences for ad targeting."[26]

32. Advertisers can also utilize the "Conversions API." Rather than using pixels that rely on cookies (browser Pixel events), the Conversions API enables tracking directly through advertisers' website servers (server events).[27]

33. Thus, the Conversions API's tracking capabilities are not impacted by a consumer's browser settings, cookies opt-outs, or device-specific privacy controls.[28] In addition, the Conversions API collects "customer information parameters sent with [] server event[s]"[29] so that those server events data points may be "matched to users"[30] – including "people who are more likely to take the action [advertisers] care about."[31]

[26] META, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[27] META, CONVERSIONS API, https://developers.facebook.com/docs/marketing-api/conversions-api ("The Conversions API is designed to create a connection between an advertiser's marketing data … from an advertiser's server[] … to Meta systems.").

[28] TUEORIS, DECODING CONVERSIONS API AND PRIVACY IMPLICATIONS, https://tueoris.com/privacy/decoding-conversions-api-and-privacy-implications/.

[29] META, BEST PRACTICES FOR CONVERSIONS API, https://www.facebook.com/business/help/308855623839366.

[30] META, CONVERSIONS API: VERIFYING YOUR SETUP, https://developers.facebook.com/docs/marketing-api/conversions-api/verifying-setup.

[31] META, ABOUT EVENT MATCH QUALITY, https://www.facebook.com/business/help/765081237991954.

34. When the Conversions API collects "[s]erver events," those data points are "linked to a dataset ID and are processed like events sent using the Meta Pixel."[32] As with the Meta Tracking Pixel, the Conversions API intercepts these communications contemporaneously and surreptitiously.[33] Meta "recommend[s] that advertisers implement the Conversions API alongside their Meta Pixel."[34]

35. Meta confirms, in its "Meta Business Tools Terms,"[35] that it has the capability to use information it collects for purposes other than recording it and conveying it to websites. For instance, Meta can use the information it collects "to promote safety and security on and off the Meta Products, for research and development purposes and to maintain the integrity of and to provide and improve the Meta Products." In other words, Meta can use the wiretapped information for its own "research and development," and well as to "protect" its own products and services.

36. Meta can also connect all information it collects to analyze and generate reports regarding advertising campaigns, create custom audience sets that can be shared with other advertisers, and "use your Event Data for ads delivery only after aggregating such Event Data with other data collected from other advertisers or otherwise collected on Meta Products."[36]

37. Further, Meta can use the event data to help websites "reach people with transactional and other commercial messages on [Facebook] Messenger and other Meta Products."[37]

38. Finally, Meta can use the information it collects "to personalize the features and content (including ads and recommendations) that we show people on and off our Meta Products."[38]

[32] META, CONVERSIONS API, https://developers.facebook.com/docs/marketing-api/conversions-api.

[33] META, CONVERSIONS API END-TO-END IMPLEMENTATION, https://developers.facebook.com/docs/marketing-api/conversions-api/guides/end-to-end-implementation#pick-your-integration-type ("send events in real time … via the Conversions API").

[34] *Id.*

[35] META, META BUSINESS TOOLS TERMS, https://m.facebook.com/legal/businesstech.

[36] *Id.*

[37] *Id.*

[38] *Id.*

39. Thus, Meta has the capability to use the information it wiretaps for purposes other than simply providing it to websites, including but not limited to its own contact information matching; measurement and analytics services; ad targeting; commercial and transactional messages; ad delivery improvement; feature and content personalization; product improvement, provision, and securement; and maintaining its own internal ecosystem of data for advertisers.

II. META ABUSES ANDROID LOCALHOST COMMUNICATION CHANNELS TO COLLECT DE-ANONYMIZED BROWSING INFORMATION

A. The Normal Process Through Which Meta Collects Information Through Its Tracking Pixel

40. Defendant owns and operates the Meta Tracking Pixel, which is integrated into the code of millions of websites.[39]

41. When a user visits a website—either on desktop or mobile browser—where the Meta Tracking Pixel is embedded, Defendant will collect through its Tracking Pixel the browsing information of the user that a website configures the Tracking Pixel to collect. That is, Defendant will collect (i) the detailed URL strings of the webpages or articles the user viewed or read, (ii) what items, products, articles, etc. the user searched for in a search bar, and (iii) what actions the user took on a page (*e.g.*, opened an article, added an item to a shopping cart, etc.).

42. Defendant pairs this information a user's Facebook ID via various cookies that Meta embeds on the user's device—and those cookies and identifiers are collected alongside the selected browsing information.

43. A cookie is a "small text file (up to 4KB) created by a website that is stored in the user's computer either temporarily for that session only or permanently in storage (persistent cookie)."[40] Among other things, persistent cookies can be used to "track user behavior across different sites. They store information such as geographic location, device specifications, and specific actions taken on the website."[41]

[39] WEBSITES USING FACEBOOK PIXEL, https://trends.builtwith.com/websitelist/Facebook-Pixel.

[40] PC MAGAZINE, COOKIE, https://www.pcmag.com/encyclopedia/term/cookie.

[41] COOKIEBOT, WHAT ARE TRACKING COOKIES AND HOW DO THEY WORK?, https://www.cookiebot.com/en/tracking-cookies/.

