LYNCH CARPENTER, LLP
(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Telephone: (626) 550-1250
Facsimile: (619) 756-6991

Gary F. Lynch (pro hac vice forthcoming)
gary@lcllp.com
Kelly K. Iverson (pro hac vice forthcoming)
kelly@lcllp.com
Jamisen A. Etzel (pro hac vice forthcoming)
jamisen@lcllp.com
Nicholas A. Colella (pro hac vice forthcoming)
nickc@lcllp.com
1133 Penn Ave, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

SARAH SIMPSON, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

APPLE, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

1. **Breach of Express Contract**
2. **Breach of Implied Contract**
3. **Breach of Implied Covenant of Good Faith and Fair Dealing**
4. **Violation of California's Unfair Competition Laws; Cal. Bus. & Prof. Code § 17200, *et seq*.**
5. **Violation of California's False Advertising Laws; Cal. Bus. & Prof. Code § 17500, *et seq*.**
6. **Violations of California Consumers Legal Remedies Act; Civ. Code § 1750, *et seq*.**

DEMAND FOR JURY TRIAL

Plaintiff Sarah Simpson brings this action on behalf of herself and all others similarly situated against Defendant Apple, Inc. ("Defendant" or "Apple"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

I. INTRODUCTION

1. Plaintiff brings this case to fight the rapid erosion of personal privacy rights due to pervasive corporate surveillance of consumers' internet activity. This is a proposed class action brought against Apple for allowing third parties to track users of its proprietary web browser, Safari, despite Apple's express representations of user privacy.

2. Internet-user trackers and analytics provide intimate portraits of individual consumers, and user browsing data is particularly valuable to advertisers. In today's market, data concerning consumers' habits, customs, and patterns are currency.

3. Apple claims in its advertisements that Safari is a private, secure web browser that does not disclose individuals' personal information. Further, Apple advertises Safari as having several anti-tracking features that prevent the identification of individual users by third parties as they browse the internet. These promises of privacy are illusory.

4. In reality, Safari transmits enormous amounts of user data to third parties, and its purported anti-tracking features still allow advertisers to follow consumers' every move as they browse the internet.

5. Safari transmits pieces of information about users' web browsers and devices to every website they visit as they browse the internet. This information is then related through what is called "fingerprinting." Fingerprinting allows websites and advertisers to track individual users by creating a unique profile for them. This profile is consistent from website to website. Fingerprints are shared by and between third party advertising and data providers, monetizing users' data and browsing habits without their consent. Users are fingerprinted even if they have taken measures in Safari to prevent themselves from being tracked, such as blocking cookies.

6. Apple has failed, and continues to fail, to provide the privacy protections it promises its users. Apple markets Safari as protecting users from tracking, including fingerprinting, but users

are easily fingerprinted in Safari's default browsing mode, fingerprinting scripts are not accurately flagged by Safari's Privacy Report in either default or Private Browsing, and fingerprinting scripts successfully load and execute in both default and Private Browsing modes.

7. Plaintiff and Class members reasonably relied on Apple's representations of the security and privacy of Safari. Based on Apple's representations, Plaintiff and Class members reasonably believed the data that individually identifies them would not be shared by Safari and that Apple's technology would protect them from being tracked by third parties.

8. Apple's practices disregard their consumers' privacy preferences and expectations. These practices infringe upon consumers' privacy; intentionally deceive consumers; give third parties power to learn intimate details about individuals' lives, interests, and web browser usage; and allow third parties to use consumers' browsing data for their own benefit. Through false advertisements, Apple represents to consumers that Safari prevents tracking while allowing third parties to track individual users.

9. Plaintiff brings this action individually and on behalf of a class of similarly situated individuals alleging Apple's conduct: (1) breaches express contracts; (2) breaches implied contracts; (3) breaches the implied covenant of good faith and fair dealing; (4) violates California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et. seq.* ("UCL"); (5) violates California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq.* ("FAL"); and (6) violates California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.* ("CLRA").

II. JURISDICTION AND VENUE

10. The Court has personal jurisdiction over the Defendant because Apple is incorporated and headquartered in the Northern District of California and does business in this district.

11. The Court has subject matter jurisdiction over the action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d), 1453, 1711–1715. Under § 1332(d)(2), the amount in controversy exceeds $5 million and at least one member of the proposed Class is a citizen of a state other than California. This Court is not prohibited from exercising jurisdiction over the action under § 1332(d)(4) because fewer than two thirds of the members of the proposed Class are citizens California.

12. Venue is proper in the United States District Court for the Northern District of California under 28 U.S.C. § 1391(b) because Defendant is domiciled in this district and the acts and omissions giving rise to Plaintiff and the Class's causes of action occurred in this district.

III. PARTIES

13. Plaintiff Sarah Simpson is a resident of California. Plaintiff uses Apple's proprietary web browser, Safari, to access the internet. Plaintiff uses Safari for its privacy features, including protection from fingerprinting.

14. Defendant Apple, Inc. is a multinational technology company incorporated and headquartered in Cupertino, California.

IV. FACTUAL ALLEGATIONS

A. Hundreds of millions of consumers access the internet through Apple's web browser, Safari.

15. Apple is one of the world's largest and most lucrative technology companies, reporting a 2025 fiscal year revenue of $416 billion. *Apple reports fourth quarter results*, Press Release, APPLE, https://www.apple.com/newsroom/2025/10/apple-reports-fourth-quarter-results/ (June 23, 2026). Apple manufactures and produces many of the most popular internet-connected devices, including the iPhone, Mac, iPad, and Apple Watch.

16. Part and parcel to each Apple device is Apple's proprietary web browser, Safari. Since 2012, Safari has been exclusively available on Apple devices and is the default web browser for any new Apple device.

17. The popularity of Apple's internet-connected devices ensures that Safari is the default browser used by hundreds of millions of people to browse the internet. The iPhone, Apple's smartphone, is one of the two largest smartphone platforms in the world, alongside Android. Apple sold approximately 237 million iPhones in the first three quarters of 2025. As of October 2025, Apple's share of the global smart phone market is 21.9%, and its share of the United States smart phone market is a stunning 57.3%. The projected number of iPhone users for 2025 is 1.56 billion. iPhone users now spend 5.6 hours per day on their devices, a 9% increase from 2024. Robert A. Lee,

iPhone Statistics 2025: Usage, Sales, and Market Dynamics, SQ MAGAZINE https://sqmagazine.co.uk/iphone-statistics/ (June 23, 2026).

