Matthew W. Ruan (SBN 264409)
FREED KANNER LONDON & MILLEN LLC
100 Tri-State International, Suite 128
Lincolnshire, IL 60069
Telephone: (224) 632-4500
mruan@fklmlaw.com

[additional counsel on signature page]

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JENNIFER VINCENT, WILLIAM BANEY, and DAWN MONTANEZ, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.; ALPHABET INC.; and GOOGLE LLC,

Defendants.

Case No.

<u>CLASS ACTION</u>

COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Jennifer Vincent, William Baney, and Dawn Montanez ("Plaintiffs"), individually and on behalf of all other persons similarly situated, as defined below, and based on personal knowledge, information and belief, and the investigation by counsel, allege the following against Meta Platforms, Inc. ("Meta"), Alphabet Inc. ("Alphabet"), and Google LLC ("Google," collectively "Defendants").

INTRODUCTION

1. This class-action lawsuit arises from revelations that Android device users have been subjected to systemic and malicious tracking of their online activity by Meta and Yandex Metrica ("Yandex")[1] who intentionally abused weaknesses in Android's software. Meta and Yandex exploited vulnerabilities in the Android software to deanonymize users' identities and track their online browsing activity and communications without consent. Not only did Meta and Yandex actively breach users' privacy for their own profit, but Google negligently failed to stop them and misrepresented the privacy protections available to Android users. These actions and inactions have resulted in severe privacy violations for millions of Android users across the United States.

2. On June 3, 2025, journalists at *Ars Technica* published a stunning report that "Meta and Yandex are de-anonymizing Android users' web browsing identifiers," which "allows Meta and Yandex to attach persistent identifiers to detailed browsing histories."[2] Put simply, Meta and Yandex were exploiting holes in Android software to link users' anonymous online-browsing activity with identifying information saved locally on Meta and Yandex mobile applications on their devices.

3. The journalists detailed the work of cybersecurity researchers who discovered these novel privacy breaches. The researchers uncovered covert connections Meta and Yandex created between users' online browsing activity and locally saved applications on their devices. These

[1] Yandex is a Russian technology company that provides search and advertising services.

[2] Dan Goodin, *Meta and Yandex are De-Anonymizing Android Users' Web Browsing Identifiers*, ARS TECHNICA (June 3, 2025), https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/ (last visited June 4, 2025).

connections allowed Meta and Yandex to identify the users and track their online behavior with specificity.

4. As stated by the researchers, "this method effectively allows [Meta and Yandex] to link mobile browsing sessions and web cookies to user identities, hence de-anonymizing users' visiting sites embedding their scripts" and "bypass[ing] typical privacy protections such as clearing cookies, Incognito Mode and Android's permission controls."[3]

5. The researchers detected Meta's exploitation of this attack vector since at least September 2024, whereas Yandex has been covertly tracking users in this way since at least 2017.

6. For its part, Google, the developer of the Android software, left the door wide open to this attack. The vulnerability was made possible by, among other things, the lack of controls Android imposes on developers operating on its platform. These failures are contrary to the assurances Google provided to its users, and purchasers of Android devices, about the safety and privacy of Android software.

7. For Plaintiffs and Class members the result is that when using their Android devices, and logged into a Meta or Yandex application, what they watched, clicked, bought, communicated, or read online was tracked without their consent or knowledge. By stripping users of their anonymity Defendants profited from targeted advertising and the sale of Android software and devices.

8. Defendants' actions violated multiple laws, including the Electronic Communications Privacy Act, 18 U.S.C. § 2511 ("ECPA"), California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"); the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* ("CIPA"); the Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq.* ("UCL"); and the California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA").

[3] Aniketh Girish et al., *Disclosure: Covert Web-to-App Tracking via Localhost on Android* (last updated June 3, 2025), https://localmess.github.io/#faq (last visited June 4, 2025).

Defendants have also committed negligence, invasion of privacy, and have been unjustly enriched by their unlawful conduct. Plaintiffs and Class members seek the maximum relief available at law and equity to remedy Defendants' violations.

PARTIES

9. Plaintiff Jennifer Vincent is a natural person and citizen of Pennsylvania, residing in York, Pennsylvania.

10. Plaintiff William Baney is a natural person and citizen of Pennsylvania, residing in Natrona Heights, Pennsylvania.

11. Plaintiff Dawn Montanez is a natural person and citizen of California, residing in El Monte, California.

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

13. Defendant Alphabet Inc. is a Delaware Corporation with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043.

14. Defendant Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google LLC is a wholly-owned subsidiary of Alphabet Inc.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331(d)(2) because the amount in controversy of the proposed class claims exceeds the sum or value 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 of the Defendants. The Court also has original jurisdiction over Plaintiffs' federal claims under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, *et seq.*

16. This Court has personal jurisdiction over the parties because Defendants are headquartered and have their principal places of business in California.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because all Defendants reside in this District.

COMMON FACTUAL ALLEGATIONS

A. Brief Overview of the Android Platform and Mobile Web Browsing

18. Android is a mobile operating system developed by Google that powers billions of mobile devices globally, including smartphones, tablets, and wearable devices.[4] Android software is available on smartphones made by third-party manufacturers such as Samsung and on Google's proprietary Pixel devices.[5] As of 2022, approximately 133 million individuals in the United States owned a smartphone powered by the Android operating system in the United States.[6]

19. Google pre-installs a suite of software on Android devices including the Chrome web browser. Consumers are additionally able to download third-party apps from the Google Play store including the Facebook and the Instagram mobile apps.

20. Google ensures that consumer's devices are safe when they download third-party apps on their Android devices from the Google Play store. In its article, "How we keep Google Play safe for

[4] *See* Android, https://www.android.com/ (last visited June 4, 2025).
[5] Android, Shop the Latest Android Phones, https://www.android.com/phones/shop/ (last visited June 4, 2025).
[6] iPhone vs Android Statistics, BACKLINKO.COM (last updated Mar. 31, 2025), https://backlinko.com/iphone-vs-android-statistics (last visited June 4, 2025).

users and developers" Google explains how it is "continually working on ways to weed out harmful apps and keep users, and developers, safe."[7]

21. Indeed, Google assured consumers that it created both a human and an automatic process to constantly review and evaluate mobile apps on the Google Play store. Google explains:

