

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

JOSEPH DIGIACINTO, DANIELLE TILLERY, TYLER BAKER, BOBBYJO ANDOH, and ALICIA ROOD , on behalf of themselves and all others similarly situated, Plaintiffs, v. SAMSUNG ELECTRONICS AMERICA, INC. , Defendant.	Case No. 1:26-cv-00196 JURY TRIAL DEMANDED
---	--

CLASS ACTION COMPLAINT

Plaintiffs Joseph DiGiacinto, Danielle Tillery, Tyler Baker, BobbyJo Andoh, and Alicia Rood (collectively, “Plaintiffs”), individually and on behalf of all similarly situated persons, allege the following against Defendant Samsung Electronics America, Inc. (“Defendant” or “Samsung”) based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs’ counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. When Congress passed the Video Privacy Protection Act in 1988, it sought to protect against “a new, more subtle and pervasive form of surveillance” resulting from “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems[.]” S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

Moreover, Congress was particularly alarmed about surveillance of Americans' media consumption, recognizing that:

Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy-of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye... These records are a window into our loves, lives, and dislikes.

Id. (statement of Rep. Al McCandless).

2. Unfortunately, the pervasive media surveillance that Congress envisioned in 1988 has not only come to pass but has been vastly amplified due to technological advances unimaginable at the time. Indeed, unbeknownst to American consumers, many major television (also referred to herein as “TV”) manufacturers now secretly install automatic content recognition software (the “ACR Tools”) onto TVs, which then constantly record and transmit data relating to a consumer’s use of those TVs.

3. Samsung is the largest television retailer in the world, having maintained the number one position in global TV sales every year since 2006.¹ Unfortunately, it is also one of the aforementioned TV manufacturers that has chosen to engage in mass surveillance of its customers.

4. Smart TVs sold by Samsung (referred to herein as “Samsung TVs”) include both Samsung-specific ACR technology, as well as the “Samba TV” software program, a leading ACR software tool present on over twenty TV brands and which collects data from over 11-million U.S. households.²

¹ 2025 Interim Business Report, SAMSUNG (May 15, 2025), at p. 25, available online at: https://images.samsung.com/is/content/samsung/assets/global/ir/docs/2025_1Q_Interim_Report.pdf.

² Katie North-Fisher, *A Closer Look at Samba TV’s Partnership with Publicis Groupe’s Epsilon, SAMBA TV* (Apr. 25, 2023), <https://www.samba.tv/resources/a-closer-look-at-samba-tvs-partnership-with-publicis-groupe-epsilon> (last accessed Dec. 26, 2025).

5. Unbeknownst to Samsung's customers, these ACR Tools record the image and audio played by the Samsung TV screen every **500 milliseconds**. Then, the ACR Tools use sophisticated machine learning algorithms to identify the content being played on the television, regardless of its source. This data includes the specific programs being watched by the viewer, information relating to content streamed through third-party apps, information relating to content accessed through video game systems or other connected devices, and even information displayed when the Samsung TV is used as a computer monitor (collectively, the "Sensitive Information").

6. Through sophisticated technical analysis of data collected through the ACR Tools and compiled from other sources, Samsung is then able to identify and trace the Sensitive Information back to specific consumers, even where multiple individuals in a household use the same Samsung TV. Samsung exploits this Sensitive Information by (a) selling targeted advertisements to its corporate advertising clients, and (b) providing it to third-party advertising companies such as Google and X (f/k/a Twitter) for targeted advertising.

7. Each of the Plaintiffs and Class Members purchased a Samsung TV and had their personal Sensitive Information tracked by Defendant using the ACR Tools. However, Defendant **never** obtained informed consent from Plaintiffs or Class Members to collect their Sensitive Information or to share it with third parties, some of which constitute the largest advertisers and data compilers in the world.

8. Moreover, Defendant's tracking of Samsung TV users violated numerous state and federal laws, including the Video Privacy Protection Act ("VPPA"), which was passed specifically to prevent the disclosure and aggregation of data relating to an individual's video consumption.

9. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with

electronics retailers; (iii) emotional distress and heightened concerns related to the release of Sensitive Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of the Sensitive Information; (vi) statutory damages; and (viii) continued and ongoing risk to their Sensitive Information.

10. Therefore, Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and assert the following statutory and common law claims against Defendant: Invasion of Privacy; Negligence; Breach of Implied Contract; Unjust Enrichment; violations of the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710, *et seq.*; violations of the Electronic Communications Privacy Act (“ECPA”); violations of N.Y. Gen. Bus. Law § 349; violations of the California Invasion of Privacy Act (“CIPA”); Cal. Pen. Code § 360, *et seq.*; violations of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code, § 17200, *et seq.*; violations of the Vermont Consumer Fraud Act, Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*; and violations of the New Jersey Consumer Fraud Act, N.J. Stat. Ann. 56:8-1, *et seq.*

II. PARTIES

Plaintiff Joseph DiGiacinto

11. Plaintiff DiGiacinto is a citizen of the state of California residing in Sonoma County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

12. Plaintiff DiGiacinto purchased a Samsung TV in or about July of 2024 and used his Smart TV to watch television programs and streaming application content, from about July of 2024 to present.