18. In fiscal year 2025, sales of Macs, Apple's line of desktop computers and laptops, increased 13% year over year. Roman Loyola, *Apple posts record Q4 2025, with double-digit Mac sales increase*, MACWORLD, https://www.macworld.com/article/2958203/apple-posts-record-q4-2025-with-double-digit-mac-sales-increase.html (June 23, 2026).

19. In 2024, Apple's tablet, the iPad, held the largest market share in the global tablet market at 55.03%. Saisuman Revankar, *iPad Statistics by Sales, Revenue, Shipment, Model, Usage and Demographics*, COOLEST GADGETS, https://coolest-gadgets.com/ipads-statistics/ (last updated June 23, 2026).

20. The Apple Watch held just under 50% of the global smartwatch market share for the fiscal year 2024. In 2024, Apple led the United States smartwatch market with a 56% share. Pramod Pawar, *Apple Watch Statistics by Revenue, Sales, Series, Market Share, Country, Users and Usage*, COOLEST GADGETS, https://coolest-gadgets.com/apple-watches-statistics/ (last updated June 23, 2026).

21. Apple's internet-connected devices are the means by which hundreds of millions of consumers access the internet, both around the world and in the United States. Apple's internet-connected devices account for the majority of the corporation's revenue. Apple represents that its products protect the privacy of their users.

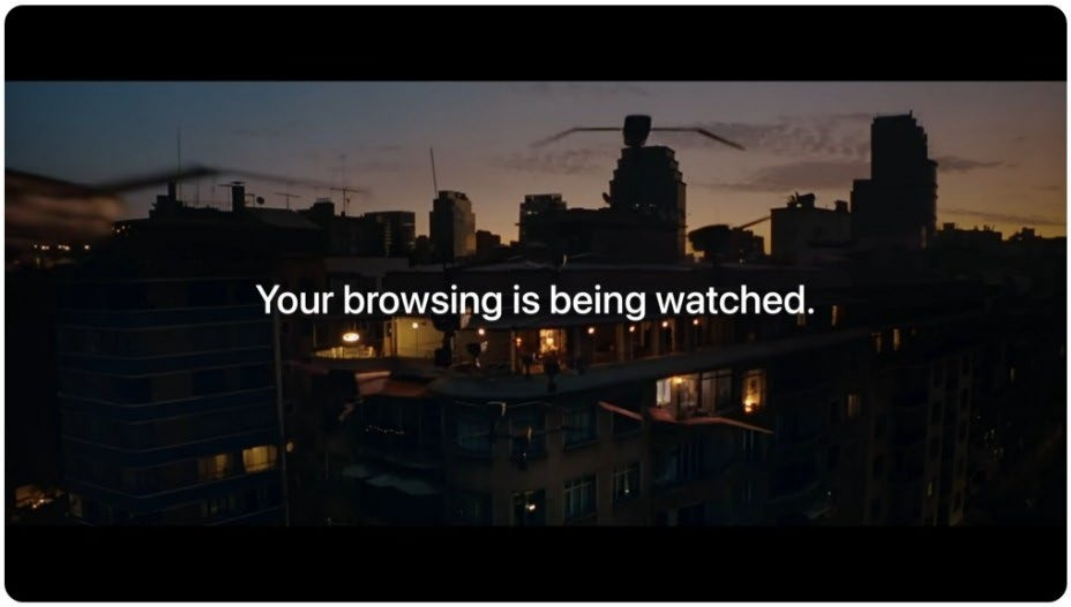
B. Apple markets its Safari web browser as having advanced privacy protections.

22. Consumers value their data privacy and increasingly find that safeguarding their privacy is critical in a virtual and interconnected society. People have become more aware and concerned that large corporations are tracking their activity, both on and off the internet, for profit.

23. In response to consumer concern, Apple has made privacy its brand, even going so far as saying: "Privacy. That's Apple." *Privacy*, APPLE, https://www.apple.com/privacy/ (last accessed June 23, 2026).

24. In addition to marketing the security of its devices, Apple touts the privacy features of Safari. Apple describes Safari as "Blazing Fast. Incredibly Private[,]" and states that "Safari comes

with industry-leading privacy protection technology built in, including Intelligent Tracking Prevention that identifies trackers and helps prevent them from profiling or following you across the web. And Private Browsing adds even more protections . . . . Online privacy isn't just something you should hope for—it's something you should expect." *Safari*, APPLE, https://www.apple.com/safari/ (last accessed June 23, 2026).



Privacy on iPhone | Flock | Apple

Apple 20.5M subscribers Subscribe 39K Share

20,280,136 views Jul 16, 2024 #PrivacyOniPhone #Privacy
Your browsing is being watched. Safari helps stop it. Using industry-leading privacy protection technology, including Intelligent Tracking Prevention — Safari protects your privacy.

25. Apple heavily markets Safari's purported anti-tracking features, detailing the ways in which Safari protects users from being identified and monitored at length on its website.

26. Recently, Apple launched an ad campaign centered on Safari's privacy features. The campaign includes billboards and TV spots that state: "Your browsing is being watched." Apple's official YouTube channel states "Your browsing is being watched. Safari helps stop it. Using industry-leading privacy protection technology, including intelligent tracking prevention—Safari protects your privacy." As of early 2026, the YouTube video of Apple's Safari ad had been viewed over 20 million times, indicating the breadth of Apple's audience.

27. Apple advertises Safari's "Intelligent Tracking Prevention" as using "machine learning and on-device intelligence to fight cross-site tracking. It hides your IP address from trackers so what you look at on the web remains your business—not an advertiser's. And you don't have to change any settings for these protections because Intelligent Tracking Prevention is on by default." *Privacy - Features*, APPLE, https://www.apple.com/privacy/features/ (last accessed June 23, 2026).

28. Safari also offers "Private Browsing." According to Apple, when a user activates Private Browsing in Safari, it "won't add the sites you visit to your history, remember your searches, or save any information from forms you fill out online[.]" *Id.*

29. In 2023, Apple announced that Private Browsing would include "[a]dvanced tracking and fingerprinting protections" that would "go even further to help prevent websites from using the latest techniques to track or identify a user's device." *Apple announces powerful new privacy and security features*, Press Release, APPLE, https://www.apple.com/au/newsroom/2023/06/apple-announces-powerful-new-privacy-and-security-features/ (June 23, 2026).

30. In 2025, Apple announced that Safari would become "even more private with advanced fingerprinting protection *extending to all browsing by default*." *Apple elevates the iPhone experience with iOS 26*, Press Release, APPLE, https://www.apple.com/newsroom/2025/06/apple-elevates-the-iphone-experience-with-ios-26/ (June 23, 2026) (emphasis added).