44. Meta "place[s] cookies on [a person's] computer or device and receive[s] information stored in [those] cookies when [said person] use[s] or visit[s]: [] Meta Products [(i.e., Facebook, Messenger, Instagram, etc.)]; [and] Products provided by other members of the Meta Companies; and Websites and apps provided by other companies that use the Meta Products, including companies that incorporate Meta' technologies [(i.e., the Facebook Business Tools)] into their websites and apps."[42]

45. In short, Meta, through its Tracking Pixel (a nearly invisible, pixel-sized dot on websites), places cookies on a user's computer or smartphone that allows Meta to follow a user's surfing behavior across other websites which have implemented a Meta Tracking Pixel or other Meta component.[43]

46. When a user accesses a website while logged into Facebook, the Meta Tracking Pixel will compel that user's browser to transmit several cookies, including the c_user, datr, fr, and _fbp[44] cookies.

[42] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[43] *See, e.g.*, Paschalis Bekos et al., *The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs* (Apr.2023), https://dl.acm.org/doi/pdf/10.1145/3543507.3583311 at 2139 ("FB Pixel[is] a conversion tracking tool embedded via JavaScript on websites, and be used to track users' activities both in space (i.e., in websites utilizing FB Pixel), and in time (i.e., in the past and future). Although FB Pixel advertises a 3-month-long lifespan and can seemingly limit any tracking to at most 3 months, unfortunately, in a great majority of websites with FB Pixel, the pixel employs rolling expiration dates for the f[i]rst-party cookies it places (_fbp), which can postpone its lifespan (and its associated tracking) indef[i]nitely.") (cleaned up).

[44] Note, the Meta Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, the Website. PC MAGAZINE, FIRST-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/first-party-cookie. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, Facebook. PC MAGAZINE, THIRD-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/third-party-cookie. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook. Pictured here and in the *infra* two images is the _fbp cookie, sent as a first-party cookie.

47. The c_user cookie contains, at least, the user's unencrypted Facebook ID.[45] The c_user cookie has a lifespan of three hundred sixty-five days.[46]

48. The datr cookie contains, at least, a value that uniquely identifies a browser.[47] The datr cookie has a lifespan of four hundred days.[48]

49. The fr cookie contains, at least, a value that uniquely identifies a browser and the user's encrypted Facebook ID.[49] The fr has a lifespan of ninety days.[50]

50. The _fbp cookie "identifies browsers for the purposes of providing advertising and site analytics services and has a lifespan of 90 days."[51]

51. When a website visitor's browser has recently logged out of an account, Meta compels the visitor's browser to send a smaller set of cookies, including the datr, fr, and _fbp cookies.

52. Absent the below discussed breach of communication protocols, Meta, at a minimum, would only be able to use the c_user, datr, fr, and _fbp cookies to link Facebook IDs and corresponding Facebook profiles and identify users.[52] Meta, itself, explains that these, and/or other "customer information parameters," are ultimately "matched to Meta accounts."[53] In this way, the "cookie[s] identif[y] browsers for the purposes of providing advertising and site analytics services."[54]

[45] MICROSOFT, COOKIE COMPLIANCE, https://learn.microsoft.com/en-us/dynamics365/commerce/cookie-compliance ("Cookie[:] c_user. Description[:] Cookie contains the user ID of the currently signed-in user.").

[46] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[47] *Id.* ("'Datr' is a unique identifier for your browser.").

[48] *Id.*

[49] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf ("The first part of the cookie is a browser ID, used to identify the web browser. The second part of the cookie is an encrypted version of the logged in user's Facebook ID.").

[50] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[51] FACEBOOK, COOKIE POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[52] *Id.*

[53] FACEBOOK, ABOUT EVENT MATCH QUALITY, https://www.facebook.com/business/help/765081237991954.

[54] FACEBOOK, COOKIES POLICY, https://www.facebook.com/policy/cookies.

53. These cookies are used to pair event data with personally identifiable information so Meta can later retarget consumers on Facebook.

54. There has been some debate amongst courts as to whether these Facebook cookies identify a user. *Compare Ghanaat v. Numerade Labs, Inc.*, 689 F. Supp. 3d 714, 720 (N.D. Cal. 2023) ("Most, if not all, courts to address the question have found at the pleading stage that Facebook IDs are PII."); *with Solomon v. Flipps Media, Inc.*, 136 F.4th 41, 54 (2d Cir. 2025) ("Nor does the Complaint plausibly allege that an ordinary person could identify Solomon through her FID.").

