Robert G. Loewy (SBN 179868)
rloewy@rloewy.com
LAW OFFICES OF ROBERT G. LOEWY, P.C.
20 Enterprise, Suite 310
Aliso Viejo, CA 92656
Tel: (949) 468-7150

Eric S. Dwoskin (*pro hac vice* forthcoming)
DWOSKIN WASDIN LLP
433 Plaza Real, Ste. 275
Boca Raton, Florida 33432
Tel.: 561-849-8060
edwoskin@dwowas.com

Attorneys for Plaintiff Vedat Asrak and the Proposed Classes

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

VEDAT ASRAK, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

SAMSUNG ELECTRONICS AMERICA, INC., a New York corporation; and DOES 1-100, inclusive.

Defendants.

Case No.: 25STCV10293

CLASS ACTION COMPLAINT FOR:

(1) VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT
(2) INVASION OF PRIVACY;
(3) INTRUSION UPON SECLUSION;
(4) CAL. UNFAIR COMPETITION LAW
(5) UNJUST ENRICHMENT;
(6) VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
(7) VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Vedat Asrak, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Samsung Electronics America, Inc. (Defendant or "Samsung"), to put an end to its unlawful collection, use and disclosure of Plaintiff's and Class members' private data and communications. Plaintiff, on behalf of himself and all others similarly situated, upon personal knowledge as to Plaintiff's own conduct, and on information and belief as to all other matters, including based on an investigation by counsel, complains and alleges as follows:

NATURE OF THE ACTION

1. This is a class action against Defendant for violating Plaintiff's and Class members' privacy rights under California law by collecting, using and disclosing Plaintiff's and Class members' personal data and communications via analytical and tracking technology on Defendant's website.

2. Defendant operates the website https://www.samsung.com/us/ (the "Website").

3. The Website is configured such that, when it is first accessed by a user, a pop-up consent banner titled "Samsung and Cookies" appears on the page. The consent banner: (a) states that the Website "uses cookies to personalise your experience, analyse site traffic and keep track of items stored in your shopping basket;" and (b) includes a link for the user to reject the Website's use of such cookies.

4. The link takes the user to Samsung's Privacy and Cookie Preference Center. Once there, Website users are told that the Website uses two types of technologies: (1) "strictly necessary cookies," which Samsung defines as those cookies that are "necessary for the website to function and cannot be switched off in our systems"; and (2) "share or sale of personal information," which category includes "cookies, website trackers and similar technologies" that "collect and disclose"

information to "third parties" for "targeted ads and for analytics purposes." Website users are given the option of disabling the latter but not the former.

5. The tracking technologies that users can disable on the Website are pieces of code that are placed on users' computers. Once there, the technologies collect data on users' online browsing behavior and disclose that information to third-party marketing companies, which use it to, among other things, create profiles of individual users to target them with advertising across the internet.

6. Many consumers, including Plaintiff, prefer their online activities to not be subject to tracking and surveillance, and thus opted to deactivate tracking technology on the Website.

7. Based on Defendant's representations, and their reasonable expectations for privacy, Plaintiff and Class members reasonably believed that, once they elected to disable tracking cookies, their data and communications with the Website would not be collected and disclosed via tracking technologies.

8. Unbeknownst to Plaintiff and other consumers, Defendant used tracking technologies to collect and disclose user's browsing activity and communications with the Website, even after the user opted to disable those technologies through the process described above.

9. Thus, throughout the Class Period, Defendant: (a) told Website users that tracking technologies would not be installed on their computers if they opted to disable those technologies; but (b) nevertheless installed those technologies on users' computers and used them to collect and disclose users' browsing histories and communications with the Website, even after users expressly declined to consent to such tracking.

10. Defendant's practices infringe upon users' privacy; intentionally deceive consumers; and give Defendant and its employees and third-party marketing companies the power to learn private details about Defendant's customers' interests

and internet browsing history that Defendant promised would not be tracked and disclosed.

THE PARTIES

11. Plaintiff Vedat Asrak is a resident of Los Angeles, California. Within the last two years, Plaintiff visited Defendant's Website. Plaintiff opted to disable online tracking technologies on the Website. Despite Plaintiff's selection to disable tracking technologies, Defendant still deployed tracking technologies on Plaintiff's computer and used those technologies to collect and disclose Plaintiff's personal data and communications with the Website to third parties. Plaintiff did not consent to the installation of these tracking technologies on his computer, or these technologies' subsequent collection and disclosure of his personal data and communications. After Plaintiff disabled tracking technologies on the Website, Plaintiff noticed targeted advertising from Defendant related to Defendant's products and services.

12. Defendant Samsung Electronics America, Inc. is a company formed under the laws of New York with its headquarters located at 85 Challenger Road, Ridgefield Park, NJ 07660. Defendant owns and operates the Website.

13. Plaintiff is genuinely ignorant of the identities of the Defendants he has named as DOES 1-100, inclusive, and therefore sues such Defendants by fictitious names. Plaintiff is informed and believes and thereon alleges that each of DOES 1-100 is liable for the conduct alleged herein as an agent, partner, co-conspirator, alter ego, joint tortfeasor or in some other manner is legally responsible for the facts set forth herein. Plaintiff will amend this Complaint to state the true names of DOES 1-100 once ascertained. Each reference to "Defendant" in this Complaint also refers to DOES 1-100.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to Article VI, section 10 of the California Constitution and Cal. Code Civ. Proc. § 410.10.