31. Apple promises that Safari produces a "Privacy Report" that "shows you all the cross-site trackers that are being blocked by Intelligent Tracking Prevention in Safari." *Privacy - Features*, APPLE, https://www.apple.com/privacy/features/ (last accessed June 23, 2026).

32. Apple further assures individual users they can disable cookies—small pieces of data that a server sends to an individual's device when they access a website, allowing the server to identify users and maintain information about their browsing activity—in Safari: "If you want to disable cookies and you're using the Safari web browser, choose 'Block all cookies' in Safari's privacy settings." *Apple Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (last accessed June 23, 2026).

C. "Fingerprinting" is a method of tracking individual users through web browsers.

33. Despite Apple promising that Safari's advanced privacy features protect individual users from being tracked, Safari transmits large amounts of identifying information from its users to third parties. Third parties utilize this information to track users through what is called "fingerprinting." Users are fingerprinted even if they have expressly taken measures to prevent data sharing, such as disabling cookies. Apple represents that Safari effectively prevents fingerprinting through the many anti-tracking features it contains by default, but this is not the case.

34. Fingerprinting allows websites to track an individual using pieces of data that a web browser routinely sends to each website that it loads, such as the make of the user's device, the device's operating system, downloaded software, web browser and version, default language settings, time zone, keyboard layout, and display settings, among others. Web browsers send these pieces of data without most users' knowledge. Jacob Roach, *Here's What Your Browser Is Telling Everyone About You*, WIRED, https://www.wired.com/story/what-is-browser-fingerprinting/ (June 23, 2026).

35. By themselves, these data points do not identify an individual user. When combined, they create an identifier that is unique enough to track individuals as they browse from website to website, thus bypassing the need to use IP addresses and cookies. *Id.*

36. Fingerprinting may be "passive" or "active." "Passive fingerprinting is browser fingerprinting based on characteristics observable in the contents of Web requests, without the use of any code executed on the client[.]" Characteristics of a web browser are "sent via Web requests in HTTP headers, meaning they can be collected by servers, exposing users to 'passive fingerprinting', without detection by browsers." Berke, et al., *How Unique is Whose Web Browser? The Role of Demographics in Browser Fingerprinting among US Users*, 2025 PROC. ON PRIV. ENHANCING TECH. 1, at 724, https://petsymposium.org/popets/2025/popets-2025-0038.pdf.

37. Passive fingerprinting is especially difficult to combat because "[t]he most uniquely identifying attributes" of a web browser include User agent and Language. *Id.* at 728.

38. Active fingerprinting occurs "where a site runs JavaScript or other code on the local client to observe additional characteristics about the browser, user, device or other context." World

Wide Web Consortium, *Mitigating Browser Fingerprinting in Web Specifications*, W3C Group Note, https://www.w3.org/TR/fingerprinting-guidance/#types-of-fingerprinting (June 23, 2026).

39. Active fingerprinting "might include accessing the window size, enumerating fonts or connected devices, evaluating performance characteristics, reading from device sensors, and rendering graphical patterns. Key to this distinction is that active fingerprinting takes place in a way that is potentially detectable on the client." In most cases, however, "the characteristics are sent en masse to a server, which can combine them in unobservable ways." *Id*.

40. Unlike cookies, which web browsers and websites may allow users to block, there is nothing a user can do to completely prevent fingerprinting without significantly compromising the functioning of their web browser. For instance, if a user disables JavaScript (the code that collects the majority of web browser data), many websites will not function altogether. *Id.*

41. Active fingerprinting methods are used by third parties to identify individual website visitors. "Canvas fingerprinting," defined below, can produce a nearly unique signature for an individual user.

42. In its November 2019 "Safari Privacy Overview," Apple stated that "[t]o combat fingerprinting, Safari presents a simplified version of the system configuration to trackers so more devices look identical, making it harder to single one out. And unlike some other browsers, Safari doesn't add any custom tracking headers or unique identifiers to web requests." According to Apple, this "dramatically reduces data companies' ability to identify a single device uniquely—and all without compromising the web-browsing experience." *Safari Privacy Overview: Learn How the Safari web browser protects your privacy*, APPLE https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf (Nov. 2019).

43. Further, Apple claims that "fingerprinting defense [is] turned on by default, so there is no need to make changes in Settings or Safari preferences to benefit from these privacy protections." *Id.*

D. Safari does not prevent fingerprinting by default, identify fingerprinting scripts in its Privacy Report, or stop transmitting trackable information in Private Browsing.

44. When Apple launched iOS 26 and macOS 26 in 2025, it claimed that it was extending Safari's advanced fingerprinting protection to "all browsing by default."

45. However, even after the launch of Safari 26, individual users can easily be fingerprinted by fingerprinting scripts in Safari's default browsing mode.

46. Safari's default settings provide no defenses against canvas fingerprinting, which allows third parties to gather information about how invisible or subtle content on the canvas element of a browser is drawn, revealing characteristics specific to a user's hardware and software. Hoang Dai Nguyen and Phani Vadrevu, *Breaking the Shield: Analyzing and Attacking Canvas Fingerprinting Defenses in the Wild*, PROC. OF THE ACM WEB CONF. 2025, at 4339, https://dl.acm.org/doi/pdf/10.1145/3696410.3714713 (April 28 – May 2, 2025).