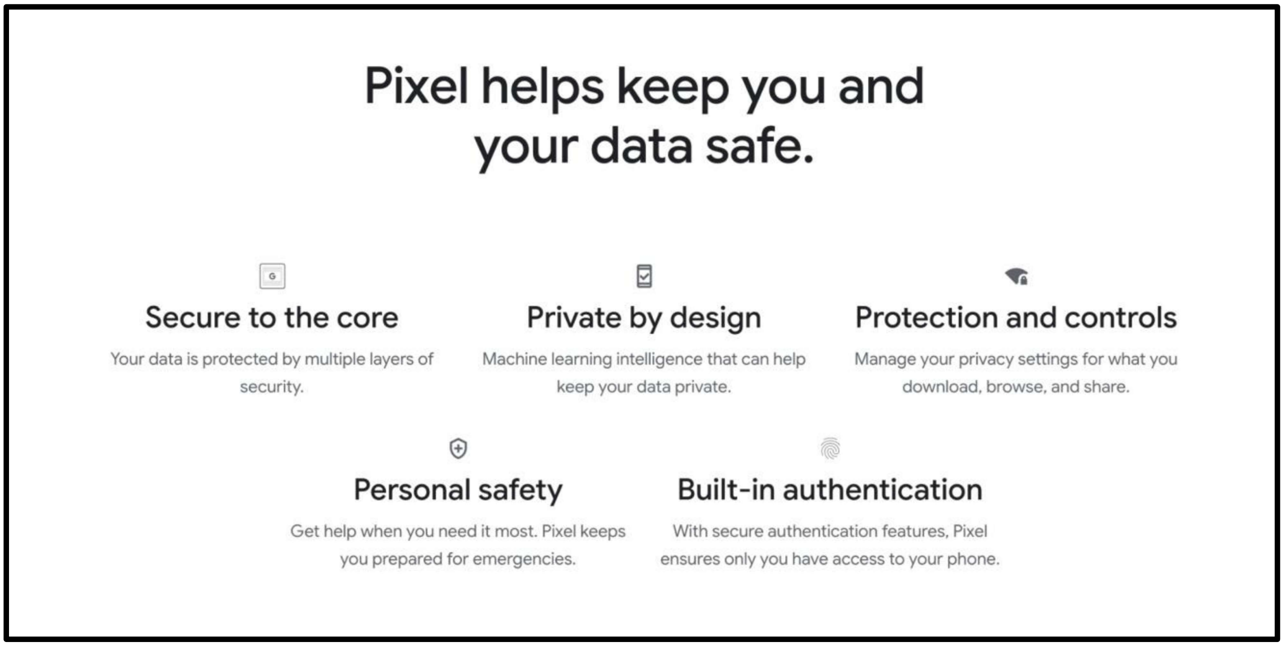
> Human review plays an important role in content safety at Google overall, combined with our machine learning systems which together strengthen the way that we review apps. Automated classifiers constantly scan apps at scale to look for policy violations. This includes new apps, updates to existing apps, and apps that are already live on the Google Play store. These extensive review processes help to prevent harmful apps from getting into the store and find live apps that require updating as we launch new standards for user safety.[8]

22. Google recently confirmed the removal of over 180 million apps from the Play Store after detecting various harmful vulnerabilities and exploits such as trojan viruses, ad fraud schemes, and other "nasty new spyware" responsible for collecting consumer's location data, audio, screenshots, and other sensitive data. [9]

23. Furthermore, Google represents that its smartphone devices such as its Pixel smart phone are "designed to help protect you and your stuff, and to keep you in control."[10]" Google's marketing representations claim that "Pixel helps keep you and your data safe" [and] "private by design[because

[7] How we help keep Google Play safe for users and developers, Google, https://safety.google/intl/en_us/stories/google-play-safety/ (last visited June 5, 2025).
[8] *Id.*
[9] Zak Doffman, *Google Confirms Play Store App Deletion—What You Do Now* (Mar. 16, 2025) https://www.forbes.com/sites/zakdoffman/2025/03/16/google-confirms-play-store-app-deletion-what-you-do-now/ (last visited June 5, 2025).
[10] Google Pixel Privacy and Security Features, GOOGLE, https://safety.google/pixel/ (last visited June 4, 2025).

it employs] machine learning intelligence." Google even touts that its Pixel devices are "secure to the core" and ensures that "your data is protected by multiple layers of security." *See* Figure 1.



Pixel helps keep you and your data safe.

Secure to the core

Your data is protected by multiple layers of security.

Private by design

Machine learning intelligence that can help keep your data private.

Protection and controls

Manage your privacy settings for what you download, browse, and share.

Personal safety

Get help when you need it most. Pixel keeps you prepared for emergencies.

Built-in authentication

With secure authentication features, Pixel ensures only you have access to your phone.

(Figure 1)

24. Google knows and appreciates that consumers' phone data is sensitive and understands the importance of keeping consumer data safe and mobile apps downloaded from its own Google Play store free of malicious software and vulnerabilities. Google proclaims: "Your life is on your phone: your

financial information, personal data, photos, and more. So Pixel is built with security at its core. Pixel hardware and software work together to help keep your phone and data private, safe, and secure."[11]

25. With Google's strong focus on privacy and protecting data, consumers feel confident browsing the internet on their Android and Pixel devices.

26. When a user navigates to a website from their Android device, the browser sends an HTTP "GET" request to the website's server asking for the server to send back HTML code that will allow the browser to display the website's content.

27. When responding to users' browsers, websites may also embed additional code within their reply transmission that include third-party tracking scripts, cookies, or pixels that can then transmit a user's website activity instantaneously to third-party tracking companies for advertising purposes.

28. A "cookie" is a small text file that a website server transmits to a user's browser and can be stored on the user's device. Cookies can either be first- or third-party cookies, with the former generally used for website functionality and the latter used for advertising and tracking purposes. A third-party cookie typically is used by companies to track users across websites and serve them advertisements. In many cases, a third-party cookie will assign a unique ID to a cookie that allows the user to be identified and tracked while browsing the internet and across websites.[12]

29. A tracking "pixel"—also known as a web beacon, clear GIF, or web bug—is a discreet, single-pixel image embedded in a webpage or email to monitor user interactions. Though invisible to the user, it enables the server hosting the image to gather data such as the user's device type, operating system, IP address, the time the content was accessed, and whether any related cookies are already stored

[11] *Id.*

[12] All About Internet Cookies, COOKIEYES.COM (June 2, 2025), https://www.cookieyes.com/blog/internet-cookies/ (last visited June 4, 2025).

in the browser. This mechanism helps identify user behavior without requiring visible elements or direct interaction.[13]

30. To avoid this tracking, Google claims that Android users can "personalize [their] privacy experience" by altering their privacy settings and controlling their application permissions.[14] Additionally, some web browsers will automatically block or anonymize users' web browsing activity to stop third-party tracking. For example, Google claims users can opt to block third-party cookies completely from their Android devices.[15]

31. Unfortunately, Meta and a Russian company called Yandex exploited vulnerabilities in the Android operating system allowing them to de-anonymize and otherwise obtain protected information from consumers.