This action is brought as a class action on behalf of Plaintiff and Class Members pursuant to Cal. Code Civ. Proc. § 382.

15. This Court has personal jurisdiction over Defendant. First, as noted above, Defendant offers its Website to consumers in California and ships its products to consumers in California. Thus, Defendant has availed itself of the privilege of doing business in California. Second, when Plaintiff and other California class members accessed the Website from their computers in California, Defendant installed the tracking technologies at issue on those users' computers in California. Third, the tracking technologies installed on Website users' computers in California caused Plaintiff's and California class members' personal data and communications with the Website to be intercepted in California (because the interception occurred on the users' computers in California) and sent to third-party marketing companies, such as Google and Adobe, that were also located in California.

16. This Court is the proper venue for this action under Cal. Code Civ. Proc. § 395.5 because the tracking technologies were placed on Plaintiff's computer in this County, and Plaintiff's personal data and communications with the Website were unlawfully intercepted in, and disclosed to third parties from, this County. Thus, a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this County.

COMMON FACTUAL ALLEGATIONS

A. Website Functionality & Tracking Technologies

17. When an individual uses a web browser to navigate to a website, a number of communications occur between the user's computer and the server that hosts the website.

18. Internet users access websites via web browsers installed on their computers. When an individual uses a web browser to navigate to a website, a number of communications occur between the user's computer and the server that hosts the website, including, among many other things: (a) a "GET request" sent from the user's

computer to the website server, which tells the server what information is being requested and instructs the server to send the information back to the web browser on the user's computer; (b) a "POST request" sent from the website server to the user's computer, which contains the information requested in the GET request and instructions for how the web browser should present the requested information on the user's computer; (c) the URL of the requested web page, which is sent back and forth from the user's web browser and the website server; and (d) information on the requesting user and device. This series of requests and responses is a type of electronic communication.

19. In addition to exchanging the above communications with users' computers, websites can also cause tracking technologies (sometimes referred to as "cookies," "pixels," or "beacons") to be installed on the accessing users' computer. These technologies are small files that the website places on the user's web browser to collect data about the user's online activity. These technologies work by assigning or associating the user with a unique identifier, storing that identifier and other information about the user within the cookie file (*e.g.*, geographic location, device specifications, etc), gathering data on the user's activity on the website in real time, and transmitting that data to either the website host or a third party. The primary reason websites use these technologies is to track user's activity and interests on the website and enable the website host to analyze user's use of the website and subsequently serve the website user with targeted advertising across the internet. Tracking technologies are not strictly necessary for a website to function, and many websites can and do function without them.

20. Many tracking technologies are created by third-party analytics and marketing companies, such as Google, Adobe, Akamai, Medallia, Bazaar Voice, and Teads. These companies develop the tracking technologies and then offer them to website hosts, who can integrate them into their websites to track user activity online. These technologies collect data on the user's online activity (including the

communications the user's web browser exchanges with the web server hosting the website, such as the GET and POST requests and the URLs the user is requesting and viewing), and send that data to the third party to be used for analytical and marketing purposes, including to create profiles of the user's browsing histories and preferences to facilitate the creation of custom audiences for the website host's marketing on the associated third-party marketing platform or for other pecuniary purposes.

21. Through the use of tracking technologies, much internet browsing activity is collected and stored in sophisticated databases. As information associated with a particular individual is aggregated over time, third party marketing companies can create detailed profiles of the individual's likes and dislikes that can be used to target the individual with "relevant" advertising across many different websites and platforms.

22. In light of the pervasive use of tracking technologies, consumers browsing the internet today are concerned with maintaining the privacy of their personal data and communications, including those related to their website browsing history. Businesses, in turn, often make representations to consumers regarding any tracking technologies they use and the data they either do or do not collect. Consumers care about the promises businesses make on what data the businesses will or won't collect. Legislators and courts have become increasingly aware of online threats to consumer privacy, too, and many laws have been passed or interpreted to protect the privacy of users' personal data and communications online.

23. To comply with new laws like the California Consumer Privacy Act (the "CCPA") and Europe's General Data Privacy Regulation (the "GDPR"), businesses—like Defendant's—represent that users have control over what information is collected, used, and shared with third parties and that users can prevent the business from tracking their browsing history and collecting their personal data and communications online. One way that businesses purport to provide website users control over their data is through pop-up banners or processes (like Samsung's Privacy and Cookie Preference

Center) soliciting users' consent to collect, analyze, track, and disclose information collected by tracking technologies. These banners or processes are sometimes referred to as "consent banners."

B. Defendant's Website & Use of Tracking Technologies

24. Defendant operates the Website https://www.samsung.com/us/.

25. The Website is configured such that, when it is first accessed by a user, a pop-up consent banner titled "Samsung and Cookies" appears on the page. The consent banner: (a) states that the Website "uses cookies to personalise your experience, analyse site traffic and keep track of items stored in your shopping basket;" and (b) includes a link for the user to reject the Website's use of such tracking technologies.

26. The link takes the user to Samsung's Privacy and Cookie Preference Center. Once there, Website users are told that the Website uses two types of technologies: (1) "strictly necessary cookies," which Samsung defines as those cookies that are "necessary for the website to function and cannot be switched off in our systems"; and (2) "share or sale of personal information," which category includes "cookies, website trackers and similar technologies" that "collect and disclose" information to "third parties" for "targeted ads and for analytics purposes." Website users are given the option of disabling the latter but not the former.

