

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

6 Gary F. Lynch (pro hac vice forthcoming)  
gary@lcllp.com  
7 Kelly K. Iverson (pro hac vice forthcoming)  
kelly@lcllp.com  
8 Jamisen A. Etzel (pro hac vice forthcoming)  
jamisen@lcllp.com  
9 Nicholas A. Colella (pro hac vice forthcoming)  
nickc@lcllp.com  
10 1133 Penn Ave, 5th Floor  
Pittsburgh, PA 15222  
11 Telephone: (412) 322-9243  
12 Facsimile: (412) 231-0246

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

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

16 Plaintiff,

17 vs.

18 APPLE, INC.,

19 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**

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

5 **I. INTRODUCTION**

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

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

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

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

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

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

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

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

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

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

20 **II. JURISDICTION AND VENUE**

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

23 11. The Court has subject matter jurisdiction over the action pursuant to the Class Action  
24 Fairness Act of 2005, 28 U.S.C. §§ 1332(d), 1453, 1711–1715. Under § 1332(d)(2), the amount in  
25 controversy exceeds \$5 million and at least one member of the proposed Class is a citizen of a state  
26 other than California. This Court is not prohibited from exercising jurisdiction over the action under  
27 § 1332(d)(4) because fewer than two thirds of the members of the proposed Class are citizens  
28 California.

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

4 **III. PARTIES**

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

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

10 **IV. FACTUAL ALLEGATIONS**

11 **A. Hundreds of millions of consumers access the internet through Apple’s web browser,  
12 Safari.**

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

18 16. Part and parcel to each Apple device is Apple’s proprietary web browser, Safari. Since  
19 2012, Safari has been exclusively available on Apple devices and is the default web browser for any  
20 new Apple device.

21 17. The popularity of Apple’s internet-connected devices ensures that Safari is the default  
22 browser used by hundreds of millions of people to browse the internet. The iPhone, Apple’s  
23 smartphone, is one of the two largest smartphone platforms in the world, alongside Android. Apple  
24 sold approximately 237 million iPhones in the first three quarters of 2025. As of October 2025,  
25 Apple’s share of the global smart phone market is 21.9%, and its share of the United States smart  
26 phone market is a stunning 57.3%. The projected number of iPhone users for 2025 is 1.56 billion.  
27 iPhone users now spend 5.6 hours per day on their devices, a 9% increase from 2024. Robert A. Lee,  
28

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

3 18. In fiscal year 2025, sales of Macs, Apple’s line of desktop computers and laptops,  
4 increased 13% year over year. Roman Loyola, *Apple posts record Q4 2025, with double-digit Mac*  
5 *sales increase*, MACWORLD, [https://www.macworld.com/article/2958203/apple-posts-record-q4-](https://www.macworld.com/article/2958203/apple-posts-record-q4-2025-with-double-digit-mac-sales-increase.html)  
6 [2025-with-double-digit-mac-sales-increase.html](https://www.macworld.com/article/2958203/apple-posts-record-q4-2025-with-double-digit-mac-sales-increase.html) (June 23, 2026).

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

11 20. The Apple Watch held just under 50% of the global smartwatch market share for the  
12 fiscal year 2024. In 2024, Apple led the United States smartwatch market with a 56% share. Pramod  
13 Pawar, *Apple Watch Statistics by Revenue, Sales, Series, Market Share, Country, Users and Usage*,  
14 COOLEST GADGETS, <https://coolest-gadgets.com/apple-watches-statistics/> (last updated June 23,  
15 2026).