B. The Meta Tracking Pixel

32. Defendant Meta is a tech company that owns various social media mobile apps including Facebook and Instagram. Meta's core business is digital advertising of highly targeted ads to consumers.

33. To facilitate its advertising enterprise, Meta collects vast amounts of user data such as interests, behavior, demographics through the Meta Tracking Pixel. The Meta Tracking Pixel is estimated to be installed on 5.8 million websites.[16]

[13] Patti Croft, What Is a Web Beacon and Why Should You Care? (Feb. 19, 2025), https://allaboutcookies.org/what-is-a-web-beacon (last visited June 4, 2025).
[14] Android, Android Privacy Settings and Permissions, https://www.android.com/safety/privacy/#safety-privacy-dashboard (last visited on June 4, 2025).
[15] Delete, Allow and Manage Cookies in Chrome, Google, https://support.google.com/chrome/answer/95647?hl=en&co=GENIE.Platform%3DAndroid (describing how to delete and block third-party cookies on an Android device) (last visited June 5, 2025).
[16] Goodin, *supra* note 2.

34. The Meta Pixel is a snippet of code that websites embed to facilitate the tracking of user interactions, including page views, button clicks, form submissions, and other browser events.[17]

35. User's online-browsing data is valuable and has economic value to Plaintiffs and Class members.[18]

36. When a user visits a website containing the Meta Pixel, the Pixel causes the user's browser to make a request to Meta's external servers to then send back instructions to the individual's browser. These instructions include requests that the user's browser transmit data from the user's device to Meta. This data is generated while the user navigates and interacts with the website and can include webpage URLs, search requests, events on the websites (e.g., button clicks), and form-field information inputted by the user.

37. The Meta Pixel associates users' online activity with their Meta accounts through Facebook and Instagram. When a user is logged into Facebook or Instagram, the Pixel can match the user's off-site activity with their profile on Meta's platforms, thereby creating detailed behavioral profiles used for ad targeting, content customization, and algorithmic inference. As Meta explains the Meta Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts" and "the Pixel will track URLs visited, domains visited, and the devices your visitors use."[19]

[17] About Meta Pixel, FACEBOOK.COM, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited June 4, 2025).

[18] Online Insights Study, Google, https://onlineinsightsstudy.google/signup (offering up to $130 per year for browsing data); Computer & Mobile Panel, Nielson, https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (offering up to $60 for browsing data).

[19] Get Started – Meta Pixel, META, https://developers.facebook.com/docs/meta-pixel/get-started/ (last visited June 4, 2025).

38. When a user visits a website that has the Meta Pixel embedded, the Meta Pixel will download a series of cookies onto the user's device with unique identifiers that allow Meta to track that user.

39. The cookies that Meta causes to be downloaded on users' devices include the "c_user," "datr," "fr,"' and "_fbp" cookies. These are different types of cookies that perform different functions for Meta.

40. The c_user cookie contains a unique identifier linked to an individual's Facebook account that necessarily reveals a consumer's Meta social media profile. For example, appending the c_user value to the Facebook URL reveals the consumer's Facebook profile. If the c_user value is 123456, the corresponding user profile can be accessed at www.facebook.com/123456. This cookie enables Facebook to uniquely identify a user and associate their activity on external websites with their Facebook profile.

41. The fr cookie is a browser-based tracking tool used by Meta to support personalized advertising and collect usage analytics. It includes a unique ID that allows Meta to monitor user activity across multiple sites and devices, building insights into user behaviors and interests. In contrast to the c_user cookie, which is tied specifically to authenticated Facebook users, the fr cookie can be used to track both Facebook account holders and non-users alike. This means Meta can gather data on individuals even if they're not actively logged into or registered on Facebook.

42. The datr and _fbp cookies are both used by Meta to identify users' browsers and related data.[20]

[20] Meta Cookies Policy, META, https://www.facebook.com/privacy/policies/cookies?annotations[0]=explanation%2F1_common_cookies_and_uses (last visited June 4, 2025).

43. In combination with the cookies listed above, the Meta Pixel enables Meta to intercept users' communications. When the Meta Pixel is embedded on a website, its script will cause a user's browser to duplicate and transmit communications that the user sends to the website and transmit that information instantaneously to Meta, along with cookie values, browser, and device information.

44. While Meta's tracking capabilities through the Meta Pixel are extensive, they are usually limited to the activity that occurs within the device's web browser and related processes. Typically, a device's web browser functionality will be "sandboxed" or separated from the processes on the local device. Meaning, for example, the Facebook application on a device would not be able to access information from a user's web browsing.

45. Users can, and regularly do, take measures to limit the information collected by Meta and anonymize their browsing activity and separate it from their conduct on Meta's platforms. In fact, users regularly opt not to share identifying information with Meta and to disable the c_user cookie. When users do this, they believe that Meta will not be able to track their identity with their browsing activity.[21]

46. However, as discussed in detail below, Meta and Yandex's exploitation of vulnerabilities in the Android software left users powerless to defeat the secret and malicious tracking accomplished by breaching the barriers between a user's browser and the applications downloaded on the device itself.

C. Meta and Yandex Exploit Android's Vulnerabilities

47. Meta and Yandex were able to form a secret software connection between Android users' web browsers and locally-installed applications that allowed them to de-anonymize users' online

[21] Delete, Allow and Manage Cookies in Chrome, Google, https://support.google.com/chrome/answer/95647?hl=en&co=GENIE.Platform%3DAndroid (describing how to delete and block third-party cookies on an Android device) (last visited June 5, 2025).

activity. This connection should not have been possible and violated "[o]ne of the fundamental security principles [that?] exists in the web, as well as the mobile system," called "sandboxing."[22]

48. Sandboxing is the principle that online websites and mobile applications each operate in their own "sandbox" and cannot be permitted to interact with one another. Thus, an application installed on a user's Android device should have no way of interacting with, or collecting data from, websites that a user visits on their browser.[23]

49. However, since at least 2017, Android's operating system allowed developers to breach these sandboxes and "bypass core security and privacy protections provided by both the Android operating system and browsers that run on it."[24]

50. By contrast, upon information and belief, other smart phone and mobile device operating systems, such as Apple's iOS, impose greater controls on developers attempting to access similar device functions.[25]

51. In the case of Meta, from September 2024 to June 3, 2025, it was able to covertly transmit the _fbp cookie—which Meta represents is only intended to identify a user's browsers—and other data from mobile browsers to native Facebook and Instagram apps using WebRTC STUN messages over local UDP ports. This means that Meta was able to correlate the _fbp cookie—which is an ostensibly anonymous browser identifier—with the account of a logged in Instagram or Facebook user.