27. Plaintiff and Class members accessed Defendant's Website and opted to reject Defendant's ability to place tracking technologies on their computers. In that way, Plaintiff and Class members declined to consent to Defendant installing tracking technologies on their computers and Defendant using tracking technologies to collect and share their personal data and communications with the Website to third parties.

28. But the consent banner did not function as represented by Defendant. Rather, even after a user opts to deactivate tracking technologies, Defendant nevertheless (a) installed tracking technologies on the user's computer in the location where the computer was located (in this case, on Plaintiff's computers in California); and (b) used those technologies to track the user's browsing history, personal

information and communications with the Website, and share that information with third parties (some of which are also located in California, such as Google and Adobe).

29. The tracking technologies that operated on Website users' computers *after* a user opted to deactivate tracking technologies include tracking technologies created by third parties Google, Adobe, Akamai, Medallia, Bazaar Voice, Microsoft, and Teads. None of these technologies were strictly necessary for the Website to function, and each of these technologies could be disabled without impacting Defendant's ability to host and operate a website; indeed, many websites can and do function without any of these tracking technologies. Once installed on users' computers, these technologies tracked, collected and disclosed at least the following data and communications: browser information, device information, internet protocol ("IP") address, a unique personal identifier assigned to the individual user, the user's communications with the Website (*e.g.*, the GET and POST requests and other information exchanged between the user's web browser and the website server), and the URLs the user visited. That information was collected in real time while the user was accessing the Website and transmitted in real time to the third-party company that created the tracking technology.

30. The unique personal identifiers collected by these technologies can be used by the third-party providers to identify and target the specific Website user and/or their devices in the real world for advertising.

31. Moreover, the consent banner itself functions through yet another tracking cookie offered by a third party. In essence, when a user selects the option to "deactivate" tracking technologies on the Website, the "consent banner" causes *another* tracking cookie to be installed on users' computers. That cookie is supposed to prevent the other tracking technologies from operating on that users' web browser. However, unbeknownst to consumers, the cookie installed by the consent banner after a user opts to deactivate tracking technologies is *itself* a tracking cookie that tracks users' use of the Website and sends that information to: (a) the third party company that created the opt-out cookie; and (b) Defendant. That cookie tracks, collects and

discloses at least the following data and communications: browser information, device information, IP address, a unique personal identifier assigned to the individual user, the user's communications with the Website (*e.g.*, the GET and POST requests and other information exchanged between the user's web browser and the website server), and the URLs the user visited. That information was collected in real time while the user was accessing the Website and transmitted in real time to the third-party company that created the tracking technology.

32. None of the tracking technologies described above are "strictly necessary" for the Website to function and each can be removed from the Website or otherwise switched off in Samsung's systems. Indeed, Samsung operated its website prior to using any of these tracking technologies, and other websites can and do function without using these technologies.

C. Plaintiff's Reasonable Expectation of Privacy

33. Defendant did not have Plaintiff's and Class members' consent to install tracking technologies on their computers and use those technologies to track, collect, and share their personal data and communications with third parties.

34. Defendant knew it did not have Plaintiff's and Class members' consent because Defendant expressly solicited Plaintiff's and Class members' consent via the consent banner and Privacy and Cookie Preference Center and Plaintiff and Class members expressly declined to provide it by opting to reject tracking technologies.

35. Having selected the option to reject Defendant's use of tracking technologies, Plaintiff and Class members reasonably expected that Defendant would not install those technologies on their computers, would not cause or allow those technologies to be active on their computers, and would not use those technologies to collect, track and share their browsing history, personal data and communications with the Website to third parties, including third party marketing companies.

36. Plaintiff's and Class members' expectation of privacy was reasonable because of Defendant's own statements in the consent banner and Privacy and Cookie Preference Center.

37. Moreover, survey data showing the expectations of Internet users also makes clear that Plaintiff's and Class members' expectation of privacy was reasonable. A number of studies examining the collection of consumers' personal data confirms that the surreptitious taking of personal, confidential, and private information—as Defendant has done—violates reasonable expectations of privacy that have been established as general social norms. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares their personal data. Indeed, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data and the same percent believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[1] It is also simply common sense that Defendant should not collect user personal data and communications via online tracking technologies when users are browsing its Website after having selected the option to reject and disable those technologies, as selecting that option demonstrated a clear expectation that personal data and communications under these circumstances were intended to be private or confidential.

38. Just as importantly, since 2018, California passed the California Consumer Privacy Act (CCPA), which requires that data collection practices be

---

[1] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

disclosed at or before the actual collection is done.[2] Otherwise, "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."[3]

D. The Value of the Data Taken from Plaintiff

39. Defendant and the third-party providers of the tracking technologies at issue profit from their use of Plaintiff's and Class member's personal data to target them with advertising and for other economic benefits, such as improving their internal operations, products, and services.

40. The value of personal data is well understood and generally accepted as a form of currency. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[4] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[5] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

41. The Organization for Economic Cooperation and Development ("OECD") has published numerous volumes discussing how to value data such as that which is the subject matter of this complaint, including as early as 2013, with its publication "Exploring the Economics of Personal Data: A Survey of Methodologies

---

[2] Cal. Civ. Section 1798.100(b). *See also* Nev. Rev. Stat. Section 603A.340.