B. Meta Ties Android Users' Browsing Information To Their Facebook Or Instagram Profiles, Rendering Users Non-Anonymous And Identifiable

55. For Android users, however, the data Meta collects is anything but anonymous.

56. Typically, websites and mobile applications operate in "sandboxes." "By default, apps can't interact with each other and have limited access to the [operating system]. If app A tries to do something malicious, such as read app B's data or dial the phone without permission, it's prevented from doing so because it doesn't have the appropriate default user privileges."[55]

57. To put this more simply, an app installed on an Android phone is not supposed to be able to access data collected from or on websites, and vice versa. "You run everything in a sandbox, and there is no interaction within different elements running on it."[56] This "cut[s] off access to sensitive data or privileged system resources."[57]

58. Beginning in September 2024 and continuing through at least June 2, 2025, however, Defendant "abus[ed] legitimate Internet protocols [and platform capabilities], causing Chrome and other browsers [on Android mobile phones] to surreptitiously send unique identifiers to native apps installed on a device."[58]

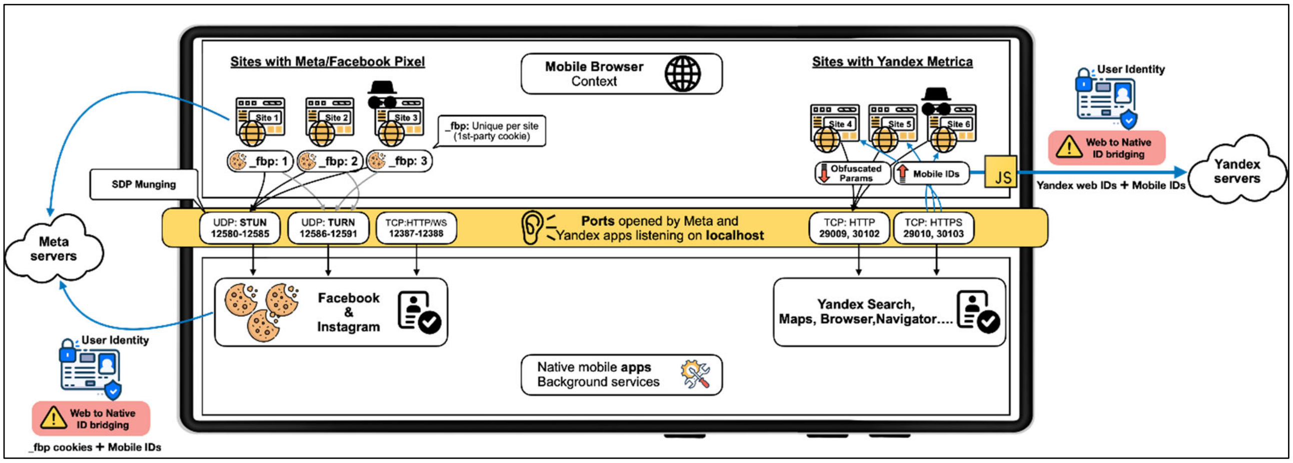
[55] APPLICATION SANDBOX, https://source.android.com/docs/security/app-sandbox.

[56] Goodin, *supra*, https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/.

[57] *Id.*

[58] *Id.*

59. This abuse allowed Defendant to "bypass core security and privacy protections provided by both the Android operating system and browsers that run on it," enabling Defendant to "pass cookies or other identifiers from [websites with the Meta Tracking Pixel loaded on] Firefox and Chromium-based browsers to native Android apps for Facebook [and] Instagram … apps, tying "that vast browsing history to the account holder logged into the app."[59]


Sites with Meta/Facebook Pixel
Mobile Browser Context
Sites with Yandex Metrica
Site 1
Site 2
Site 3
_fbp: Unique per site (1st-party cookie)
_fbp: 1
_fbp: 2
_fbp: 3
Site 4
Site 5
Site 6
Obfuscated Params
Mobile IDs
JS
User Identity
Web to Native ID bridging
Yandex servers
Yandex web IDs + Mobile IDs
SDP Munging
Meta servers
UDP: STUN 12580-12585
UDP: TURN 12586-12591
TCP:HTTP/WS 12387-12388
Ports opened by Meta and Yandex apps listening on localhost
TCP: HTTP 29009, 30102
TCP: HTTPS 29010, 30103
Facebook & Instagram
Yandex Search, Maps, Browser,Navigator....
User Identity
Web to Native ID bridging
_fbp cookies + Mobile IDs
Native mobile apps Background services

60. In other words, when an Android user accesses a website on their mobile device where the Meta Tracking Pixel is installed—and if the Android user has the Facebook or Instagram app installed on their phone—Defendant abuses localhost communication sockets typically "used for legitimate purposes such as web development"[60] to share the fbp values generated on the web browser that Defendant uses to tie browsing information with the native apps where users are logged in, hence persistently and "effectively de-anonymizing users' browsing habits on sites containing these trackers."[61]

61. This process renders the browsing history of Android users completely identifiable and more comprehensive than intend, as Meta collects a user's browsing information and ties the browsing information to PII like full name, e-mail address, and other contact information provided on Facebook and Instagram profiles that is not anonymous. And, of course, Meta profits

[59] *Id.*

[60] NARSEO VALLINA-RODRIGEZ ET AL., DISCLOSURE: COVERT WEB-TO-APP TRACKING VIA LOCALHOST ON ANDROID, https://localmess.github.io/.

[61] Goodin, *supra*, https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/.

considerably from this data collection, as Meta's advertising business depends on compiling as much data about users as possible to enable the greatest precision for ad targeting.