52. This communication was not visible to users, did not seek user consent, and was able to bypass Incognito Mode, cookie clearing, and Android permission mechanisms.

[22] Goodin, *supra* note 2 (quoting Narseo Vallina-Rodriguez, a researcher behind the discovery of the Android breach).
[23] *Id.*
[24] *Id.*
[25] Goodin, *supra* note 2.

53. Meta's tracking technology transmitted intercepted data instantaneously along with persistent user identifiers stored within those applications—effectively de-anonymizing users and linking their browsing activity to their Meta profiles.

54. When an Android user navigated to a website with the Meta Pixel embedded in it, the Meta Pixel instructed the user's browser to send a separate message to Meta's external servers simultaneously. This separate message included data collected by the Pixel as well as cookie data. At the same time, cookie data was passed through the Android device's local capabilities and paired with the identity of the logged-in user of the Facebook or Instagram applications.

55. Meta accomplished this by abusing access to "local host sockets" which allow applications, such as Facebook and Instagram, to "listen" and read data transmitted by the browsers.[26]

56. Due to this breach, when Android users with a Meta application installed on their device visited websites the Meta Pixel sent "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)."[27] Depending on the users' activity, this means that sensitive information such as healthcare searches, financial data inputted in form fields, and any other private activities users conducted online on their devices would be transmitted to Meta *and* linked with their identities stored on their Meta applications. This invasion is especially harmful as Meta operates a "real identity" platform where users are required to create "one account using the name they go by in everyday life that represents their authentic identity."[28]

57. Yandex, a Russian-owned technology company, has since 2017 accomplished its breach in similar ways by utilizing the local host, except that "[a]s opposed to Meta's Pixel case, all this

[26] *Id.*; Girish, *supra* note 3.
[27] Girish, *supra* note 3.
[28] Authentic Identity Representation, META, https://transparency.meta.com/policies/community-standards/authentic-identity-representation (last visited June 5, 2025).

information is aggregated and uploaded together to the Yandex Metrica server (e.g., mc[.]yango[.]com) by the JavaScript code running on the web browser, rather than by the native app. In the case of Yandex, the native app acts as a proxy to collect native Android-specific identifiers and transfer them to the browser context through localhost sockets."[29]

D. Google Failed to Protect its Users' Privacy

58. Google's failure to secure its Android software to prevent unauthorized access to consumers' devices by Meta and Yandex is unacceptable and has led to a violation of its users' privacy and subjected them to actual harm and put them at a future risk of harm.

59. Google has implemented an "overly permissive" Android design that "allows Meta Pixel and Yandex Metrica to send web requests with web tracking identifiers to specific local ports that are continuously monitored by the Facebook, Instagram, and Yandex apps."[30]

60. Specifically, Google's decision to allow third-party developers to access specific local ports should have been, and upon information and belief was not, supplemented with a security protocol to ensure such access was not misused. Due to this failure, Meta and Yandex were able to exploit Android's software and de-anonymize users and their browsing activity with no sufficient oversight from Google.

61. Google knew, or should have known, that by failing to monitor this access it had allowed a core vulnerability in the Android software that would allow developers such as Meta and Yandex to identify users and track their online activity without consent.

62. Google has falsely claimed that Android allows users to "choose when to share certain sensitive data with apps you download."[31] It is now clear that users had no control over their privacy

[29] *Id.*

[30] Goodin, *supra* note 2.

[31] Android, Android Privacy Settings and Permissions, https://www.android.com/safety/privacy/#safety-privacy-dashboard (last visited June 4, 2025).

while Google negligently and/or recklessly allowed developers to manipulate fundamental aspects of Android's software without corresponding safeguards. Google's additional claims that "Android minimizes and de-identifies your data from intelligent features. And restricts access to technically ensure your privacy and safety," was also false.

63. Indeed, Google sold its Pixel phones with the false promise that "[a]ll Pixel devices are designed to respect your privacy. … we ensure the privacy and safety of your data by minimizing the amount of data stored, **de-identifying it so that the data is not linked to you**, and restricting its access altogether."[32]

64. Google can and should have done more to protect Android users from Meta and Yandex's malicious attack and unauthorized tracking by securing its Android software. Google failed Android users and violated the privacy promises it had made to them in exchange for their business.

65. Google's failures are especially egregious when considering that Yandex has been exploiting these vulnerabilities since at least 2017.

PLAINTIFFS' PERSONAL EXPERIENCES

Plaintiff Jennifer Vincent

66. Plaintiff Jennifer Vincent owns a Google Pixel, an Android device, and has downloaded the Meta applications Facebook and Instagram on that device.

67. Plaintiff Vincent purchased that device in approximately late 2023 or early 2024.

68. Plaintiff Vincent regularly browses online and visits websites on her device and communicates with those websites by inputting information and making selections.

69. Plaintiff Vincent recalls visiting, among others, the Disney Store and USAA Insurance websites on her Android device, which, upon information and belief, include the Meta Pixel Tracker.

[32] Google Pixel Privacy and Security Features, GOOGLE, https://safety.google/pixel/ (last visited June 4, 2025).

Plaintiff Vincent recalls inputting personal information into these websites, including personal financial and insurance-related information.

70. Plaintiff Vincent values her privacy and did not, and would not, consent to having Meta track her online activity or connecting it with her real identity through the Facebook and Instagram applications on her phone.

71. Plaintiff Vincent believed that Android's software included privacy and safety protections that would keep her online activity private.

Plaintiff William Baney

72. Plaintiff William Baney owns a Samsung Galaxy S20 Ultra 5G, an Android device, and has downloaded the Meta applications Facebook and Instagram on that device.

73. Plaintiff Baney purchased that device in approximately 2020.

74. Plaintiff Baney regularly browses online and visits websites on his device and communicates with those websites by inputting information and making selections.

75. Plaintiff Baney recalls visiting, among others, the PNC bank website on his Android device, which, upon information and belief, includes the Meta Pixel Tracker. Plaintiff Baney recalls inputting personal information into this website, including his username, password, and account-related information.