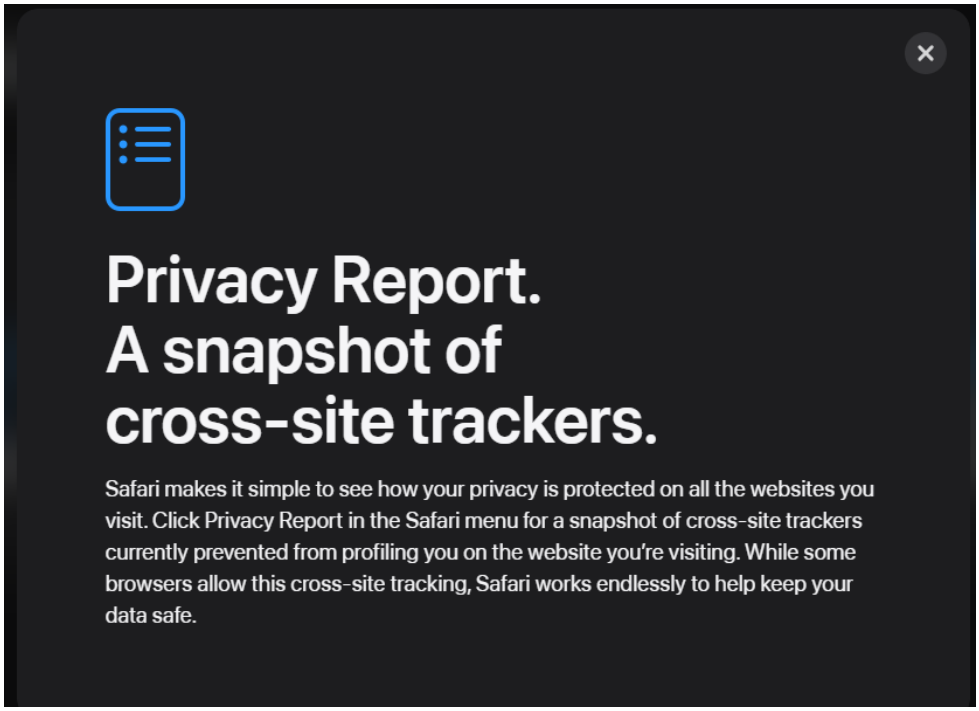
47. Canvas fingerprinting is the most precise fingerprinting method for identifying individual users. Canvas fingerprinting scripts embedded on websites can identify individual users by telling their browsers to invisibly draw complex shapes, text, or other graphical elements on the canvas element of the browser. The script then records these differences and generates a unique digital signature.

48. The website can then identify the user by this digital signature even if the user closes the browser and returns to the page later.

49. If multiple websites have embedded the same commercial canvas fingerprinting script, the individual user can be recognized across websites.

50. Despite Apple's express representations that advanced fingerprinting protection operates in Safari "by default," Safari's default settings do not protect users from canvas fingerprinting at all. On the contrary, in Safari 26, users browsing in default mode must affirmatively make changes in Safari's settings to enable any kind of fingerprinting protection. Before users can even enable canvas fingerprinting protection, they must find the appropriate settings to change—something that the average consumer is unlikely to know how to do.

51. Safari's "Privacy Report" further misleads consumers and lulls them into a false sense of security. Apple describes the Safari "Privacy Report" as "a snapshot of cross-site trackers currently prevented from profiling you on the website you're visiting. While some browsers allow this cross-site tracking, Safari works endlessly to keep your data safe." *Safari - Privacy*, APPLE, https://www.apple.com/safari/privacy/ (last accessed June 23, 2026).

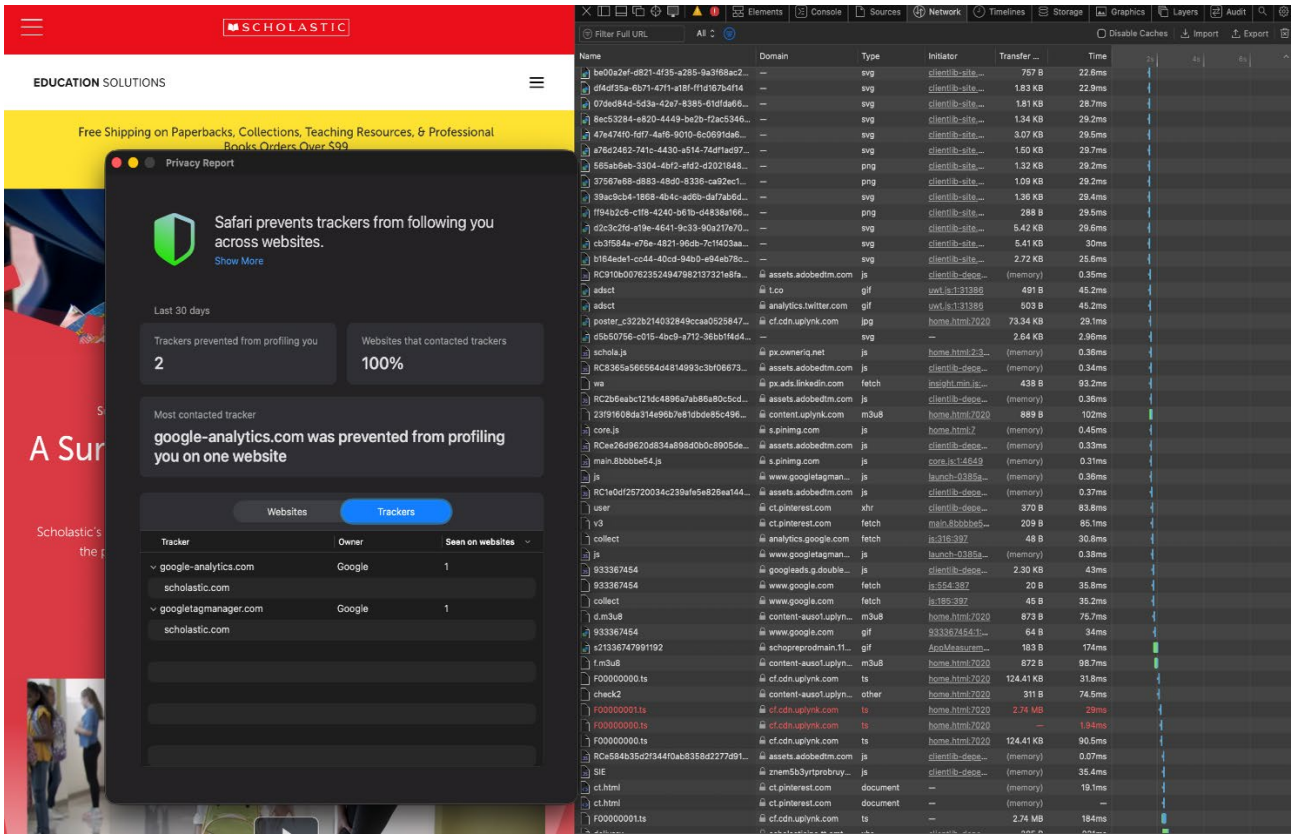


52. When a new tab is opened in Safari, it prominently displays the "Privacy Report," stating "Safari prevents trackers from profiling you." This language implies that Safari protects users from all online tracking.

53. The Privacy Report further promises that "Safari defends against common fingerprinting techniques for any website you visit."

54. The Privacy Report also represents that "[i]n Private Browsing, connections are blocked to data collection companies that use advanced fingerprinting techniques and known tracking parameters are removed from all URLs."

55. However, the Privacy Report does not show well-known fingerprinting scripts such as Adobe in its list of trackers detected in default browsing mode, even on websites where the Adobe tracking script is present.