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

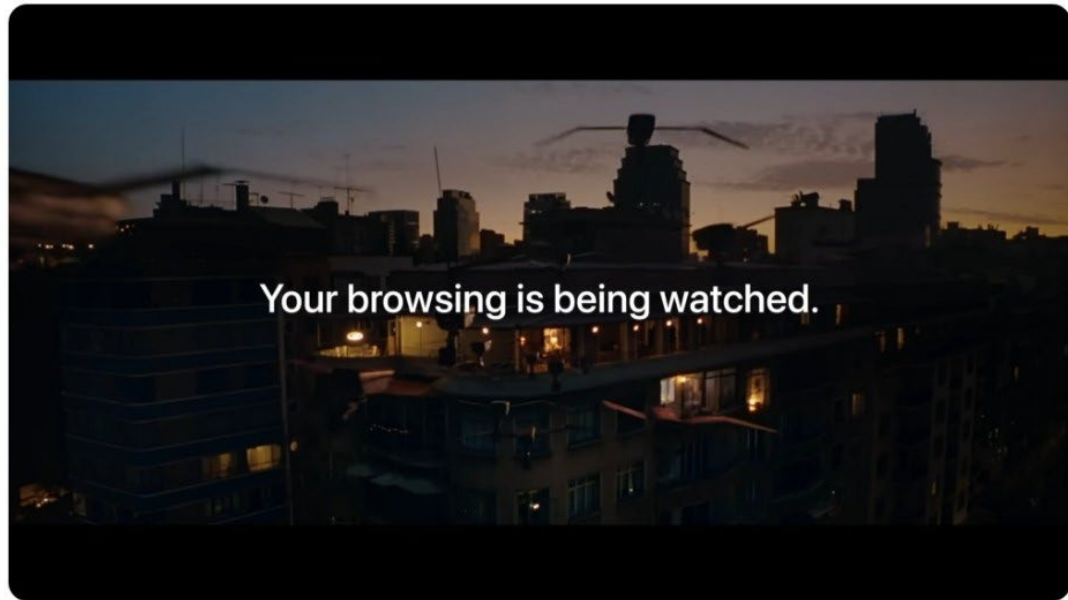
20 **B. Apple markets its Safari web browser as having advanced privacy protections.**

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


24 23. In response to consumer concern, Apple has made privacy its brand, even going so far  
25 as saying: “Privacy. That’s Apple.” *Privacy*, APPLE, <https://www.apple.com/privacy/> (last accessed  
26 June 23, 2026).

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

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



6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16 **Privacy on iPhone | Flock | Apple**

17  **Apple** ✓  
20.5M subscribers   39K   Share 

18  
19 20,280,136 views Jul 16, 2024 #PrivacyOniPhone #Privacy  
20 Your browsing is being watched. Safari helps stop it. Using industry-leading privacy protection  
technology, including Intelligent Tracking Prevention – Safari protects your privacy.

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

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

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

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

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

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

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

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

27  
28

1 **C. “Fingerprinting” is a method of tracking individual users through web browsers.**

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

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

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

17 36. Fingerprinting may be “passive” or “active.” “Passive fingerprinting is browser  
18 fingerprinting based on characteristics observable in the contents of Web requests, without the use of  
19 any code executed on the client[.]” Characteristics of a web browser are “sent via Web requests in  
20 HTTP headers, meaning they can be collected by servers, exposing users to ‘passive fingerprinting’,  
21 without detection by browsers.” Berke, et al., *How Unique is Whose Web Browser? The Role of*  
22 *Demographics in Browser Fingerprinting among US Users*, 2025 PROC. ON PRIV. ENHANCING TECH.  
23 1, at 724, <https://petsymposium.org/popets/2025/popets-2025-0038.pdf>.

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

26 38. Active fingerprinting occurs “where a site runs JavaScript or other code on the local  
27 client to observe additional characteristics about the browser, user, device or other context.” World  
28

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

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

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

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

15 42. In its November 2019 “Safari Privacy Overview,” Apple stated that “[t]o combat  
16 fingerprinting, Safari presents a simplified version of the system configuration to trackers so more  
17 devices look identical, making it harder to single one out. And unlike some other browsers, Safari  
18 doesn’t add any custom tracking headers or unique identifiers to web requests.” According to Apple,  
19 this “dramatically reduces data companies’ ability to identify a single device uniquely—and all  
20 without compromising the web-browsing experience.” *Safari Privacy Overview: Learn How the*  
21 *Safari web browser protects your privacy*, APPLE [https://www.apple.com/safari/docs/Safari\\_White\\_](https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf)  
22 [Paper\\_Nov\\_2019.pdf](https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf) (Nov. 2019).

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

26  
27  
28

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

3 44. When Apple launched iOS 26 and macOS 26 in 2025, it claimed that it was extending  
4 Safari’s advanced fingerprinting protection to “all browsing by default.”