76. Plaintiff Baney values his privacy and did not, and would not, consent to having Meta track his online activity or connecting it with his real identity through the Facebook and Instagram applications on his phone.

77. Plaintiff Baney believed that Android's software included privacy and safety protections that would keep his online activity private.

Plaintiff Dawn Montanez

78. Plaintiff Dawn Montanez owns a Samsung Galaxy A54, an Android device, and has downloaded the Meta applications Facebook and Instagram on that device.

79. Plaintiff Montanez purchased that device prior to 2024.

80. Plaintiff Montanez regularly browses online and visits websites on her device and communicates with those websites by inputting information and making selections.

81. Plaintiff Montanez recalls visiting, among others, www.ancestry.com, www.lowes.com, www.zillow.com, and www.ups.com on her Android device, which, upon information and belief, include the Meta Pixel Tracker. Plaintiff Montanez recalls inputting personal information into these websites.

82. Plaintiff Montanez values her privacy and did not, and would not, consent to having Meta track her online activity or connecting it with her real identity through the Facebook and Instagram applications on her phone.

83. Plaintiff Montanez believed that Android's software included privacy and safety protections that would keep her online activity private.

CLASS ACTION ALLEGATIONS

84. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure Rule 23 on behalf of themselves and all others similarly situated as a class action on behalf of the following classes:

> **Class Definition**
>
> All users of an Android device in the United States, with a Meta or Yandex application installed on their devices, who visited websites on those devices and whose browsing information was collected without their consent within the applicable statute of limitations period(s).
>
> **California Subclass**
>
> All users of an Android device in California, with a Meta or Yandex application installed on their devices, who, while in California, visited websites on those devices and whose browsing information was collected without their consent within the applicable statute of limitations period(s).

> **<u>California Purchaser Subclass</u>**
>
> All residents of California who, within the applicable statute of limitations period(s), purchased an Android device for purposes other than resale.

85. The following people are excluded from the Class: (i) any Judge presiding over this action and members of her or her family; (ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiffs' counsel and Defendants' counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

86. *Numerosity.* Members of the Class are so numerous that joinder of all class members is impractical. Given the popularity of Android devices, the number of persons in the Class is estimated to be in the millions. Additionally, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical.

87. *Commonality and predominance.* A well-defined community of interest exists in the questions of law and fact involved in this case. Questions of law and fact common to the members of the class that predominate over questions affecting only individual Class members include:

(a) Whether Defendants intentionally or negligently allowed the unauthorized tracking of Class members.

(b) Whether Defendants' conduct violates ECPA, CIPA, or any other relevant statute.

(c) Whether Plaintiffs and Class Members are entitled to statutory damages;

(d) Whether Plaintiffs and Class Members are entitled to injunctive relief;

(e) Whether Defendants were unjustly enriched by their violation of Class members' privacy;

(f) Whether Defendants misrepresented the privacy protections of the Android software.

88. *Typicality.* Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, are Android users with the relevant applications installed that visited websites within the statutory period and/or are purchasers of Android devices.

89. *Adequacy.* Plaintiffs will adequately safeguard the interests of the Class members, as Plaintiffs' interests align with, and do not contradict, those of the Class. Plaintiffs' counsel has experience in handling class action litigation, including sophisticated data privacy and product liability litigation.

90. *Superiority.* A class action is the most effective, efficient and fair way to resolve this dispute, as individual litigation by all Class members is impractical and would overburden the court system. It would also risk inconsistent judgments and increase delays and expenses for all involved parties. In contrast, proceeding as a class action presents few management challenges, conserves resources, and protects the rights of each Class member. Plaintiffs expect no difficulties in managing this case as a class action.

91. Plaintiffs reserve the right to revise the foregoing allegations based on facts learned through additional investigation and discovery.

FIRST CAUSE OF ACTION
Violation of the California Computer Data Access and Fraud Act
(California Penal Code § 502)
(Against Meta on behalf of the Class or, in the Alternative, the California Subclass)

Plaintiffs incorporate the above paragraphs by reference and say—

92. Plaintiffs bring this claim individually and on behalf of the Class. In the alternative, Plaintiff Montanez brings this claim individually and on behalf of the members of the proposed California Subclass against Meta.

93. The California Legislature enacted the CDAFA with the intent to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

94. The Legislature further declared that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

95. For purposes of the statute, a number of definitions were provided. The term "access" means to "gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

96. The term "computer program or software" is defined as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions." Cal. Penal Code § 502(b)(3).

97. The term "computer system" refers to "a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

98. Plaintiffs' and Class members' web browsers used to access the Website are "computer software," and the Android devices on which Plaintiff Montanez and Class members used their web browsers constitute computers or "computer systems" within the scope of the CDAFA.

99. The statute also defines the term "data" to mean a "representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions." The statute further provides that data may be in "any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(8).

100. As discussed above, a website cookie value, including the Meta third-party tracker cookie, and Android users' browsing-activity information are both "data" within the meaning of the statute.

101. Under California Penal Code § 502(c)(1), it is unlawful knowingly to access and without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network in order to…wrongfully control or obtain money, property or data. Cal. Penal Code § 502(c)(1).

102. The statute also makes it unlawful to access knowingly and without permission take, copy, or make use of any data from a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2).

103. The CDAFA further prohibits any person from knowingly accessing and without permission adding, altering, damaging, or destroying any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(4).

104. Under subsections (6) and (7) of Penal Code § 502(c), a person also may not knowingly and without permission (i) provide or assist in providing a means of accessing or (ii) access or cause to

be accessed any computer, computer system, or computer network. Cal. Penal Code §§ 502(c)(6) and (7).

105. Based on Meta's unauthorized breach of the Android software to cause users' web browsers to send information to native applications on their devices to track and identify Plaintiffs' and Class members' browsing activity, as alleged above, Defendant knowingly accessed and without permission altered and used Plaintiffs' and Class members' data and computer systems in violation of Penal Code § 502(c)(1).

106. Similarly, the exploitation of the Android software by Meta violates subsection (c)(4) because Meta added and altered data and computer software on Plaintiffs' and Class members' computers or computer systems. Cal. Penal Code § 502(c)(4).

107. By exploiting the Android software, Meta also knowingly and without permission provided its trackers with a means of accessing Plaintiffs' and Class members' computers, computer systems, and/or computer networks in violation of Penal Code §§ 502(c)(6) and (7).

108. Further, Meta's unauthorized collection and use of Plaintiffs' and Class members' personally identifying and addressing information violates Penal Code § 502(c)(2) because Defendant took and made use of sensitive data from Plaintiffs' and Class members' computers, computer systems, or computer networks.