[3] *Id.*

[4] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[5] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

for Measuring Monetary Value."[6] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[7]

42. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[8] In essence, Professor Zuboff explains that revenue from Internet user data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a market for this data.

43. Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily

---

[6] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[7] https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en

[8] Shoshanna Zuboff, THE AGE OF SURVEILLANCE CAPITALISM 166 (2019).

> in software that facilitates the collection of consumer information.[9]

44. Likewise, in *The Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online. Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[10]

45. As Professors Acquisti, Taylor, and Wagman relayed in their 2016 article "The Economics of Privacy," published in the *Journal of Economic Literature*: "Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income,

---

[9] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

[10] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties."[11]

46. The cash value of the personal user information unlawfully collected by Defendant provided during the Class Period can be quantified. For example, a group of researchers studied the value that internet users place on their online browsing history and concluded that users value items of their online browsing history at $10.[12]

47. Similarly, the value of user-correlated internet browsing history can be quantified, because Google Inc. was willing to pay users for similar information. Google had a panel called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Internet." Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated that internet industry participants understood the value in internet users' browsing habits. Google pays Screenwise panelists up to $3 per week to be tracked.

---

[11] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf

[12] Juan Pablo Carrascal, et al., *Your browsing behavior for a big mac: economics of personal information online*, Proceedings of the 22nd International Conference on the World Wide Web, available at https://dl.acm.org/doi/abs/10.1145/2488388.2488406.

48. User-correlated URLs have monetary value. They also have non-monetary, privacy value. For example, in a study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90% of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

49. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that "online companies . . . control too much of our personal information and know too much about our browsing habits."

50. A number of platforms have appeared where consumers can and do directly monetize their own data, and prevent tech companies from targeting them absent their express consent:

a) Brave's web browser, for example, will pay users to watch online targeted ads, while blocking out everything else.[13]

b) Loginhood states that it "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to

---

[13] Get Paid to Watch Ads in the Brave Web Browser, at: https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an (Lifehacker, April 26, 2019) ("The model is entirely opt-in, meaning that ads will be reject by default. The ads you view will be converted into Brave's cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly").

control their data sharing," via a "consent manager" that blocks ads and tracking on browsers as a plugin.[14]

c) Ex-presidential candidate Andrew Yang's "Data Dividend Project" aims to help consumers, "[t]ake control of your personal data. If companies are profiting from it, you should get paid for it."[15]

d) Killi is a new data exchange platform that allows you to own and earn from your data.[16]

e) Similarly, BIGtoken "is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[17]

f) The Nielsen Company, famous for tracking the behavior of television viewers' habits, has extended their reach to computers and mobile devices through Nielsen Computer and Mobile Panel. By installing the application on your computer, phone, tablet, e-

---

[14] https://loginhood.io/. *See also* https://loginhood.io/product/chrome-extension ("[s]tart earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[15] How Does It Work, at: https://www.datadividendproject.com/ ("Get Your Data Dividend…We'll send you $$$ as we negotiate with companies to compensate you for using your personal data.").

[16] https://killi.io/earn/.

[17] https://bigtoken.com/faq#general_0 ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

> reader, or other mobile device, Nielsen tracks your activity, enters you into sweepstakes with monetary benefits, and earn points worth up to $50 per month.[18]

51. Technology companies recognize the monetary value of users' sensitive, personal information, insofar as they encourage users to install applications explicitly for the purpose of selling that information to technology companies in exchange for monetary benefits.[19]

52. The CCPA recognizes that consumers' personal data is a property right. Not only does the CCPA prohibit covered businesses from discriminating against consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

---

[18] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[19] Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019), https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacystudy; Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-datatechcrunch.html; Jay Peters, *Facebook will now pay you for your voice recordings*, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voicespeech-recognition-viewpoints-prounciations-app.

E. Defendant was Unjustly Enriched from the Use of the Tracking Technologies.

53. The purpose of the tracking technologies used on Defendant's Website was for analysis and marketing and, ultimately, profit.

54. In exchange for disclosing Plaintiff's and Class members' data and communications, Defendant is compensated by the third-party tracking technology vendors in the form of enhanced analytical and/or advertising services and more cost-efficient sales and marketing.

55. Upon information and belief, Defendant uses the online tracking technologies that are not strictly necessary to increase sales and to help Defendant market its products.

56. By utilizing online tracking technologies that are not strictly necessary, the cost of sales, advertising and retargeting was reduced, thereby benefitting Defendant.

57. Through its false representations and unlawful data collection, Defendant is unjustly enriching itself at the cost of consumer choice, when the consumer would otherwise have the ability to choose how they would monetize their own data.

58. Through its false representations and unlawful data collection, Defendant is unjustly enriching itself based on the value of Defendants' unauthorized access to Plaintiff's and Class members' data and communications resulting from Defendant's wrongful conduct. This value is analogous to the value for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would

not have otherwise licensed such IP to the infringer. A similar royalty or license measure of value is appropriate here under common law principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their data and communications; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

F. Defendant Collected the Personal Data for the Purpose of Committing Further Tortious and Unlawful Acts

59. The data collected from users after they have rejected the use of online tracking technologies qualifies as "personal information" that is protected by the CCPA. Cal. Civ. Code § 1798.140(v).