Screenshot of Privacy Report in default browsing mode on the left; on the right, the "Network" tab from Safari's developer tools shows loaded tracking scripts not listed in the Privacy Report, including Adobe.

56. What is more, tracking scripts such as Adobe still successfully load and execute on the Safari web browser in Private Browsing.

57. For instance, if a user visits a website with Adobe's script embedded on it while in Private Browsing mode, the Privacy Report states that Adobe is one of the trackers that is "blocked from profiling you."

58. In fact, the Adobe script executes successfully. If a user subsequently visits another website in the same Private Browsing session that incorporates the Adobe tracking script, Adobe can successfully identify the individual user across those websites.

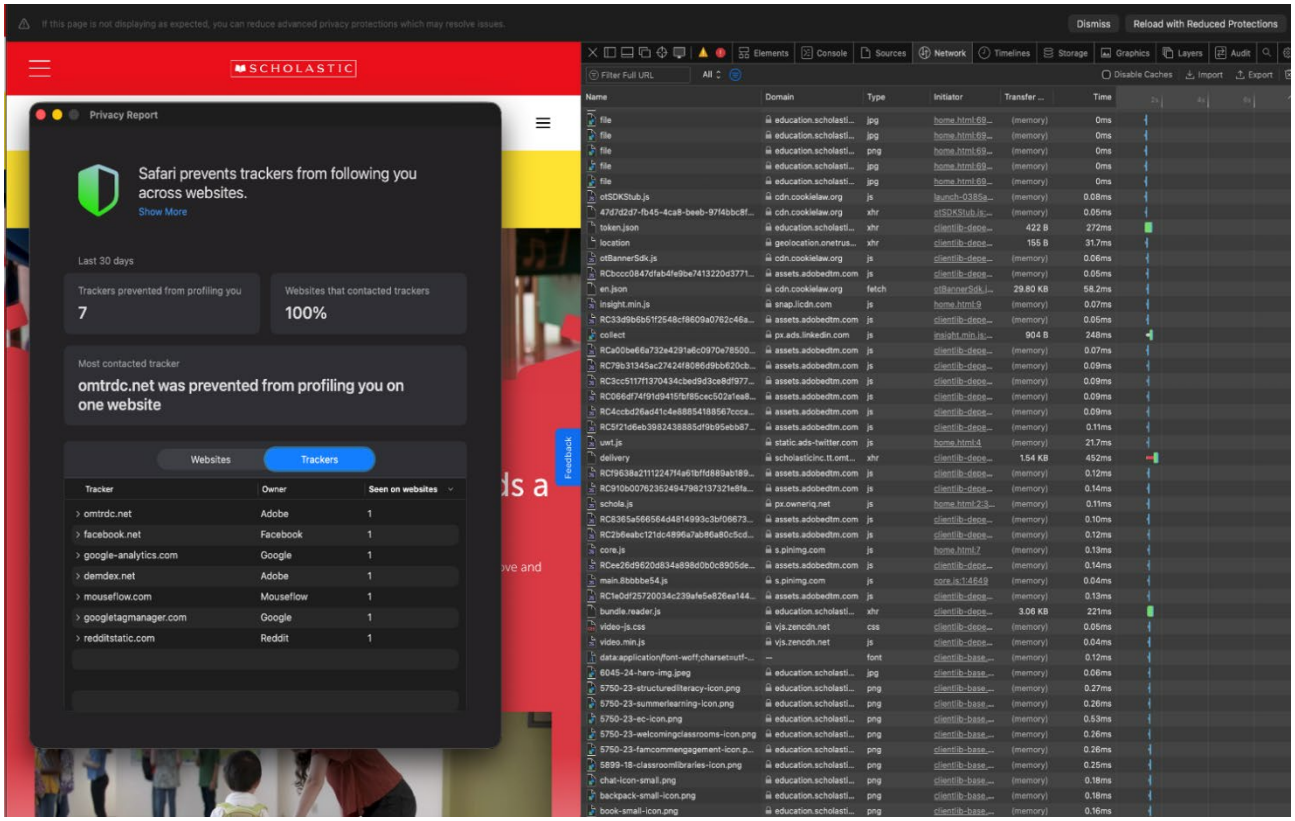
59. Even in Private Browsing, the Adobe script successfully transmits information such as the webpage URL, page name, screen and browser dimensions, a marketing identifier, a persistent visitor identifier, and a session/correlation identifier—all of which contribute to third parties' ability to determine that the same user is visiting a website across different domains, effectively tracking that user's behavior.

60. Adobe can also successfully set identity cookies in Private Browsing, indicating that identifying users by tracking cookies is still possible.

61. Despite Apple's representations that in Private Browsing, "connections are blocked to data collection companies that use advanced fingerprinting techniques[,]" the Adobe script successfully requests WebGL contexts and gathers individual web browser data such as user agent, language settings, time zone, screen width, screen height, screen orientation, color depth, pixel ratio, window width, and window height, all parameters that are commonly used in fingerprinting.

62. Therefore, neither Safari's default browsing mode nor its Private Browsing mode live up to Apple's promises about Safari's fingerprinting defenses.

63. Further, the Privacy Report is highly misleading. A reasonable consumer would understand that a tracker listed in the Privacy Report had been completely blocked, but when the Privacy Report listed Adobe as blocked in Private Browsing mode, the script continued to transmit the user's identifiable information.



Screenshot of Privacy Report in Private Browsing listing Adobe as a blocked tracker on the left; on the right, the "Network" tab from Safari's developer tools shows loaded tracking scripts, including Adobe.

E. Fingerprints are used for profiling.

64. Fingerprinting does more than identify devices. A 2025 study found that "user demographics, such as gender, age, income level and race, can be inferred from browser attributes commonly used for fingerprinting[.]" Berke, et al., at 720.

65. What is more, the study found that fingerprinting is "used on more than a third of the top 500 US websites." *Id.*

66. In their investigation of whether fingerprinting varies by demographic group, Berke, et al. observed that the language attribute of a web browser leads to greater ease of fingerprinting of self-identified Hispanic users and non-white users. Self-identified lower income users and older users were found to be more susceptible to fingerprinting overall. The study even showed that a user's demographic information can be successfully inferred from web browser attributes such as screen resolution, User agent, and how the browser displays colors. *Id.* at 728–30.

67. The ramifications of fingerprinting are greater than users merely receiving targeted ads; when web browser attributes are used to infer demographic information, users are at risk of targeted information campaigns. *Id.* at 731.