109. Plaintiff Montanez is a resident of California who used her Android device (i.e., computers, computer systems, and/or computer networks) in California. Meta accessed or caused to be accessed Plaintiff Montanez's and Class members' data and other personally identifying information from within California.

110. Meta was unjustly enriched by accessing, acquiring, taking, and using Plaintiffs' and Class members' data and computer systems without their permission or consent, and using all of that

identifying information to maximize revenue from advertising for Meta's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

111. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs and Class members have suffered damages. Under Penal Code § 502(e)(1), Plaintiffs and Class members are entitled to compensatory damages, injunctive relief, and other equitable relief in an amount to be determined at trial.

112. Plaintiffs and Class members suffered an economic injury when their data was misappropriated without their consent and used for Meta's profit. Plaintiffs' and Class Members' browsing activity and data has economic value; indeed, Google itself pays for this data as do other third-party research panels.33

113. Plaintiffs and Class members also are entitled to an award of reasonable attorneys' fees and costs under Penal Code § 502(e)(2).

SECOND CAUSE OF ACTION

Violation of the California Invasion of Privacy Act, Cal. Penal Code § 638.51(a)

(Against Meta on behalf of the Class or, in the Alternative, the California Subclass)

Plaintiffs incorporate the above paragraphs by reference and say—

114. Plaintiffs bring this claim individually and on behalf of the Class. In the alternative, Plaintiff Montanez brings this claim individually and on behalf of the members of the proposed California Subclass against Meta.

115. CIPA section 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."

[33] Online Insights Study, Google, https://onlineinsightsstudy.google/signup (offering up to $130 per year for browsing data); Computer & Mobile Panel, Nielson, https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (offering up to $60 for browsing data).

116. A “pen register” is “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).)

117. Meta’s software installed on users’ Android devices acts as a “pen register” because it is a “device or process” that captures the “routing, addressing, or signaling information”—including the cookie values, browser information, identifying user information—from the electronic communications transmitted by Plaintiffs’ and Class Members’ Android devices. Cal. Penal Code § 638.50(b).

118. At all relevant times, Meta installed and used its malicious tracking software, as described above, on Plaintiffs’ and Class Members’ Android devices, and used the Trackers to collect Plaintiffs’ and Class Members’ identifying information and data.

119. The identifying browser information, cookie values, and identifying user information transmitted by the Meta software on the Android devices, described above, constitutes routing, signaling, and addressing information.

120. Meta’s Pixel and the covert code on the Android device is a “device” or “process” that identifies Android users, gathers data, and correlates that data through its malicious exploit of the Android software.

121. Plaintiffs and Class Members did not provide their prior consent to Defendant’s installation or use of the Trackers on their browsers.

122. Meta did not obtain a court order to install or use its tracking technology.

123. Plaintiffs and the Class members seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

THIRD CAUSE OF ACTION
Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631(a)

(Against Meta on behalf of the Class or, in the alternative, California Subclass)

Plaintiffs incorporate the above paragraphs by reference and says—

124. Plaintiffs bring this claim individually and on behalf of the Class. In the alternative, Plaintiff Montanez brings this claim individually and on behalf of the members of the proposed California Subclass against Meta.

125. The California Invasion of Privacy Act, Cal. Penal Code §§ 630, et seq. ("CIPA"), is intended by California's legislature to address "advances in science and technology [that] 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."

126. To establish liability under section 631(a), Plaintiffs need only establish that Defendant, "by means of any machine, instrument, or contrivance, or in any other manner," did or does any of the following:

> [i] [I]ntentionally 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*
>
> [ii] [W]illfully 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*

> [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> [iv] [A]ids, 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.

127. Under § 631, a defendant must show that it had all parties' consent to the interception.

128. Meta is a "person" for the purposes of CIPA.

129. Meta maintains its headquarters and principal place of business in California.

130. Meta's tracking technology–including the Meta Tracking Pixel, related cookies, and Meta software installed on users' devices constitute a "machine, instrument, or contrivance … or other manner."

131. Meta covertly used its tracking technology to intercept Plaintiffs' and Class members' communications made to websites visited on their Android devices and identify those users as associated with the contents of these communications. As described above, the content of these communications included, but was not limited to, users' search requests, website selections (e.g., button clicks), form-field data inputted onto websites. This information was collected on the browser by the Meta Tracking Pixel and then paired with cookies and identifying data from the Android's native Meta applications to identify those users.

132. The interceptions and de-anonymization of Plaintiffs' and Class Members' communications occurred instantly while those electronic communications were in transit or were being sent from or received within California.

133. Meta, without consent of the parties to the communication, read, attempted to read, or learned the contents of Plaintiffs' and Class members' communications to websites and paired those communications with Plaintiffs' and Class members' identities without authorization. Indeed, Meta's conduct was secret and Plaintiffs' and Class members' had no opportunity to consent or authorize Meta's malicious conduct on their Android devices.

134. Meta uses the intercepted communications for its own advertising and analytics purposes to create profiles on consumers and serve them highly targeted advertising; as such Meta was a third-party to any communications between Plaintiffs and Class members and the websites to which they communicated.

135. Plaintiffs and the Class members seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

FOURTH CAUSE OF ACTION

Violation of the California Invasion of Privacy Act, Cal. Penal Code § 635
(Against Meta on behalf of the Class or, in the alternative, the California Subclass)

Plaintiffs incorporate the above paragraphs by reference and say–

136. CIPA § 635(a) prohibits the "manufacture[], assembl[y], s[ale], offer[] for sale, advertis[ment] for sale, possesses[ion], transport[], import[], or furnish[ing] to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another."

137. As described above, the Meta Pixel is a "device" that is "primarily or exclusively designed or intended for eavesdropping upon the communication of another."

138. Meta manufactured, assembled, sold, offered for sale, advertised for sale, possessed, transported, imported, and/or furnished the Meta Pixel device.

139. Meta's prohibited use of the Meta Pixel device in this way on numerous websites visited by Plaintiffs and members of the Class caused Plaintiffs and members of the Class harm, including but

not limited to loss of control of their personal information, invasion of their privacy, and Meta's unjust enrichment.

140. As a result, Plaintiffs and members of the Class are entitled to bring a claim for Meta's violation of CIPA § 635. See In re Meta Pixel Tax Filing Cases, 724 F. Supp. 3d 987, 1009 (N.D. Cal. 2024) (holding § 635 provides for parties to bring a private right of action for "injuries caused by use of an eavesdropping device are traceable to the manufacture, sale, and provision of that device," and finding allegations sufficient to plead the Meta Pixel is a device primarily designed for eavesdropping).