62. Incredibly enough, this process enables Meta to "link pseudonymous web identities with actual user identities, *even in private browsing modes*."[62]

63. Meta specifically targets "only Android users" through this process.[63] However, "similar data sharing between iOS browsers and native apps is technically possible. iOS browsers, which are all based on WebKit, allow developers to programmatically establish localhost connections and apps can listen on local ports. It is possible that technical and policy restrictions for running native apps in the background may explain why iOS users were not targeted by these trackers."[64]

64. The technical flow of Meta's process is as follows:

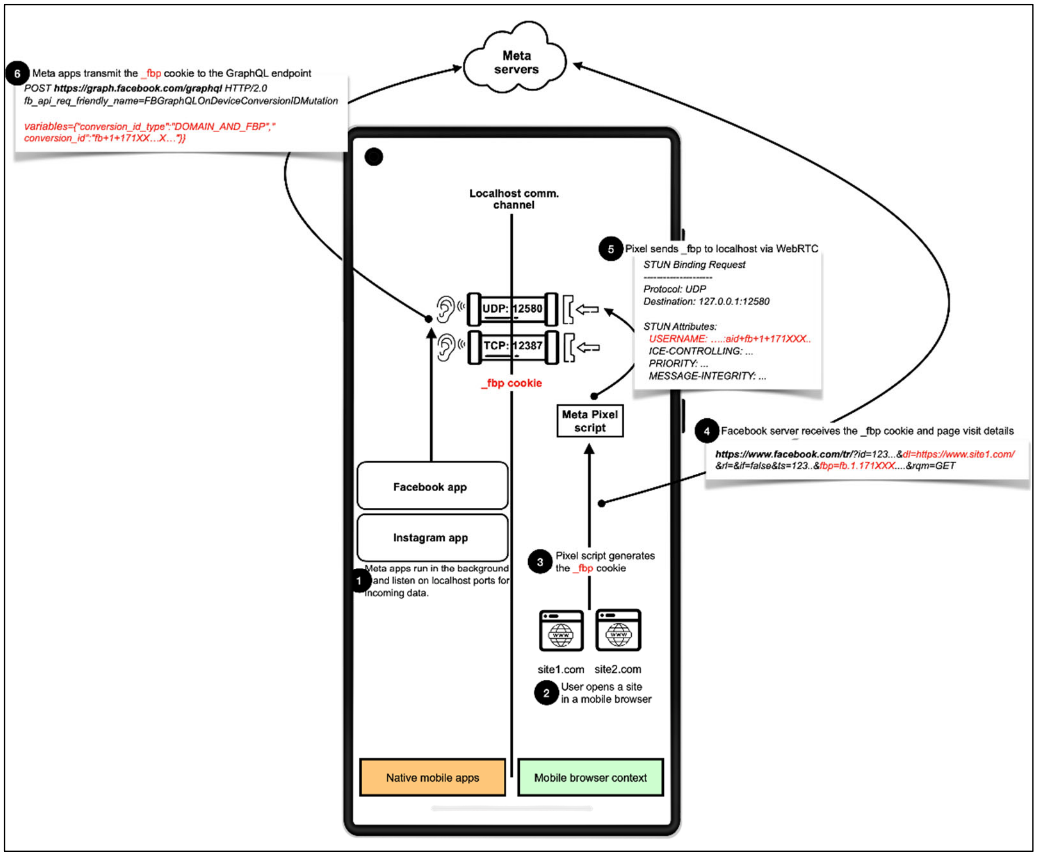
- The user opens the native Facebook or Instagram app, which eventually is sent to the background and creates a background service to listen for incoming traffic on a TCP port (12387 or 12388) and a UDP port (the first unoccupied port in 12580–12585). Users must be logged-in with their credentials on the apps.
- The user opens their browser and visits a website integrating the Meta Pixel.
- At this stage, some websites wait for users' consent before embedding Meta Pixel. Measurements of the top 100K website homepages, found websites that require consent to be a minority (more than 75% of affected sites does not require user consent).
- The Meta Pixel script is loaded and the _fbp cookie is sent to the native Instagram or Facebook app via WebRTC (STUN) SDP Munging.
- The Meta Pixel script also sends the _fbp value in a request to https://www.facebook.com/tr along with other parameters such as page URL (dl), website and browser metadata, and the event type (ev) (e.g., PageView, AddToCart, Donate, Purchase).
- The Facebook or Instagram apps receive the _fbp cookie from the Meta JavaScripts running on the browser and

[62] *Id.*

[63] *Id.*

[64] VALLINA-RODRIGEZ, *supra*, https://localmess.github.io/.

> transmits it to the GraphQL endpoint (https://graph[.]facebook[.]com/graphql) along with other persistent user identifiers, linking users' fbp ID (web visit) with their Facebook or Instagram account.[65]