68. Fingerprinting is therefore pervasive, detrimental, intrusive, and contrary to Apple's claims about Safari's capabilities, often impossible to protect against.

F. Users' fingerprints are monetized without their consent.

69. Fingerprinting is also extremely lucrative. In a 2025 study, researchers examined "whether browser fingerprints are indeed adopted for online tracking, thus violating web privacy." The study found "evidence that browser fingerprinting is indeed utilized in advertisement tracking and targeting." Liu, et al., *The First Early Evidence of the Use of Fingerprinting for Online Tracking*, PROC. OF THE ACM WEB CONF. 2025, https://spies.engr.tamu.edu/wp-content/uploads/sites/239/2025/03/Browser_fingerprints_in_Advertisement__Copy_.pdf (Apr. 28–May 2, 2025).

70. Header bidding is a method employed by website publishers to designate specific advertising spaces on their websites for potential advertisers. The advertiser securing the highest bid has the chance to display their ads in the corresponding slots. Advertisers with knowledge of users through data syncing tend to submit higher bid values. Liu., et al. found that browser fingerprinting

significantly influenced the amount advertisers bid for header spots. "Based on our analysis of bid values and HTTP events, we can draw the conclusion that browser fingerprinting indeed plays a significant role in targeting and tracking within the realm of advertising." *Id.*

71. Apple benefits directly from third parties' advertising business. In 2023 proceedings against Google by the Department of Justice, it was revealed that Google sends 36% of the advertising revenue it makes on the Safari web browser to Apple. *Google sends a third of Safari ad revenue to Apple*, BBC (Nov. 14, 2023), https://www.bbc.com/news/business-67417987.

G. Plaintiff's allegations.

72. Plaintiff Sarah Simpson is a citizen of California. She purchased two new iPhones from Apple in 2025.

73. Plaintiff Simpson accesses the internet using her iPhone and primarily uses iPhone's default web browser, Safari.

74. Plaintiff Simpson values her online privacy. She saw Apple's advertisements promising that Apple protects users' privacy as they browse the internet and reasonably believed that Apple's products, including Safari, would do so for her.

V. CLASS ALLEGATIONS

75. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action individually and on behalf of a class of similarly situated individuals defined as follows:

> All persons residing in the United States who purchased an Apple device with the Safari web browser pre-installed.

Excluded from the Class are Defendant, its officers, employees, agents or affiliates, and any judge who presides over this action, as well as all past and present employees, officers and directors of Defendant. Plaintiff reserves the right to expand, limit, modify, or amend this class definition, including the addition of one or more subclasses, in connection with their motion for class certification, or at any other time, based upon, *inter alia*, changing circumstances and/or new facts obtained during discovery.

76. **Numerosity:** The Class members are so numerous that joinder of all members is impractical. Plaintiff is informed and believes that the proposed Class contains millions of individuals

who have been damaged by Apple's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff.

77. **Existence and Predominance of Common Questions of Law and Fact:** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant breached an express contract with Plaintiff and the Class;

b. whether Defendant breached an implied contract with Plaintiff and the Class;

c. whether Defendant's alleged conduct constitutes violations of the laws asserted herein;

d. whether Defendant engaged in unfair, unlawful and/or fraudulent business practices under the laws asserted;

e. whether Defendant engaged in false or misleading advertising;

f. whether Plaintiff and the Class are entitled to damages and/or restitution and the proper measure of that loss; and

g. whether an injunction is necessary to prevent Defendant from continuing to use false, misleading or illegal advertising and allowing Safari users to be fingerprinted.

78. **Typicality:** Plaintiff's claims are typical of the claims of the Class members because, *inter alia*, all Class members have used the Safari web browser and have been deceived (or were likely to be deceived) by Apple's false and deceptive advertisements as alleged herein. Plaintiff is advancing the same claims and legal theories on behalf of herself and all Class members.

79. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff has retained counsel who are experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff has no antagonistic or adverse interests to those of the Class.

80. **Superiority:** The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action format a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged. The damages or other financial detriment

suffered by individual Class members are relatively modest compared to the burden and expense that individual litigation of their claims against Apple would entail. It would thus be virtually impossible for Plaintiff and the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Absent the class action, Class members and the general public would not likely recover or would not likely have the chance to recover damages or restitution, and Apple will be permitted to retain the proceeds of its misconduct.

81. All Class members, including Plaintiff, were exposed to one or more of Apple's misrepresentations relating to the privacy features of Safari. Due to the scope and extent of Apple's advertising scheme, which has been disseminated to United States consumers over many years, it can be reasonably inferred that such misrepresentations were uniformly made to all members of the Class. In addition, it can be reasonably presumed that all Class members, including Plaintiff, affirmatively acted in response to the representations contained in Apple's false advertising scheme when using the Safari web browser.

82. Apple keeps extensive computerized records of its customers through, *inter alia*, Apple user accounts. Apple has one or more databases through which a significant majority of Class members may be identified and ascertained, and it maintains contact information, including phone numbers and email addresses, through which notice of this action could be disseminated in accordance with due process requirements.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Breach of Express Contract
(On behalf of Plaintiff and the Class)

83. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

84. Plaintiff brings this claim individually and on behalf of the Class.

85. Generally, the elements for a breach of contract claim are as follows: "(1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to the plaintiff." *Oasis W. Realty, LLC v. Goldman*, 250 P.3d 1115, 1121 (Cal. 2011).

86. Apple's contract with Plaintiff and the Class incorporates the Privacy page of Apple's website, any user agreements accompanying Plaintiff's and the Class's use of Apple devices, and Apple's public representations about the Safari web browser.

87. Apple promises that Safari will prevent third parties from tracking Plaintiff and the Class as they browse the internet because "Safari comes with industry-leading privacy protection technology built in, including Intelligent Tracking Prevention that identifies trackers and helps prevent them from profiling or following you across the web."

88. Apple further promises that Safari's "[a]dvanced tracking and fingerprinting protections" extends to "all browsing by default."

89. Plaintiff fully performed her obligations under the agreement by purchasing Apple products and using Safari to browse the internet.

90. Despite promising Plaintiff and the Class that their browsing activity would not be tracked, Apple breached the contract by allowing Safari users to be fingerprinted in default browsing mode, allowing fingerprinting scripts to load, execute, and install tracking cookies on users' browsers in Private Browsing, and failing to identify fingerprinting scripts in Safari's "Privacy Report."

91. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class members have suffered and will continue to suffer injury, including but not limited to the premium they paid for Apple products in the belief that they would be protected from tracking and other damages to be determined at trial.