60. The CCPA provides:

> "A business that collects a consumer's personal information shall, ***at or before the point of collection***, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. ***A business shall not . . . use personal information collected for additional purposes without providing the consumer with notice consistent with this section***." Cal. Civ. Code § 1798.100(b) (emphasis added).

61. At the time Defendant deployed the tracking technologies at issue, Defendant had knowledge of their functionality, including because: (a) the terms of use agreements Defendant entered into with the third-party technology providers discloses the technologies' functionality; (b) descriptions of the technologies' functionality are publicly available online; and (c) the entire purpose of the technologies is to track users' online activities and disclose that information to the third-party technology provider for the purposes of analyzing website use and targeting website users with marketing messages.

62. At the time Defendant collected and disclosed data from users after they had rejected the use of tracking technologies, Defendant intended to "use" that data "for additional purposes without providing the consumer with notice consistent with this section." Thus, Defendant collected the data with the intent to violate the California Consumer Privacy Act (CCPA). Whenever Defendant uses the confidential communications wrongfully collected, or aggregates it with other information to gain additional insight and intelligence, Defendant has violated the express prohibitions of the CCPA.

63. Moreover, Defendant carried out its intent: As described elsewhere in this Complaint, Defendant made use of the data it collected from users for the "additional purposes" of analytics and targeted advertising. The users had never been "informed" that their data and communications with the Website would be used for those "additional purposes" after they opted out of tracking technologies on the Website. Defendant never gave its users "notice consistent with" the CCPA's requirements regarding these "additional purposes" for which Defendant used the data collected after they had rejected the use of online tracking technologies.

64. Defendant also collected the data with the intent to intrude upon users' seclusion and invade their constitutional privacy. The California Constitution and common law protect consumers from invasions of their privacy and intrusion upon seclusion.

65. Users declined Defendant's online tracking technologies for the purpose of preventing Defendant and others installing online tracking technologies on their computers and surveilling and intercepting their interactions and communications with Defendant's website, including to avoid targeted advertising.

66. By causing user data and communications to be collected, disclosed and shared with third-party technology providers after users had rejected online tracking technologies, and by causing targeted advertisements to be sent to users and to users' devices based on data collected after users had rejected online tracking technologies,

Defendant has caused that data to be revealed to others and has thereby invaded the privacy and intruded upon the seclusion, of the users whose data and communications were collected after rejecting online tracking technologies.

67. Defendant had the intent to send these targeted advertisements at the time that Defendant was collecting data from users who rejected online tracking technologies.

G. Delayed Discovery & Tolling

68. Each unauthorized collection of private, personal data by Defendant is a separate "wrong" which triggers anew the relevant statute of limitations.

69. Further, all applicable statutes of limitation have been tolled by operation of the delayed discovery doctrine, which delays accrual until Plaintiff have, or should have, inquiry notice of the cause of action. Plaintiff and Class members were not on inquiry notice despite acting with reasonable diligence. Plaintiff does not have the expertise in identifying and interpreting the underlying coding and the operation of the fake consent banner in order to discover Defendant's wrongful conduct.

70. Plaintiff did not discover and could not reasonably have discovered that Defendant was collecting, storing, and using their personal, private data in the ways set forth in this Complaint until they consulted with counsel—shortly before the Complaint was filed.

CLASS ACTION ALLEGATIONS

71. This is a class action on behalf of the following Classes:

The Nationwide Class: All natural persons residing in the United States who (a) visited Defendant's Website during the Class Period, and (b) rejected online tracking technologies that are not strictly necessary through Defendant's consent banner.

The California Subclass: All natural persons residing in the state of California who (a) visited Defendant's Website during the Class Period, and (b) rejected

online tracking technologies that are not strictly necessary through Defendant's consent banner.

72. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel, Class counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

73. **Numerosity**. The Classes are so numerous that joinder of individual members therein is impracticable. The exact number of Class members, as herein identified and described, is not known, but Defendant's website is known to have millions of users based on publicly available data.

74. **Commonality**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class members, including the following:

a) Whether Defendant's practice of collecting, using, or sharing personal, private data from Plaintiff and Class members after they had declined online tracking technologies that are not strictly necessary constitutes conversion under California law;

b) Whether Defendant's practice of collecting, using, or sharing personal, private data from Plaintiff and Class members after they had declined online tracking technologies that are not strictly necessary constitutes an intrusion upon seclusion under California law;

c) Whether profits obtained by Defendant through the use of personal, private data that they obtained from Plaintiff and Class members were unjustly obtained and should be disgorged;

d) Whether Defendant sold personal, private data or access to personal, private data unlawfully obtained from Plaintiff and Class members after they had declined online tracking technologies that are not strictly necessary;

e) Whether Plaintiff and Class members sustained damages as a result of Defendant's alleged conduct, and, if so, what is the appropriate measure of damages and/or restitution;

f) Whether Defendant enabled third-party analytical or tracking technology providers to read, attempt to read, learn, attempt to learn, eavesdrop, record, use, intercept, receive, and/or collect electronic communications of private data from Plaintiff and Class members during the Class Period;

g) Whether Defendant's practice of enabling third-party analytical or tracking technology providers to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications of private data from Plaintiff and Class members during the Class Period, violates the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.*;

h) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of private data from Plaintiff and Class members through third-party analytical or tracking technology providers violates Cal. Pen. Code §§ 484, 496; and

i) Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

75. **Typicality**. Plaintiff's claims are typical of the claims of members of the Classes because, among other things, Plaintiff and members of the Classes sustained similar injuries as a result of Defendant's uniform wrongful conduct and their legal claims all arise from the same events and wrongful conduct by Defendant.