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

7 46. Safari’s default settings provide no defenses against canvas fingerprinting, which  
8 allows third parties to gather information about how invisible or subtle content on the canvas element  
9 of a browser is drawn, revealing characteristics specific to a user’s hardware and software. Hoang Dai  
10 Nguyen and Phani Vadrevu, *Breaking the Shield: Analyzing and Attacking Canvas Fingerprinting*  
11 *Defenses in the Wild*, PROC. OF THE ACM WEB CONF. 2025, at 4339, [https://dl.acm.org/doi/pdf/10.](https://dl.acm.org/doi/pdf/10.1145/3696410.3714713)  
12 [1145/3696410.3714713](https://dl.acm.org/doi/pdf/10.1145/3696410.3714713) (April 28 – May 2, 2025).

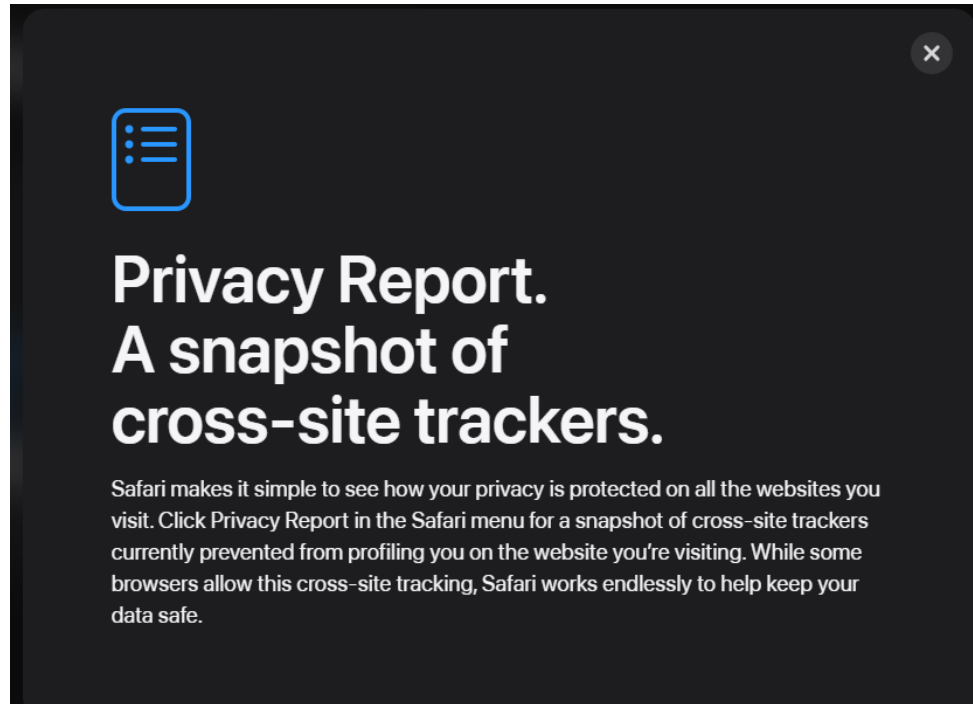
13 47. Canvas fingerprinting is the most precise fingerprinting method for identifying  
14 individual users. Canvas fingerprinting scripts embedded on websites can identify individual users by  
15 telling their browsers to invisibly draw complex shapes, text, or other graphical elements on the  
16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

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

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

22 50. Despite Apple’s express representations that advanced fingerprinting protection  
23 operates in Safari “by default,” Safari’s default settings do not protect users from canvas  
24 fingerprinting at all. On the contrary, in Safari 26, users browsing in default mode must affirmatively  
25 make changes in Safari’s settings to enable any kind of fingerprinting protection. Before users can  
26 even enable canvas fingerprinting protection, they must find the appropriate settings to change—  
27 something that the average consumer is unlikely to know how to do.  
28