Meta servers
6 Meta apps transmit the _fbp cookie to the GraphQL endpoint
Localhost comm. channel
5 Pixel sends _fbp to localhost via WebRTC
UDP: 12580
TCP: 12387
_fbp cookie
Meta Pixel script
4 Facebook server receives the _fbp cookie and page visit details
Facebook app
Instagram app
1 Meta apps run in the background and listen on localhost ports for incoming data.
3 Pixel script generates the _fbp cookie
site1.com
site2.com
2 User opens a site in a mobile browser
Native mobile apps
Mobile browser context

```
POST https://graph.facebook.com/graphql HTTP/2.0
fb_api_req_friendly_name=FBGraphQLOnDeviceConversionIDMutation

variables={"conversion_id_type":"DOMAIN_AND_FBP","
conversion_id":"fb+1+171XX...X..."}}
```

```
STUN Binding Request
-------------------
Protocol: UDP
Destination: 127.0.0.1:12580

STUN Attributes:
  USERNAME: .....:aid+fb+1+171XXX..
  ICE-CONTROLLING: ...
  PRIORITY: ...
  MESSAGE-INTEGRITY: ...
```

```
https://www.facebook.com/tr/?id=123...&dl=https://www.site1.com/
&rl=&if=false&ts=123..&fbp=fb.1.171XXX....&rqm=GET
```

65. To again distill this flow, Meta "insert[ed] key_fbp cookie content into" "a real-time peer-to-peer communication protocol commonly used for making audio or video calls in the browser," "caus[ing] the browser to send that data … to the Android local host, where the Facebook or Instagram app can read it and link it to the user."[66] This means Meta is de-anonymizing and linking Android users' browsing information to their Facebook and Instagram accounts in real time.

C. Neither Android Users Nor Websites Consent To Meta's Conduct

66. Meta's cookie and privacy policies do not disclose that Meta is linking Android users' browsing information to their Facebook and Instagram accounts. Indeed, common sense would

[65] Goodin, *supra*, https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/.

[66] *Id*.

dictate the opposite, given such linkage goes against general security and "sandboxing" settings on Android phones.

67. Further, this linkage occurs even if users are "not logged in to Facebook [or] Instagram … on their mobile browsers," "use[] Incognito Mode," or "clear[] their cookies or other browsing data."[67] Thus, Meta's tracking "defeats Android's inter-process isolation and tracking protections based on partitioning, sandboxing, or clearing client-side state."[68] And given the way Android operating systems typically work, a reasonable user would not read Meta's policies (to the extent they have notice of and assent to them, which is disputed) to disclose this conduct.

68. Notably, *even websites* were not aware of and do not consent to Meta's conduct. Again, what Meta is doing is in breach of typical Android security protocols. And, in fact, there have been "several complaints from puzzled website owners questioning why Meta Pixel communicates with localhost in Facebook developer forums by September 2024" with "[n]o official response from Meta representatives."[69] This suggests that website developers were unaware of what Meta was doing and did not consent to Meta's conduct.

69. Further, pursuant to its terms, Meta is only supposed to collect information that websites configure the Meta Tracking Pixel to collect. Therefore, a website operator can configure Meta's Tracking Pixel to transmit non-sensitive information, but theoretically prevent the Tracking Pixel from collecting sensitive or non-anonymous information. However, per the above breach of Android protocols by Meta, Meta's Tracking Pixel collects de-anonymized information, *regardless* of any configuration settings by the website.

70. On top of this, Meta changed protocols between September 2024 and the present (from HTTP to Websocket and STUN) to make it harder for web developers to detect.[70]

[67] VALLINA-RODRIGEZ, *supra*, https://localmess.github.io/.

[68] *Id.*

[69] *Id.*

[70] *Id.*

71. Compounding all of this, Google—who owns and develops the Android operating system—"said [Meta's] behavior violates the terms of service for its Play marketplace and the privacy expectations of Android users":

> The developers in this report [Meta] are using capabilities present in many browsers across iOS and Android in unintended ways that blatantly violate our security and privacy … We've already implemented changes to mitigate these invasive techniques and have opened our own investigation and are directly in touch with the parties.[71]

72. In other words, not only does Google believe that Meta's practices are not consented to and are a violation of Google's policies, Google believes the privacy breach to be so severe that Google is actively working to block further exploitations by Meta.

III. PLAINTIFF'S EXPERIENCE

73. Between September 2024 and the present, Plaintiff visited several websites on his Android mobile phone where the Meta Tracking Pixel was installed, including but not limited to techcrunch.com and wired.com. Both of these websites are among those affected by the aforementioned practices.[72]

74. When Plaintiff visited these websites on his Android phone, Plaintiff was located in California and had both the Facebook and Instagram apps installed on his phone.

75. Unbeknownst to Plaintiff, when Plaintiff visited these websites, everything Plaintiff did on these websites—*e.g.*, what articles Plaintiff viewed, what things Plaintiff searched for and the specific search terms—and Facebook ID were collected by Meta in real time using the Meta Tracking Pixel. This was so regardless of what the websites may or may not have configured Meta to collect.

76. Further, when Plaintiff visited these websites, and unbeknownst to Plaintiff, Meta sent a separate signal to itself that allowed Meta to tie Plaintiff's browsing information to the information he submitted on his Facebook and Instagram profiles (his name, address, e-mail address, etc.) in real-time, thus de-anonymizing and identifying Plaintiff and his browsing information in real-time.

[71] Goodin, *supra*, https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/.

[72] VALLINA-RODRIGEZ, *supra*, https://localmess.github.io/ (search bar for websites where the Meta Tracking Pixel was installed that were affected by this practice).