92. Plaintiff and the Class seek damages to compensate for the detriment caused by Apple's breach of the express contract between the parties, including: (1) general damages; (2) special or consequential damages; (3) nominal damages; (4) and, if applicable, attorneys' fees.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

93. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

94. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Count I.

95. The existence and terms of an implied contract are manifested by the parties' conduct. Cal. Civ. Code § 1621.

96. An implied contract consists of obligations arising from mutual agreement and intent to promise even though the agreement and promise have not been expressed in words.

97. Like an express contract claim, the elements of an implied-in-fact contract claim are (1) a valid implied-in-fact contract, (2) the plaintiff's performance or excuse for nonperformance, (3) the defendant's breach of the agreement, and (4) the resulting damages to the plaintiff.

98. The nature of the agreement, as detailed in the foregoing paragraphs, between Plaintiff, Class members, and Apple was established through Apple's marketing materials, website, and privacy features on the Safari web browser. The totality of Apple's statements in these documents, to the extent they are not ultimately deemed part of the express contract, creates an implied contract that Apple would protect Plaintiff and the Class from being tracked as they browsed the internet.

99. By representing that Safari includes "Intelligent Tracking Prevention that identifies trackers and helps prevent them from profiling or following you across the web" Apple made an implied promise that Safari would protect users from third-party internet trackers.

100. By representing that that Safari would become "even more private with advanced fingerprinting protection extending to all browsing by default" Apple made an implied promise to prevent Safari users from being fingerprinted in default browsing mode.

101. By representing in Safari's Privacy Report that "[w]hile some browsers allow this cross-site tracking, Safari works endlessly to keep your data safe[,]" Apple made an implied promise that Safari is capable of preventing all third-party tracking.

102. Plaintiff and the Class fully performed their obligations under the agreement by purchasing Apple products and browsing the internet using Safari.

103. Defendant breached its implied contracts with Plaintiff and the Class by allowing third parties to gather information commonly used in fingerprinting as they browsed the internet using Safari despite users taking express steps to prevent tracking, such as browsing in Safari's "Private Browsing" mode.

104. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class have suffered and will continue to suffer injury, including but not limited to the premium they paid for Apple products in the belief that they would be protected from tracking and other damages to be determined at trial.

105. Plaintiff and the Class seek damages to compensate for the detriment caused by Apple's breach of the implied contract between the parties, including: (1) general damages; (2) special or consequential damages; (3) nominal damages; (4) and, if applicable, attorneys' fees.

THIRD CAUSE OF ACTION
Breach of Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Class)

106. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

107. Plaintiff brings this claim individually and on behalf of the Class.

108. Plaintiff and the Class entered into a contract with Apple, as alleged above. Implied in this contract was a promise between the Parties not to unfairly interfere with the rights of the other party to receive the benefits of the contract.

109. Plaintiff and the Class performed their obligations under the contract by purchasing Apple devices and using the Safari web browser in exchange for what they believed were comprehensive privacy protections.

110. Apple prevented Plaintiff and the Class from receiving the benefit of the contract not only by failing to provide the promised tracking protections in the Safari web browser, but also by affirmatively representing to Plaintiff and the Class that Safari was protecting against fingerprinting by representing that "advanced fingerprinting protection extend[s] to all browsing by default" and by listing certain trackers as blocked in its "Privacy Report" when in fact they were not.

111. Apple falsely represented to Plaintiff and the Class that it was performing its obligations under the contract by, among other representations, displaying the Privacy Report in Safari containing a list of supposedly blocked trackers, creating a false sense of security on the part of Plaintiff and the Class. In fact, Safari does not detect common fingerprinting scripts and does not flag them in its Privacy Report.

112. Further, despite representing that "[i]n Private Browsing, connections are blocked to data collection companies that use advanced fingerprinting techniques and known tracking parameters are removed from all URLs[,]" third-party scripts that are widely known to track users, such as Adobe, can fully load, execute, gather information that can be used in fingerprinting, and place tracking cookies on users' browsers in Private Browsing mode.

113. In so doing, Apple did not act fairly or in good faith.

114. Plaintiff and the Class were harmed by Apple's conduct because they fully performed on but did not receive the benefit of the agreement between the Parties. Plaintiff was intentionally misled into believing Apple was performing its end of the agreement through the representations in, for example, the Privacy Report.

115. Apple breached the implied covenant of good faith and fair dealing in its agreement with Plaintiff and the Class. Plaintiff and the Class seek damages for Apple's breach, including: (1) general damages; (2) special or consequential damages; (3) nominal damages; and (4) punitive damages.

FOURTH CAUSE OF ACTION
Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiff and the Class)

116. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

117. Plaintiff brings this claim individually and on behalf of the Class.

118. Apple is a "person" as that term is defined by Cal. Bus. & Prof. Code § 17201.

119. Defendant violated the UCL by engaging in unlawful, unfair, and deceptive business acts and practices in relation to its practice of allowing users of the Safari web browser to be tracked by third parties.

120. Defendant's unlawful, unfair, and deceptive acts and practices include, as detailed above, but are not limited to:

a. leading users to believe that Safari blocks third party trackers, including fingerprinting scripts, while Safari transmits identifiable information without users' knowledge or consent; and

b. misrepresenting that it would protect the privacy of Plaintiff and the Class who used the Safari web browser and took steps to prevent third-party tracking, including using Safari's "Private Browsing" mode. Apple employed a systematic marketing campaign in which Defendant represented to customers that they would not be tracked when they used Safari. Defendant further omitted, suppressed, and/or concealed the material fact that Safari's default privacy features do not protect users from fingerprinting.

121. Defendant's misrepresentations led to injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition as contemplated under the UCL. Because Plaintiff and the Class members did not and could not know that Safari allows third-party tracking through fingerprinting, they could not have reasonably avoided the harm caused by Defendant's practices.

122. Defendant's misrepresentations to Plaintiff and the Class were material because they were likely to deceive reasonable individuals about the nature and effectiveness of Safari's privacy features.

123. Defendant intended to mislead Plaintiff and the Class as well as induce them to rely on its representations about the privacy features of Safari in order to sell its products.

124. If Apple had disclosed to Plaintiff and the Class that third parties could track their browsing activity through fingerprinting, that the Privacy Report does not identify fingerprinting scripts, and that fingerprinting scripts can load, execute, and place tracking cookies on users' browsers, even in "Private Browsing" mode, Defendant could have continued its business without falling afoul of the law. However, Defendant transmitted Plaintiff's and the Class's identifiable data without advising them that Apple allows third parties to track them without their knowledge. Accordingly, Plaintiff and the Class acted reasonably in relying on Defendant's misrepresentations that Safari would protect them from tracking, including fingerprinting.