76. **Adequacy**. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff's interests do not conflict with the interests of the Classes, and Plaintiff has retained counsel with experience in complex class actions, as well as sufficient financial and legal resources to prosecute this case on behalf of the Classes. Plaintiff and his counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes. Plaintiff anticipates no difficulty in the management of this litigation as a class action.

77. **Predominance & Superiority**: Common questions of law and fact predominate over any questions affecting only individual members of the Classes, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. Here, common issues predominate because liability can be determined on a class-wide basis, even where some individualized damages determination may be required. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by complex legal and factual issues of the case to all parties and the court system. Furthermore, the expense and burden of individual litigation make it impossible for Class members to individually redress the wrongs done to them. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

FIRST CAUSE OF ACTION: VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502 *ET SEQ.*

(On Behalf of Plaintiff and the California Subclass Against All Defendants)

78. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

79. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

80. Plaintiff's and Class members' computers and smart phone devices with the capability of using web browsers are "computers" within the meaning of the statute.

81. Defendant violated Cal. Penal Code § 502(c)(1) by knowingly accessing and without permission using data, computers, computer systems, or computer networks in order to either (A) devise or execute any scheme or artifice to defraud or deceive, or (B) wrongfully control or obtain money, property, or data from Plaintiff and Class members.

82. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiff's and Class members' data.

83. Defendant violated Cal. Penal Code § 502(c)(6) by knowingly and without permission providing or assisting in providing a means of accessing a computer, computer system, or computer network in violation of Cal. Penal Code § 502.

84. Defendant violated Cal. Penal Code § 502(c)(7) by knowingly and without permission accessing or causing to be accessed any computer, computer system, or computer network.

85. Defendant violated Cal. Penal Code § 502(c)(8) by knowingly introducing a computer contaminant into any computer, computer system, or computer network.

86. Despite Defendant's false representations to the contrary, Defendant effectively charged Plaintiff and Class members for use of Defendant's Website by acquiring users' personal information without permission and using it for their own financial benefit to advance their business through targeted advertising. Plaintiff and Class members retain a stake in the profits Defendant earned from their personal browsing histories and other data because, under the circumstances, it is unjust for Defendant to retain those profits.

87. Defendant deployed a consent banner on Plaintiff's and Class members' computers in the State of California, and Plaintiff and Class members rejected the use of online tracking technologies. Defendant nevertheless deposited online tracking technologies onto Plaintiff's and Class members' computers in California, and thereafter accessed, copied, took, analyzed, and used data from Plaintiff's and Class members' computers.

88. As a direct and proximate result of Defendant's unlawful conduct within the meaning of Cal. Penal Code § 502, Defendant has caused loss to Plaintiff and Class members and has been unjustly enriched in an amount to be proven at trial.

89. Plaintiff, on behalf of himself and Class members, seeks compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

90. Plaintiff and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violations were willful and, upon information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

91. Plaintiff and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

SECOND CAUSE OF ACTION: INVASION OF PRIVACY

(On Behalf Of Plaintiff and the California Subclass Against All Defendants)

92. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

93. The right to privacy in California's constitution creates a right of action against private entities such as Defendant.

94. Plaintiff's and Class members' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, and privacy.

95. The phrase "and privacy" was added by the "Privacy Initiative" adopted by California voters in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone… It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[20]

---

[20] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972).

96. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendant.

97. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

98. As described herein, Defendant has intruded upon the following legally protected privacy interests:

a) The California Wiretap Act as alleged herein;

b) A Fourth Amendment right to privacy contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c) The California Constitution, which guarantees Californians the right to privacy; and

d) Defendant's promise not to collect, use or share Plaintiff's and Class members' personal data via online tracking technologies that are not strictly necessary after Plaintiff and Class members rejected Defendant's use of online tracking technologies that are not strictly necessary.

99. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiff and Class members could not reasonably expect Defendant would commit acts in violation of state civil and criminal laws; and Defendant affirmatively promised users (including Plaintiff and Class members) it would not collect, use or share Plaintiff's and Class members' personal data via online tracking technologies after Plaintiff and Class members rejected online tracking technologies on Defendant's website.

100. Defendant's actions constituted a serious invasion of privacy in that it:

a) Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including browsing histories

b) Violated state laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

c) Invaded the privacy rights of millions of Americans (including Plaintiff and Class members) without their consent

d) Constituted the unauthorized taking of valuable information from millions of Americans through deceit; and

e) Further violated Plaintiff's and Class members' reasonable expectation of privacy via Defendant's review, analysis, and subsequent uses of Plaintiff's and Class members' private browsing activity that Plaintiff and Class members considered sensitive and confidential.

101. Committing the above privacy violations against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

102. The surreptitious and unauthorized tracking of the confidential browsing history of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

103. Defendant's intentional intrusion into Plaintiff's and Class members' computing devices and web-browsers was highly offensive to a reasonable person in that Defendant violated state criminal and civil laws designed to protect individual privacy and against theft.

104. The taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior.

105. Secret monitoring of private web browsing is highly offensive behavior.

106. Wiretapping, eavesdropping on, and surreptitious recording of communications, and/or enabling the same, is highly offensive behavior.