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

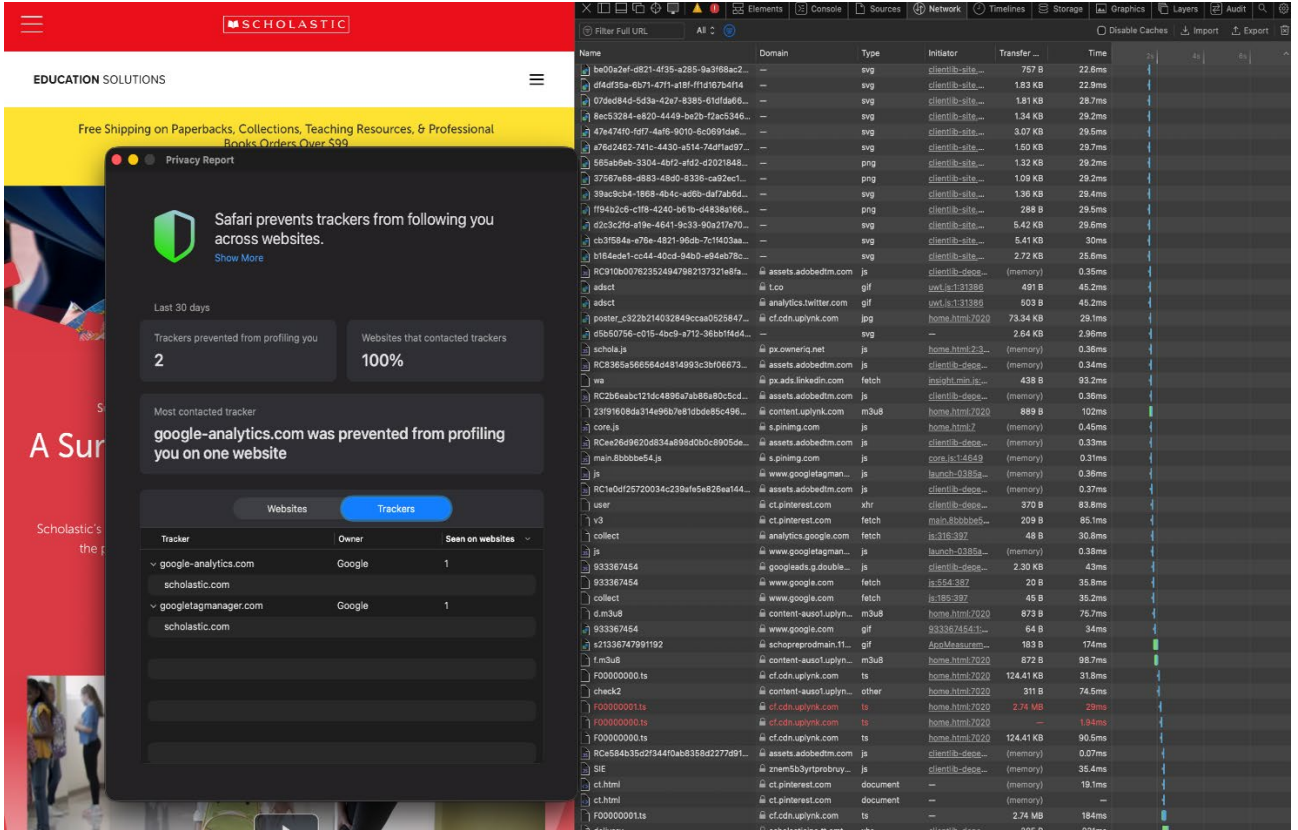


6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18 52. When a new tab is opened in Safari, it prominently displays the “Privacy Report,”  
19 stating “Safari prevents trackers from profiling you.” This language implies that Safari protects users  
20 from all online tracking.

21 53. The Privacy Report further promises that “Safari defends against common  
22 fingerprinting techniques for any website you visit.”

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

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



14 *Screenshot of Privacy Report in default browsing mode on the left; on the right, the “Network” tab*  
 15 *from Safari’s developer tools shows loaded tracking scripts not listed in the Privacy Report,*  
 16 *including Adobe.*