125. Defendant acted intentionally, knowingly, and maliciously to violate the UCL in reckless disregard of Plaintiff's and the Class's rights.

126. Without such misrepresentations, Plaintiff and Class members would not have used Defendant's products or would have paid less for them. Plaintiff and the Class have lost money due to Apple's violation of the UCL.

127. As a direct and proximate result of Defendant's violations of the UCL, Plaintiff and the Class sustained actual losses and damages as described herein.

128. Plaintiff and the Class seek restitution, injunctive relief, and other and further relief as the Court may deem just and proper. To the extent any of these remedies are equitable, Plaintiff seeks them in the alternative to any adequate remedy at law available to them.

FIFTH CAUSE OF ACTION
Violation of California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, *et seq*.
(On behalf of Plaintiff and the Class)

129. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

130. Plaintiff brings this claim on behalf of themselves and the Class.

131. Cal. Bus. & Prof. Code § 17500 provides:

> It is unlawful for any . . . corporation . . . to make or disseminate or cause to be made or disseminated . . . from this state before the public in any state, in any newspaper or other publication, or any advertising device, or by public outcry or proclamation, or in any other manner or means whatever, including over the Internet, any statement…which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading[.]

132. Defendant advertises Safari as preventing tracking by third parties through advanced privacy features. Defendant targets Plaintiff and the Class with this message through ads and through the representations on its website.

133. Defendant misled consumers by making untrue and misleading statements regarding Safari's ability to prevent fingerprinting and failing to disclose material facts as required by Cal. Bus. & Prof. Code § 17500.

134. As a direct and proximate result of Defendant's misleading and false advertisements, Plaintiff and Class members have suffered injury in fact by paying a premium for Apple products that they would not have otherwise paid. Plaintiff and the Class have lost money due to Apple's violation of the FAL.

135. As such, Plaintiff requests that this Court order Apple to disgorge the benefit it received through its misleading advertisements and enjoin Apple from continuing its unfair practices in violation of the FAL. Otherwise, Plaintiff, Class members, and the broader general public, will be irreparably harmed and/or denied an effective and complete remedy.

136. Plaintiff and the Class seek restitution, injunctive relief, and other and further relief as the Court may deem just and proper. To the extent any of these remedies are equitable, Plaintiff seeks them in the alternative to any adequate remedy at law available to them.

SIXTH CAUSE OF ACTION
Violation of California's Consumers Legal Remedies Act, Civ. Code § 1750, *et seq.*
(On behalf of Plaintiff and the Class)

137. Plaintiff incorporates the allegations set forth in paragraphs 1 through 82.

138. This cause of action is brought pursuant to the CLRA, Cal. Civ. Code § 1750, *et seq*. Plaintiff and each member of the proposed Class are "consumers" as defined by Cal. Civ. Code § 1761(d). Apple's sale of products with Safari pre-installed to Plaintiff and the Class were "transactions" within the meaning of Cal. Civ. Code § 1761(e). The products purchased by Plaintiff and the Class are "goods" within the meaning of Cal. Civ. Code § 1761(a).

139. Defendant violated and continues to violate the CLRA by engaging in the following practices proscribed by Cal. Civ. Code § 1770(a) in transactions with Plaintiff and the Class which were intended to result in, and did result in, the sale of its merchandise:

a. advertising goods or services with intent not to sell them as advertised; and

b. making false or misleading statements of fact concerning the privacy features of Safari.

140. As a direct and proximate result of Defendant's misleading and false advertisements, Plaintiff and Class members have suffered injury in fact by paying a premium for Apple products that they would not have otherwise paid.

141. Plaintiff and the Class have suffered damage as a result of the use or employment by any Defendant of a practice declared to be unlawful by § 1770(a) and seek to recover the following: (1) actual damages, but a total award of no less than one thousand dollars ($1,000); (2) an order

enjoining Apple's deceptive practices; (3) punitive damages; and (4) any other relief that the court deems proper.

142. Pursuant to Cal. Civ. Code §1780(a), Plaintiff seeks an order enjoining such methods, acts, or practices as well as any other relief the Court deems proper. Plaintiff additionally seeks costs and reasonable attorneys' fees pursuant to Cal. Civ. Code § 1780(e).

143. Plaintiff, through counsel, will send a CLRA demand letter by certified mail to Defendant that provides notice of Defendant's violation of the CLRA as alleged herein, and demand that Defendant notify all members of the Class and correct, repair, replace, or otherwise rectify the unlawful, unfair, false, and deceptive practices complained of herein. If Defendant does not respond to Plaintiff's letter and agree to rectify the problems associated with the actions detailed above and give notice to all affected consumers within 30 days of the date of written notice pursuant to § 1782, Plaintiff will amend this complaint to seek actual, punitive, and statutory damages, as appropriate against Defendant.

VII. PRAYER FOR RELIEF

144. Wherefore, Plaintiff, on behalf of herself and on behalf of the other members of the Class, requests that this Court award relief against Apple as follows:

a. order certification of the Class and designate Plaintiff as Class Representative and her counsel as Class Counsel;

b. award Plaintiff and the proposed Class members damages, including but not limited to actual, general, special or consequential, nominal, and/or punitive damages;

c. award disgorgement of all profits that Apple obtained from Plaintiff and the Class members as a result of its unlawful, unfair, and fraudulent business practices described herein;

d. award declaratory and injunctive relief as permitted by law or equity;

e. order Apple to engage in a corrective advertising campaign;

f. Award attorneys' fees and costs, including under California Code of Civil Procedure Section 1021.5; and

g. Such other and further relief as the Court may deem necessary or appropriate.

VIII. DEMAND FOR JURY TRIAL

145. Plaintiff hereby demands a jury trial for all claims so triable.

Dated: June 24, 2026

LYNCH CARPENTER, LLP

By: */s/ (Eddie) Jae K. Kim*

(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
9171 Towne Centre Dr, Ste 180
San Diego, CA 92122
Telephone: (619) 762-1910
Facsimile: (858) 313-1850

Gary F. Lynch (pro hac vice forthcoming)
gary@lcllp.com
Kelly K. Iverson (pro hac vice forthcoming)
kelly@lcllp.com
Jamisen A. Etzel (pro hac vice forthcoming)
jamisen@lcllp.com
Nicholas A. Colella (pro hac vice forthcoming)
nickc@lcllp.com
1133 Penn Ave, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246