107. Following Defendant's unauthorized collection of the sensitive and valuable personal information, the subsequent analysis and use of that private browsing activity to target Plaintiff, Class members, and consumers with advertising violated their reasonable expectations of privacy.

108. Defendant lacked a legitimate business interest in analyzing users' data and tracking users while browsing their website to target them with advertising without their consent.

109. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation and injunctive relief.

THIRD CAUSE OF ACTION: INTRUSION UPON SECLUSION

(On Behalf of Plaintiff and the California Subclass Against All Defendants)

110. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

111. Plaintiff asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

112. In carrying out its scheme to track Plaintiff's and Class members' communications while they were using a browser after they had declined online tracking technologies that are not strictly necessary in violation of its own privacy promises, Defendant intentionally intruded upon the Plaintiff's and Class members' solitude or seclusion in that it enabled third-parties to place themselves in the middle of a private place, conversation, or matter to which they were not authorized.

113. Defendant's tracking was not authorized by the Plaintiff and Class members.

114. Defendant's intentional intrusion into their computing devices and web-browsers was highly offensive to a reasonable person in that they violated state criminal and civil laws designed to protect individual privacy and against theft.

115. The taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior, particularly where, as here, Plaintiff and Class members took active (and recommended) measures to ensure their privacy.

116. Secret monitoring of private web browsing is highly offensive behavior.

117. Wiretapping and surreptitious recording of communications and/or enabling of the same is highly offensive behavior.

118. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is browsing the internet after manually disabling online tracking technologies through a website's consent banner and privacy center.

119. Plaintiff and the Class members have been damaged by Defendant's invasion of their privacy and are entitled to reasonable compensation including but not limited to the value of the data that was taken and disgorgement of profits related to the unlawful internet tracking.

FOURTH CAUSE OF ACTION: CAL. UNFAIR COMPETITION LAW ("UCL"), CAL. BUS. & PROF. CODE § 17200 *ET SEQ.*

(On Behalf of Plaintiff and the California Subclass Against All Defendants)

120. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

121. The UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof.

Code § 17200 (UCL). By engaging in the practices aforementioned, Defendant has violated the UCL.

122. Defendant's "unlawful" acts and practices include its violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *et seq.*; Invasion of Privacy; Intrusion Upon Seclusion; California Business & Professions Code § 22576; and the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632.

123. Defendant's conduct violated the spirit and letter of these laws, which protect property, economic and privacy interests and prohibit unauthorized disclosure and collection of private, personal data and unauthorized eavesdropping on electronic communications.

124. Defendant's "unfair" acts and practices include its violation of property, economic and privacy interests protected by the statutes identified above. To establish liability under the unfair prong, Plaintiff and Class members need not establish that these statutes were actually violated, although the claims pleaded herein do so.

125. Plaintiff and Class members have suffered injury-in-fact, including violations of their protected privacy interests and, separately, the loss of money and/or property, as a result of Defendant's unfair and/or unlawful practices, to wit, the unauthorized disclosure and taking of their personal information which has value, including as described above and as demonstrated by its use by Defendant (and third-parties). Plaintiff and Class members have suffered harm in the form of loss of the value of their private and personally identifiable data.

126. Plaintiff and Class members seek to recover the value of the unauthorized access to their data and communications resulting from Defendant's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention

or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their data and communications; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

127. Defendant's actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information.

128. Defendant reaped unjust profits and revenues in violation of the UCL. This includes Defendant's profits and revenues from their targeted advertising. Plaintiff and the Class seek restitution and disgorgement of these unjust profits and revenues.

129. By virtue of the conduct alleged herein, Plaintiff and Class members are also entitled to injunctive relief.

FIFTH CAUSE OF ACTION: UNJUST ENRICHMENT

(On Behalf Of Plaintiff and the California Subclass Against All Defendants)

130. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

131. Plaintiff and Class members conferred a benefit on Defendant in the form of personal, private data which has substantial monetary value that Defendant extracted and used to produce revenue and unjustly retained those benefits at the expense of Plaintiff and Class members.

132. Defendant collected and used and made available this information for their own gain, reaping economic, intangible, and other benefits.

133. Defendant unjustly retained those benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff and Class members.

134. Plaintiff and Class members did not consent to the collection and use of their personal, private data, nor did they have any control over its use. Therefore, under principles of equity and good conscience, Defendant should not be permitted to retain any money derived from their use of Plaintiff and Class members' personal, private data.

135. Plaintiff and Class members seek to recover the value of the unauthorized access to their data and communications resulting from Defendant's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their data and communications; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

136. Defendant's actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information.

137. The benefits that Defendant derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles to permit Defendant's retention of any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

SIXTH CAUSE OF ACTION: VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CALIFORNIA PENAL CODE § 631

(On Behalf of Plaintiff and the California Subclass Against All Defendants)

138. Plaintiff, individually and on behalf of the California Subclass, incorporates the foregoing allegations as if fully set forth herein.

139. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

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

Cal. Penal Code § 630.

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

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or

> in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

141. Under CIPA, a defendant must show it had the consent of all parties to a communication.

142. Defendant designed, contrived, effectuated, and enabled its scheme to track its users while they were browsing Defendant's website from a browser located in California, deposited tracking technologies on computers located in California after the owners' of those computers declined to consent to that conduct, and enabled those technologies to eavesdrop and intercept communications originating from computers in California and send those communications to third parties, including third parties, like Google and Adobe, located in California.