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

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

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

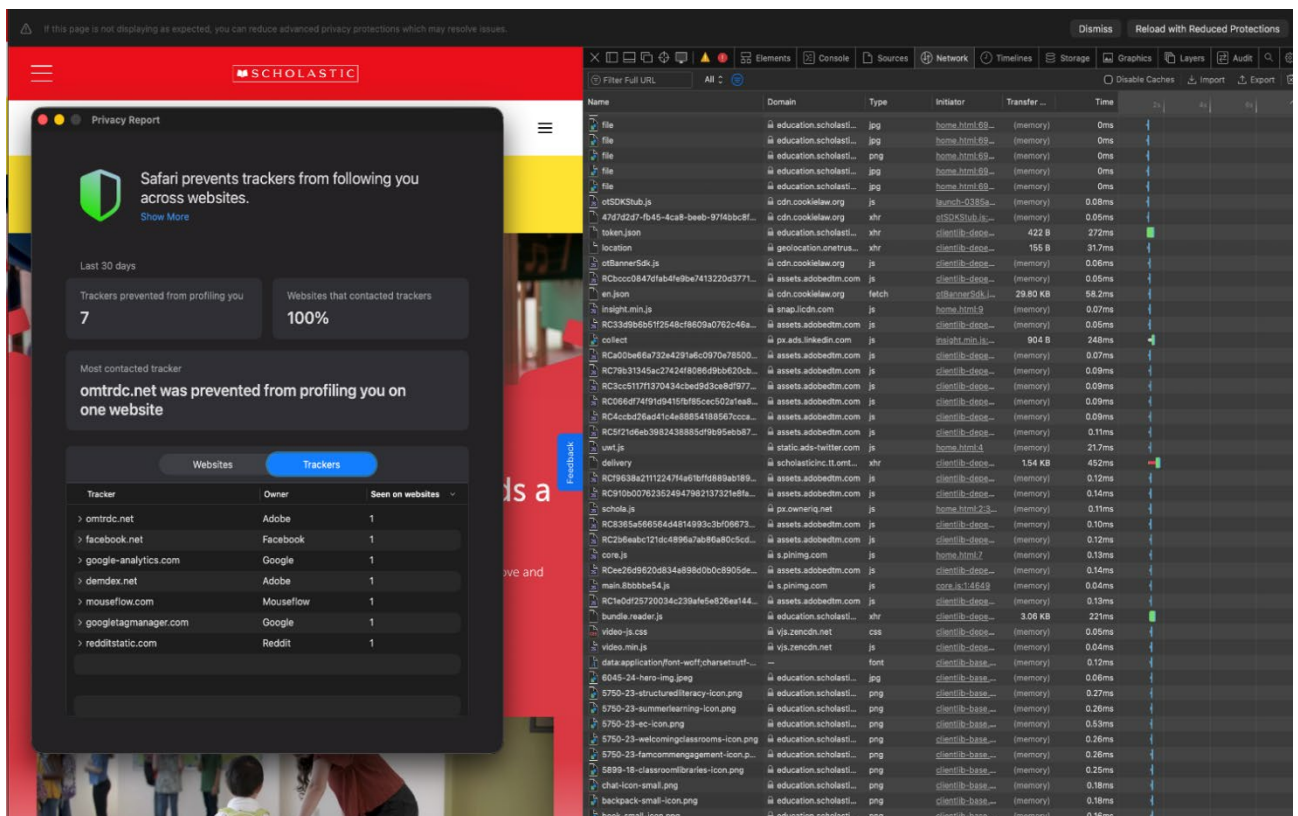
25 59. Even in Private Browsing, the Adobe script successfully transmits information such  
 26 as the webpage URL, page name, screen and browser dimensions, a marketing identifier, a persistent  
 27 visitor identifier, and a session/correlation identifier—all of which contribute to third parties’ ability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

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

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

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

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



14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27 *Screenshot of Privacy Report in Private Browsing listing Adobe as a blocked tracker on the left;*  
28 *on the right, the “Network” tab from Safari’s developer tools shows loaded tracking scripts,*  
*including Adobe.*

1 **E. Fingerprints are used for profiling.**

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

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

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

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

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

18 **F. Users’ fingerprints are monetized without their consent.**

19 69. Fingerprinting is also extremely lucrative. In a 2025 study, researchers examined  
20 “whether browser fingerprints are indeed adopted for online tracking, thus violating web privacy.”  
21 The study found “evidence that browser fingerprinting is indeed utilized in advertisement tracking  
22 and targeting.” Liu, et al., *The First Early Evidence of the Use of Fingerprinting for Online Tracking*,  
23 PROC. OF THE ACM WEB CONF. 2025, [https://spies.engr.tamu.edu/wp-content/uploads/sites/239/  
24 2025/03/Browser\\_fingerprints\\_in\\_Advertisement\\_Copy\\_.pdf](https://spies.engr.tamu.edu/wp-content/uploads/sites/239/2025/03/Browser_fingerprints_in_Advertisement_Copy_.pdf) (Apr. 28–May 2, 2025).