141. Neither Plaintiffs nor members of the Class provided their consent to Meta's manufacture, assembly, sale, offer for sale, advertisement for sale, possession, transport, import, and/or furnishing the Meta Pixel device for eavesdropping communications.

142. Plaintiffs and the Class members seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

FIFTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, *et seq.*
(Against Meta on behalf of the Class)

Plaintiffs incorporate the above paragraphs by reference and says–

143. Plaintiffs bring this claim individually and on behalf of the members of the Class against Meta.

144. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the contents of any wire, oral, or electronic communication without the consent of at least one of the parties to the communication.

145. ECPA protects both the sending and receipt of communications, and is designed to protect privacy in the face of changing technology.

146. ECPA provides a private right of action at 18 U.S.C. § 2520(a) for any person whose wire or electronic communication is intercepted, disclosed, intentionally used in violation of Chapter 119.

147. Section 2520 also provides for $10,000 in statutory damages for violation of ECPA.

148. The ECPA defines "intercept[ion]" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4).

149. "Electronic, mechanical or other device" means "any device or apparatus which can be used to intercept ... electronic communication[s]." Id. § 2510(5).

150. "[C]ontents," as to electronic communications, includes "any information concerning the substance, purport, or meaning of that communication." § 2510(8).

151. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." Id. § 2510(12).

152. Meta utilized its tracking technologies, including the Meta Tracking Pixel, cookies, and malicious code exploiting the Android software, are all "devices" under ECPA.

153. Meta used these devices to intentionally intercept, or endeavor to intercept, Plaintiffs' and Class members' communications between themselves and the websites they visited on their Android devices. Meta's conduct was intentional and malicious and was designed to unlawfully breach the privacy of Plaintiffs and Class members.

154. No party to the communication authorized, or was aware of, Meta's interception of Plaintiffs' and Class members' data for the purpose of breaching their privacy for advertising purposes.

This includes the website operators that Plaintiffs' and Class Members communicated with on their Android devices. In fact, Meta's conduct was a violation of Google's policies for Android.

155. Meta has the capability to, and does, use the communications intercepted in violation of 18 U.S.C. § 2511(1)(a) for its own advertising and analytics purposes for profit in violation of 18 U.S.C. § 2511(1)(d).

156. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages and attorney's fees and costs.

SIXTH CAUSE OF ACTION
Invasion of Privacy
(Against Defendants on behalf of the Class)

Plaintiffs incorporate the above paragraphs by reference and say—

157. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendants.

158. Plaintiffs and Class Members had a reasonable expectation of privacy in their browsing activity on their Android devices. Plaintiffs and Class members communicated information that they intended for only the websites they visited to receive and that they understood Defendants would not track and that would be kept private.

159. Defendants' tracking and disclosure of that information without the knowledge and consent of Plaintiffs and Class Members is an intrusion on Plaintiffs' and Class Members' solitude and seclusion.

160. Meta violated Plaintiffs' and Class members' privacy through intentional and malicious exploitation of software on their Android devices, while Google and Alphabet negligently allows these

intrusions and the disclosure of Plaintiffs' and Class members' private information and online browsing activity.

161. The level of invasion and systemic surveillance of Plaintiffs and Class members is highly offensive to a reasonable person. Meta designed malicious code to exploit vulnerabilities in Google's Android software that allowed Meta to collect Plaintiffs' and Class members' online activity over time and connect it with their identities. Meta then sold Plaintiffs' private information and identities for the purpose of profiting from targeted advertising. Google negligently permitted Meta to conduct this surveillance and breach of its code by failing, at minimum, to safeguard and monitor third-party developers such as Meta and Yandex.

162. Defendants profited from this invasive surveillance of Android users through sales of targeted advertising and sales of the defective Android software.

163. Defendants obtained Plaintiffs' and Class members' information under false pretenses and/or exceeded its authority to obtain such information.

164. As a result of Defendants' actions, Plaintiffs and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

165. Plaintiffs and Class members have been damaged as a direct and proximate result of Defendants invasion of their privacy and are entitled to just compensation, including monetary damages.

166. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests because of Defendants' intrusions upon Plaintiff's and Class members' privacy.

167. Plaintiffs and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

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

SEVENTH CAUSE OF ACTION
Negligence
(Against Google and Alphabet on behalf of the Class)

Plaintiffs incorporate the above paragraphs by reference and say—

169. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Google and Alphabet (collectively, "Google").

170. Google had a duty to implement reasonable data privacy protocols and policies in order to safeguard the privacy and security of Android users. This duty included, among other things, ensuring that any third-party developer, including Meta and Yandex, could not execute malicious code to form a covert connection between users' web browsing activity and their native applications which allowed Android users to be de-anonymized, as described above.

171. Indeed, Google affirmatively undertook the duty to safeguard consumers' Android devices by scanning, monitoring, and removing mobile apps from the Google Play store if they posed any security or privacy risk to consumers.

172. Google's position as the developer of Android software and approver of third-party code put it in a position of control, knowledge, and discretion regarding its privacy practices that Plaintiffs' and Class members' reasonably relied upon and required Google to implement adequate security and privacy protocols.

173. Google breached its duties in, including but not limited to, one or more of the following ways:

(a) Failing to implement reasonable data privacy measures for third-party app developers it allowed on Android;

(b) Failing to verify that the code implemented by Meta and Yandex was using the local device functions in an acceptable way;

(c) Failing to ensure that its developers were following any of Google's applicable privacy and security protocols and/or enforce those protocols;

(d) Inducing Android users to rely upon Google's representations about the ability of Android privacy controls and settings to prevent tracking and identification of online activity;

(e) Generally failing to act reasonably under the circumstances and failing to prevent, detect, or disclose the vulnerabilities in the Android software and the secret tracking by Meta and Yandex.

174. Plaintiffs and Class members were the foreseeable victims of Google's inadequate safety and security practices.

175. As a proximate and foreseeable result of Google's negligent conduct, Plaintiffs and Class members have suffered damages from the loss of control of their private information, loss of privacy, compromise of their private information, loss of the benefit of the bargain with Google, overpayment for their Android devices, and unjust enrichment by Google.

176. As a direct and proximate result of Google's negligence, Plaintiffs and Class members are entitled to recover actual, consequential, and nominal damages.