77. Meta compiled all of this information to create a comprehensive profile of Plaintiff in its databases, which was used for advertising. And, based on Meta's invasive privacy practices described herein, Plaintiff's data became more valuable for Meta based on its identifiability.

78. Neither Plaintiff nor the websites he visited were aware of Defendant's conduct, nor did either Plaintiff or the websites he visited consent to Defendant's conduct.

CLASS ALLEGATIONS

79. **Class Definition:** Plaintiff seeks to represent a class of similarly situated individuals defined as follows:

> All Android users in the United States with a Facebook or Instagram account who (i) have the Facebook or Instagram app installed on their Android phone, (ii) visited on their Android mobile phones a website between September 2024 and June 2, 2025 where the Meta Tracking Pixel was installed, and (iii) whose browsing information was collected by Meta.

80. **California Subclass:** Plaintiff also seeks to represent a subclass of similarly situated individuals defined as follows:

> All Android users in California with a Facebook or Instagram account who, while in California, (i) have the Facebook or Instagram app installed on their Android phone, (ii) visited a website on their Android mobile phones between September 2024 and June 2, 2025 where the Meta Tracking Pixel was installed, and (iii) whose browsing information was collected by Meta.

81. The Class and California Subclass shall be collectively referred to as the "Classes," and Members of the Class and Subclass will collectively be referred to as "Class Members," unless it is necessary to differentiate them.

82. Excluded from the Classes are Defendant, any affiliate, parent, or subsidiary of Defendant; any entity in which any Defendant has a controlling interest; any officer director, or employee of any Defendant; any successor or assign of any Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

83. **Numerosity**. Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of members of the Classes is unknown to Plaintiff at this time. However, it is estimated that there are tens or hundreds of millions of

individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's records and non-party records, such as those of Defendant's customers and advertising partners.

84. **Typicality**. Plaintiff's claims are typical of the claims of the Classes. Plaintiff, like all Class Members, has an Android phone, a Facebook and Instagram account, visited a website where the Meta Tracking Pixel was installed, and had his information collected and de-anonymized by Defendant for advertising purposes using the methods described herein.

85. **Adequacy**. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Classes. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Classes. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Classes.

86. **Commonality/Predominance**. Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members because Defendants have acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Classes include:

(i) Whether Defendant's acts and practices alleged herein constitute egregious breaches of social norms;

(ii) Whether Defendant acted intentionally in violating Plaintiff's and Class Members' privacy rights under the ECPA and the CIPA;

(iii) Whether Defendant was unjustly enriched as a result of its violations of Plaintiff's and Class Members' privacy rights; and

(iv) Whether Plaintiff and Class Members are entitled to damages under the ECPA, CIPA or any other relevant statute;

87. **Superiority**: Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated

persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs know of no special difficulty to that would be encountered by litigating this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

COUNT I
Intrusion Upon Seclusion

88. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

89. Plaintiff brings this claim individually and on behalf of the Classes against Defendants.

90. Plaintiff brings this claim pursuant to California law.

91. To state a claim for intrusion upon seclusion "[Plaintiff] must possess a legally protected privacy interest … [Plaintiff's] expectations of privacy must be reasonable … [and Plaintiff] must show that the intrusion is so serious in 'nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc*. 47 Cal. 4th 272, 286-87 (2009).

92. Plaintiff and members of the Classes have an interest in: (i) precluding the dissemination and/or misuse of their communications and information; and (ii) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to highly intrusive surveillance at every turn.

93. By conducting such widespread surveillance, Defendant intentionally invaded Plaintiff's and members of the Classes' privacy rights, as well as intruded upon Plaintiffs' and Class Members' seclusion.

94. Plaintiff and members of the Classes had a reasonable expectation that their communications, identities, personal activities, and other data would remain confidential.

95. Plaintiff and Class Members did not and could not authorize Defendant to intercept data on every aspect of their lives and activities.

96. The conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

(i) Defendant engage in widespread data collection and interception of Plaintiff's and members of the Classes' internet activity, including their communications with websites, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

(ii) Defendant abused a communication channel in violation of Google's policies to connect website information and Plaintiff's and members of the Classes' Facebook and Instagram accounts, thus de-anonymizing and identifying Plaintiff and members of the Classes and tying their browsing information with their identities;

(iii) Defendant combines the information collected on websites with users' identities for advertising purposes.

(iv) Defendant sells access or disclose this information, which contain the data improperly collected about Plaintiff and members of the Classes, to an unknown number of advertisers who choose to advertise on the Facebook ecosystem, which likewise violates Plaintiff's and members of the Classes' common law right to privacy and the control of their personal information.

97. Defendant was enriched through this collection of data because users' browsing information became more valuable when Defendant exploited the Android communication channels to tie browsing information to users' identities.

98. Defendant's amassment of electronic information reflecting all aspects of Plaintiff's and members of the Classes' lives into profiles for future or present use is in and of itself a violation of their right to privacy in light of the serious risk these profiles pose to their autonomy.

99. Accordingly, Plaintiff members of the Classes seek all relief available for invasion of privacy claims under common law.

COUNT II
Violation Of The California Invasion of Privacy Act
Cal. Penal Code § 631(a)

100. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

101. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

102. The California Legislature enacted the CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … 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.

103. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 363 (1985) (emphasis added, internal quotations omitted). This restriction is based on the "substantial distinction … between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor*, whether that auditor be a person or mechanical device." *Id.* at 361 (emphasis added). Such "simultaneous dissemination" "denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements." *Id.*; *see also Dept. of Justice v. Reporters Committee for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

104. Further, "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications." *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). Indeed, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, 2013 WL 5423918,

at *21 (N.D. Cal. Sep. 26, 2013). This accords with the fact that "the California Supreme Court has [] emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purposes of CIPA." *Javier*, 2022 WL 1744107, at *2. "Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

105. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or 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*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> 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.

106. To avoid liability under CIPA § 631(a), a defendant must show it had the consent of *all* parties to a communication, and that such consent was procured *prior to* the interception occurring. *See Javier*, 2022 WL 1744107, at *2.

107. Defendant's Meta Pixel is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

108. Defendant is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Defendant has the capability to use the wiretapped information for a purpose other than simply recording the communications and providing the communications to website operators. Accordingly, Defendant was a third party to any communication between Plaintiff and California Subclass Members, on the one hand, and any of the websites at issue, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

109. At all relevant times, Defendants willfully and without the consent of all parties to the communication, and in an unauthorized manner, read, attempted to read, and learned the contents the electronic communications of Plaintiff and California Subclass Members, on the one hand, and the websites at issue, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

110. At all relevant times, Defendant used those intercepted communications, including but not limited to de-anonymizing and identifying Plaintiff and California Subclass Members through the signals sent on the Android communication channels, using all of this information to build comprehensive audiences for advertisers, and selling access to those audiences to interested advertisers for a profit.

111. Neither Plaintiff nor California Subclass Members nor website operators provided their prior consent to Defendant's intentional interception, reading, learning, recording, collection, de-anonymization, and usage of Plaintiff's and California Subclass Members' electronic communications.

112. The wiretapping of Plaintiff and California Subclass Members occurred in California, where Plaintiff and California Subclass Members accessed the websites, where Defendant's Meta Pixel was loaded on Plaintiff's and California Subclass Members' browsers, where Meta used the Android communication channels to de-anonymize and identify Plaintiff and California Subclass Members, and where Defendant routed Plaintiff's and California Subclass Members' electronic communications to Defendant's servers, which were located in California where Defendant is headquartered.

113. Pursuant to Cal. Penal Code § 637.2, Plaintiff and California Subclass Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT III
Violation Of The California Invasion Of Privacy Act, Cal. Penal Code § 635

114. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

115. Plaintiff brings this claim individually and on behalf of the California Subclass against Defendant.

116. CIPA § 635(a) prohibits an entity from "manufactur[ing], assembl[ing], sell[ing], offer[ing] for sale, advertis[ing] for sale, possess[ing], transport[ing], import[ing], or furnish[ing] to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another."

117. Both the Meta Tracking Pixel and the code Meta uses to tie users' communications with websites to their identities are "devices" "primarily or exclusively designed or intended for eavesdropping upon the communication of another."

118. Meta manufactured, assembled, advertised or offered for sale, and possessed these devices.

119. Meta's use of these devices on the various websites that Plaintiff and California Subclass Members visited caused Plaintiff and California Subclass Members real and concrete harm, including but not limited to Meta's unjust enrichment and the loss of control of their personal information. Accordingly, Plaintiff and California Subclass Members may bring a claim for Meta's violation of CIPA § 635 because they have been injured by the same. *See Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *7 (N.D. Cal. Dec. 30, 2024).

120. Neither Plaintiff nor California Subclass Members nor website operators provided their prior consent to Defendant's manufacturing or use of these wiretapping devices.

121. Pursuant to Cal. Penal Code § 637.2, Plaintiff and California Subclass Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT IV
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 638.51(a)

122. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

123. Plaintiff bring this claim individually and on behalf of the proposed California Subclass against Defendant.

124. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

125. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

126. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

127. In plain English, a "pen register" is a "device or process" that records *outgoing* information, while a "trap and trace device" is a "device or process" that records *incoming* information.

128. For example, if a user sends an email, a "pen register" might record the email address it was sent from because this is the user's *outgoing* information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address it was sent from because this is *incoming* information that is being sent to that same user.

129. Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record

the numbers of incoming calls to that particular telephone line. As technology has advanced, however, courts have expanded the application of these surveillance devices. This, combined with the California Supreme Court's mandate to read provisions of the CIPA broadly to protect privacy rights, has led courts to apply CIPA § 638.50 to internet tracking technologies. *See*, *e.g.*, *Shah v. Fandom, Inc*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.* 742F. Supp. 3d 1072, 1076 (C.D. Cal. 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software was a "pen register").

130. The code Meta installs on Android users' browsers that enables Meta to tie users' communications with their Facebook or Instagram profiles is a "device or process" that ""identifies the source of visitors to [] website[s]," and is therefore a "pen register." *Heiting v. FKA Distributing Co.*, 2025 WL 736594, at *3 (C.D. Cal. Feb. 3, 2025); *see also Greenley*, 684 F. Supp. 3d at 1050 ("software that identifies consumers" is a pen register).