143. At all relevant times, Defendant lacked Plaintiff's and Class members' consent to install tracking technologies on their computers and use those technologies to enable third-party marketing companies to eavesdrop on Plaintiff's and Class members' communications with the Website.

144. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Defendant's deliberate and

purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a) The tracking technologies that Defendant integrated into the Website;

b) The computer codes and programs used by Defendant to effectuate its tracking and interception of the Plaintiff's and Class members' communications after they had rejected the use of online tracking technologies;

c) The Plaintiff's and Class members' web browsers;

d) The Plaintiff's and Class members' computing and mobile devices;

e) Defendant's web server(s); and

f) The plan Defendant carried out to effectuate its tracking and interception of the Plaintiff's and Class members' communications after they had rejected the use of online tracking technologies.

145. The third-party vendors of the tracking technologies at issue violated clauses two and three of CIPA § 631 by: (a) willfully and without the consent of all parties to the communication, or in any unauthorized manner, reading, or attempting to read, or to learn the contents or meaning of any message, report, or communication while the same was in transit or passing over any wire, line, or cable, or was being sent from, or received at any place within California; and (b) using, or attempting to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained. Indeed, the entire purpose of the tracking technologies at issue is to collect information on internet users' online activities and use that information to generate reports for website owners and target marketing at the internet users' across the internet; and the third-party vendors cannot perform those functions without reading the information received from the tracking technologies and using it to create reports and profiles based on individuals' online activities. Thus, the third-party vendors' reading and using the information obtained via the tracking technologies at issue was

not fortuitous or inadvertent; it was willful, as reading and using the information was the entire point of developing the tracking technologies and collecting the information in the first place.

146. Defendant, in turn, violated clause four of CIPA § 631 by aiding, agreeing with, employing, or conspiring with the third-party vendors of the tracking technologies at issue or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned in clauses two and three of CIPA § 631. Defendant understood the functionality of the technology it placed on the Website. By integrating that technology into the Website, Defendant enabled the third-party tracking companies to eavesdrop on Plaintiff's and Class members' communications with the Website in violation of clauses two and three of CIPA § 631. If Defendant had not installed that technology on the Website, the third-party vendors would not have been able to eavesdrop on Plaintiff's and Class members' communications with the Website.

147. Plaintiff and Class members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and, separately, loss of value in their personally identifiable information.

148. Plaintiff and Class members seek to recover the value of the unauthorized access to their data and communications resulting from Defendant's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles

authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their data and communications; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

149. Defendant's actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information.

150. Pursuant to California Penal Code § 637.2, Plaintiff and Class members have been injured by the violations of California Penal Code §§ 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

SEVENTH CAUSE OF ACTION: VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1) *et seq.* UNAUTHORIZED INTERCEPTION, USE AND DISCLOSURE

(On Behalf of Plaintiff and the Nationwide Class Against All Defendants)

151. Plaintiff, individually and on behalf of the Nationwide Class, incorporate the foregoing allegations as if fully set forth herein.

152. The Electronic Communications Privacy Act ("ECPA") protects both sending and receipt of communications.

153. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

154. The transmissions of the information described above to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

155. The transmissions of the information described above between Plaintiff and Class Members and Defendant's Website with which they chose to exchange

communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

157. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents...include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

158. The ECPA defines "electronic, mechanical, or other device" as "any device...which can be used to intercept a[n]...electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a) Plaintiff's and Class Members' browsers;

b) Plaintiff's and Class Members' computing devices (including mobile devices);

c) Defendant's web-servers;

d) Defendant's Website; and

e) The online tracking technologies deployed by Defendant to effectuate the sending and acquisition of information to third party marketing companies.

159. By utilizing and embedding the online tracking technologies that are not strictly necessary on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

160. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the online tracking technologies, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' communications with Defendant's Website to the third party marketing companies described above.

161. Defendant's intercepted communications include communications between Plaintiff and Class Members and the Website as described throughout this Complaint.

162. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

163. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

164. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, and the various other laws identified in the counts above, among others.

165. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the online tracking technologies to track and utilize Plaintiff's and Class Members' personal data and communications for financial gain.

166. Defendant was not acting under color of law to intercept Plaintiff and Class Member's wire or electronic communication.

167. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the online tracking technologies Defendant deployed on their computers.

168. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above.

169. Plaintiff and Class members seek to recover the value of the unauthorized access to their data and communications resulting from Defendant's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their data and communications; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

170. Defendant's actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information.

171. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Certify this action is a class action;

B. Appoint Plaintiff to represent the Class;

C. Appoint undersigned counsel to represent the Class;

D. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

E. Award nominal damages to Plaintiff and the Class members against Defendant;

F. Disgorgement of all of Defendant's profits that were derived, in whole or in part, from Defendant's collection and subsequent use of Plaintiff's personal data;

G. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

H. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from deploying and using tracking technologies on any Website user's computer after that user rejects the use of tracking technologies via Defendant's consent banner or privacy center;

I. Award Plaintiff and the Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

J. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues so triable.

Dated: April 7, 2025

LAW OFFICES OF ROBERT G. LOEWY, PC

/s/ Robert G. Loewy

Robert G. Loewy
Plaintiff Vedat Asrak and
the Proposed Classes