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

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

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

8 **G. Plaintiff’s allegations.**

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

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

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

16 **V. CLASS ALLEGATIONS**

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

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

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

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

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

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

- 7 a. whether Defendant breached an express contract with Plaintiff and the Class;
- 8 b. whether Defendant breached an implied contract with Plaintiff and the Class;
- 9 c. whether Defendant’s alleged conduct constitutes violations of the laws asserted  
10 herein;
- 11 d. whether Defendant engaged in unfair, unlawful and/or fraudulent business  
12 practices under the laws asserted;
- 13 e. whether Defendant engaged in false or misleading advertising;
- 14 f. whether Plaintiff and the Class are entitled to damages and/or restitution and  
15 the proper measure of that loss; and
- 16 g. whether an injunction is necessary to prevent Defendant from continuing to  
17 use false, misleading or illegal advertising and allowing Safari users to be fingerprinted.

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

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

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

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

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

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

## 19 VI. CAUSES OF ACTION

### 20 FIRST CAUSE OF ACTION 21 **Breach of Express Contract** **(On behalf of Plaintiff and the Class)**

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

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

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

28

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

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

8 88. Apple further promises that Safari’s “[a]dvanced tracking and fingerprinting  
9 protections” extends to “all browsing by default.”

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

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

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

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

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

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

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

28

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

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

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

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

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

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

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

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

24 103. Defendant breached its implied contracts with Plaintiff and the Class by allowing third  
25 parties to gather information commonly used in fingerprinting as they browsed the internet using  
26 Safari despite users taking express steps to prevent tracking, such as browsing in Safari's "Private  
27 Browsing" mode.  
28

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 a. leading users to believe that Safari blocks third party trackers, including  
26 fingerprinting scripts, while Safari transmits identifiable information without users’  
27 knowledge or consent; and  
28

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

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

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

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

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

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

27  
28

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

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

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

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

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

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

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

14 It is unlawful for any . . . corporation . . . to make or disseminate or cause to be made  
15 or disseminated . . . from this state before the public in any state, in any newspaper or  
16 other publication, or any advertising device, or by public outcry or proclamation, or in  
17 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[.]

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

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

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

28

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

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

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

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

12 138. This cause of action is brought pursuant to the CLRA, Cal. Civ. Code § 1750, *et seq.*  
13 Plaintiff and each member of the proposed Class are “consumers” as defined by Cal. Civ. Code  
14 § 1761(d). Apple’s sale of products with Safari pre-installed to Plaintiff and the Class were  
15 “transactions” within the meaning of Cal. Civ. Code § 1761(e). The products purchased by Plaintiff  
16 and the Class are “goods” within the meaning of Cal. Civ. Code § 1761(a).

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

- 20 a. advertising goods or services with intent not to sell them as advertised; and
- 21 b. making false or misleading statements of fact concerning the privacy features  
22 of Safari.

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

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

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

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

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

14 **VII. PRAYER FOR RELIEF**

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

- 17 a. order certification of the Class and designate Plaintiff as Class Representative  
18 and her counsel as Class Counsel;
- 19 b. award Plaintiff and the proposed Class members damages, including but not  
20 limited to actual, general, special or consequential, nominal, and/or punitive damages;
- 21 c. award disgorgement of all profits that Apple obtained from Plaintiff and the  
22 Class members as a result of its unlawful, unfair, and fraudulent business practices described  
23 herein;
- 24 d. award declaratory and injunctive relief as permitted by law or equity;
- 25 e. order Apple to engage in a corrective advertising campaign;
- 26 f. Award attorneys’ fees and costs, including under California Code of Civil  
27 Procedure Section 1021.5; and
- 28 g. Such other and further relief as the Court may deem necessary or appropriate.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**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

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Apple Class Action Lawsuit Claims Safari Users Are Tracked Despite Advertised Privacy Protections](#)

---