131. In the alternative, this code is a "trap and trace device" because it is a "device or process" that "identif[ies] the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication" (*i.e.*, Plaintiff and California Subclass Members who are communicating with websites and are being de-anonymized by Meta's code).

132. At all relevant times, Defendant installed or used the pen register or trap and trace device on various websites and the Android communication channels, enabling Defendant to de-anonymize and identify Plaintiff and California Subclass Members by tying their browsing information to their Facebook and Instagram profiles.

133. Neither Plaintiff nor California Subclass Members nor website operators provided

their prior consent to Defendant's installation or use of the pen register or trap and trace device. Nor did Defendant obtain a court order enabling it to do the same.

134. Pursuant to Cal. Penal Code § 637.2, Plaintiff and California Subclass Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 638.51(a).

COUNT V
Unjust Enrichment

135. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

136. Plaintiff brings this claim individually and on behalf of the Classes against Defendant.

137. Plaintiff brings this claim pursuant to California law.

138. Defendant has wrongfully and unlawfully trafficked in the Plaintiff's and members of the Classes' personal information and other personal data without their consent for substantial profits.

139. Plaintiff's and members of the Classes' personal information and data have conferred an economic benefit on Defendant, in that Defendant used its unauthorized connection with Android communication channels to link Facebook and Instagram accounts with browsing activity, this rendering the browsing activity de-anonymous and identifiable, and more valuable to advertisers. Defendant also conducted this activity without consent.

140. Defendant has been unjustly enriched at the expense of Plaintiff and members of the Classes, and has unjustly retained the benefits of their unlawful and wrongful conduct.

141. It would be inequitable and unjust for Defendant to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

142. Plaintiff and members of the Classes accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Defendant obtained as a result of their unlawful and wrongful conduct.

143. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding

loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant.

144. Defendant has been unjustly enriched by virtue of their violations of Plaintiff's and members of the Classes' legally protected rights to privacy as alleged herein, entitling Plaintiff and members of the Classes to restitution of Defendant's enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." RESTATEMENT (THIRD) OF RESTITUTION § 1, cmt. a.

145. Defendant was aware of the benefit conferred by Plaintiff and members of the Classes. Indeed, Defendant deliberately exploited the Android communication channels to link browsing information to Facebook and Instagram profiles. Defendant therefore acted in conscious disregard of the rights of Plaintiff and members of the Classes and should be required to disgorge all profit obtained therefrom to deter Defendant and others from committing the same unlawful actions again.

COUNT VI
Violation of the Electronic Communications Privacy Act
18 U.S.C. §§ 2511(1), *et seq*

146. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

147. Plaintiff brings this claim individually and on behalf of the Classes against Defendant.

148. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

150. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

151. The transmission of Plaintiff's and members of the Classes' website page visits, browsing and search information, and persistent identifiers each qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

152. The transmission of this information between Plaintiff and members of the Classes, on the one hand, and each website with which they chose to exchange communications, on the other hand, 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(12).

153. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

154. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

155. 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).

156. The following instruments constitute "devices" within the meaning of the ECPA:

(i) The Meta Tracking Pixel;

(ii) The code that enabled Meta to link browsing information with Facebook and Instagram profiles; and

(iii) Any other tracking code or SDK used by Defendant.

157. Plaintiff and members of the Classes' interactions with each website are electronic communications under the ECPA.

158. By utilizing the methods described herein, Defendant intentionally intercepted and/or endeavored to intercept the electronic communications of Plaintiff and members of the Classes in violation of 18 U.S.C. § 2511(1)(a).

159. Defendant then monetized and thus used the intercepted communications for advertising purposes. By intentionally using, or endeavoring to use, the contents of Plaintiff's and members of the Classes' electronic communications, while knowing or having reason to know that

the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

160. Defendant was not acting under the color of law to intercept Plaintiff's and members' of the Classes' electronic communications.

161. Plaintiff and members of the Classes did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy. Plaintiff and Class members had a reasonable expectation that Defendant would not intercept their communications and sell their data for advertising purposes without their knowledge or consent.

162. The websites Plaintiff and members of the Classes visited did not authorize or consent to Defendant's conduct, given Defendant's conduct constituted an abuse of Android security protocols and a violation of Google's terms.

163. The foregoing acts and omissions therefore constitute numerous violations of 18 U.S.C. §§ 2511(1), *et seq*.

164. As a result of every violation thereof, on behalf of themselves and the members of Classes, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. §§ 2510, et seq. under 18 U.S.C. § 2520.

<u>PRAYER FOR RELIEF</u>

WHEREFORE, Plaintiff, on behalf of himself and all members of the Classes, seeks judgment against Defendant, as follows:

(a) For an order certifying the Classes pursuant to Fed. R. Civ. P. 23, naming Plaintiff as the representative of the Classes, and naming Plaintiff's attorneys as Class Counsel to represent the Classes.

(b) For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

(c) For compensatory, punitive, and statutory damages in amounts to be determined by the Court and/or jury;

(d) For pre- and post-judgment interest on all amounts awarded; and

(e) For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all issues so triable.

Dated: June 3, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Emily A. Horne (State Bar No. 347723)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ehorne@bursor.com

Attorneys for Plaintiff