EIGHTH CAUSE OF ACTION

Violation of the Unfair Competition Law, Cal. Bus. & Prof. Code§ 17200, *et seq*.
(Against Google and Alphabet on behalf of the California Purchaser Subclass)

Plaintiffs incorporate the above paragraphs by reference and say—

177. Plaintiff Montanez brings this claim individually and on behalf of the members of the proposed California Purchaser Subclass against Google and Alphabet (collectively "Google").

178. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

179. Google engaged in unlawful business practices in connection with its misleading advertising regarding the safety and privacy protections available on Android devices, including Android users' ability to stay anonymous online.

180. The acts, omissions, and conduct of Google as alleged herein constitute "business practices" within the meaning of the UCL.

181. Defendant violated the "unlawful" prong of the UCL by violating, inter alia, Plaintiff Montanez's and Class members' constitutional rights to privacy, state privacy statutes, the CLRA, and state consumer protection statutes.

182. Google's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged therein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff Montanez and Class Members.

183. The harm caused by Google's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Google's legitimate business interests other than Google's conduct described therein.

184. As a result of Defendant's violations of the UCL, Plaintiff Montanez and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiff Montanez and Class Members information is ongoing.

185. As a direct and proximate result of Google's violations, Plaintiff Montanez and California Purchaser Subclass members have suffered injury in fact and lost money by purchasing

Android devices they would not have purchased or by paying price premiums they would not have paid had they known the truth about the Android security violations.

NINTH CAUSE OF ACTION
Violation of California's Consumer Legal Remedies Act Cal. Civ. Code §§ 1750 et seq.
(Against Google and Alphabet on behalf of the California Purchaser Subclass)

Plaintiff incorporates the above paragraphs by reference and says—

186. The California Consumers Legal Remedies Act ("CLRA") prohibits "unfair methods of competition and unfair or deceptive acts or practices ... undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770(a).

187. Google's and Alphabet's (collectively "Google") products – any device with Android software ("the Products") – are "goods" within the meaning of Cal. Civ. Code § 1761(a).

188. Google is a "person" within the meaning of Cal. Civ. Code § 1761(c).

189. Plaintiff Montanez and members of the California Purchaser Subclass are "consumers" within the meaning of Cal. Civ. Code § 1761(d).

190. Google violated and continues to violate the CLRA by engaging in the following practices proscribed by Cal. Civ. Code § 1770(a) in transactions with Plaintiff Montanez and members of the California Purchaser Subclass which were intended to result in, and did result in, the sale of the Products: (1) Representing that the Products have characteristics, benefits, or qualities that they do not have (§ 1770(a)(5)); (2) Representing that the Products are of a particular standard, quality, or grade when they are of another (§ 1770(a)(7)); and (3) Advertising goods with intent not to sell them as advertised (§ 1770(a)(9)).

191. Google's unfair or deceptive acts and practices were capable of deceiving a substantial portion of the California purchasing public.

192. Google's representations and omissions were material because they were likely to deceive reasonable consumers about the true nature of the Products. Specifically, Google negligently and/or recklessly failed to secure its Products to prevent unauthorized access to consumers' devices, while falsely claiming that its Products provides superior privacy protections, enables users control over their privacy, and de-identifies user data.

193. Google's uniform and material representations and omissions regarding the Products were likely to deceive, and Google knew or should have known that its representations and omissions were untrue and misleading.

194. Plaintiff Montanez and members of the California Purchaser Subclass could not have reasonably avoided such injury. Plaintiff Montanez and members of the California Purchaser Subclass were unaware of the existence of the facts that Google failed to disclose, and they would not have purchased the Products and/or would have purchased them on different terms had they known the truth.

195. Plaintiff Montanez and members of the California Purchaser Subclass suffered harm as a result of Google's violations because they relied on Google's representations that its Products provides sufficient privacy protections, enables users control over their privacy, and de-identifies user data. These privacy-related claims were a substantial factor in the purchasing decisions of Plaintiff Montanez and members of the California Purchaser Subclass. These privacy-related claims were material because a reasonable consumer would consider it important in deciding whether to purchase the Product.

196. As a direct and proximate result of Google's violations, Plaintiff Montanez and members of the California Purchaser Subclass have suffered harm in that they purchased Products they would not have purchased or paid significantly more than they would have paid had they known the truth about Google's representations.

197. Plaintiff Montanez, on behalf of herself and all class members, demands judgment against Google under the CLRA for injunctive relief to put an end to Google's violations. Plaintiff

Montanez has no adequate remedy at law. Without equitable relief, Google's unfair and deceptive practices will continue to harm Plaintiff Montanez and the California Purchaser Subclass.

198. Pursuant to Cal. Civ. Code § 1782(a), on January 17, 2025, Plaintiff Montanez intends to mail Google a notice of its alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date that Google receives that notification, Google fails to provide appropriate relief for its violations of the CLRA, Plaintiff Montanez reserves her rights to amend this Complaint to seek monetary damages.

199. Notwithstanding any other statements in this Complaint, Plaintiff Montanez does not seek monetary damages in conjunction with her CLRA claim—and will not do so—until this thirty-day period has passed.

PRAYER FOR RELIEF

200. Accordingly, Plaintiffs, on behalf of themselves and the proposed Class, respectfully requests that this Court grant judgment against the Defendants as follows:

(a) An order certifying the Class, naming Plaintiffs as representatives of the Class, and naming Plaintiffs' attorneys as Class Counsel to represent the Class.

(b) An order declaring that Defendant's conduct, as described above, violates California Penal Code §§ 502, 631, 635 and 638.51;

(c) An order finding in favor of Plaintiff and the Class on all counts;

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

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

(f) For an order of injunctive relief to remedy Defendants' violations;

(g) For an order of restitution and all other forms of equitable monetary relief; and

(h) For an order awarding and the Class their reasonable attorney's fees and expenses and costs of suit.

JURY DEMAND

Plaintiffs demand a trial by jury on all claims and issues so triable.

Dated: June 6, 2025

Respectfully submitted,

/s/ Matthew W. Ruan
Matthew W. Ruan (SBN 264409)
FREED KANNER LONDON
& MILLEN LLC
100 Tri-State International, Suite 128
Lincolnshire, IL 60069
Telephone: (224) 632-4500
mruan@fklmlaw.com

Katrina Carroll, Esq.*
Kyle Shamberg, Esq.*
CARROLL SHAMBERG LLC
111 West Washington Street Suite 1240
Chicago, IL 60602
Office: 872-215-6205
Mobile: 847-848-1384
katrina@csclassactions.com

*pro hac vice forthcoming

Attorneys for Plaintiffs and the Putative Class