13. Unbeknownst to Plaintiff DiGiacinto, the ACR Tools surreptitiously intercepted and disclosed the Sensitive Information that was communicated to and from Plaintiff DiGiacinto

as he used his Samsung TV, including the programs he watched, applications he downloaded, and other information displayed on his television screen through the normal course of use.

14. Plaintiff DiGiacinto possesses a Google account.

15. Plaintiff DiGiacinto never authorized Defendant to collect, store, analyze, monetize, and/or disclose his personally identifiable Sensitive Information.

Plaintiff Danielle Tillery

16. Plaintiff Tillery is a citizen of the state of California residing in San Francisco County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

17. Plaintiff Tillery purchased a Samsung TV in or about early 2020, and used her Smart TV to watch live television programs and streaming application content, from about early 2020 to present.

18. Unbeknownst to Plaintiff Tillery, the ACR Tools surreptitiously intercepted and disclosed the Sensitive Information that was communicated to and from Plaintiff Tillery as she and her household (which includes her three-year-old son) used her Samsung TV, including the programs they watched, applications she downloaded, and other information displayed on her television screen through the normal course of use.

19. Plaintiff Tillery possesses a Google account.

20. Plaintiff Tillery never authorized Defendant to collect, store, analyze, monetize, and/or disclose her personally identifiable Sensitive Information.

Plaintiff Tyler Baker

21. Plaintiff Baker is a citizen of the state of Vermont, residing in Chittenden County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

22. Plaintiff Baker purchased a Samsung TV in or about 2022. Plaintiff Baker used his Samsung TV to watch television and streaming application programs, from about 2022 to the present.

23. Unbeknownst to Plaintiff Baker, the ACR Tools surreptitiously intercepted and disclosed the Sensitive Information that was communicated to and from Plaintiff Baker as he used his Samsung TV, including the programs he watched, applications he downloaded, and other information displayed on his television screen through the normal course of use.

24. Plaintiff Baker possesses a Google account.

25. Plaintiff Baker never authorized Defendant to collect, store, analyze, monetize, and/or disclose his personally identifiable Sensitive Information.

Plaintiff BobbyJo Andoh

26. Plaintiff Andoh is a citizen of the state of Maryland, residing in Frederick County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

27. Plaintiff Andoh purchased a Samsung TV in or about 2022, and a second Samsung TV in or about 2025. Plaintiff Andoh used her Samsung TVs to watch television content and streaming application content.

28. Unbeknownst to Plaintiff Andoh, the ACR Tools surreptitiously intercepted and disclosed the Sensitive Information that was communicated to and from Plaintiff Andoh as she used her Samsung TV, including the programs she watched, applications she downloaded, and other information displayed on her television screen through the normal course of use.

29. Plaintiff Andoh possesses a Google account.

30. Plaintiff Andoh never authorized Defendant to collect, store, analyze, monetize, and/or disclose her personally identifiable Sensitive Information.

Plaintiff Alicia Rood

31. Plaintiff Rood is a citizen of the state of New York residing in Herkimer County, and brings this action both in an individual capacity, and on behalf of all others similarly situated.

32. Plaintiff Rood purchased a Samsung TV in or about 2021, and a second Samsung TV in or about 2022. Plaintiff Rood used her Samsung TVs to watch television content, streaming application content, and play video games, from about 2021 to present.

33. Unbeknownst to Plaintiff Rood, the ACR Tools surreptitiously intercepted and disclosed the Sensitive Information that was communicated to and from Plaintiff Rood as she used her Samsung TV, including the programs she watched, applications she downloaded, and other information displayed on her television screen through the normal course of use.

34. Plaintiff Rood possesses a Google account.

35. Plaintiff Rood never authorized Defendant to collect, store, analyze, monetize, and/or disclose her personally identifiable Sensitive Information.

Defendant Samsung

36. Defendant Samsung Electronics of America, Inc. is a for-profit corporation incorporated in the state of New York, with its principal place of business located at 700 Sylvan Avenue, Englewood Cliffs, New Jersey, in Bergen County.

III. JURISDICTION AND VENUE

37. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiffs and many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

38. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (18 U.S.C. § 2511, *et seq.*) and VPPA (18 U.S.C. § 2710, *et seq.*).

39. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein from part of the same case or controversy.

40. This Court has personal jurisdiction over Defendant because Defendant has advertised and offered its products to consumers in the State of New York and in this judicial district, including to Plaintiff Rood. Personal jurisdiction is also proper because Defendant is incorporated in the State of New York has otherwise made or established contacts in the State of New York and in this judicial district sufficient to permit the exercise of personal jurisdiction.

41. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to the claims in this action occurred in this judicial district.

IV. FACTUAL ALLEGATIONS

A. SAMSUNG'S SURVEILLANCE OF ITS TELEVISION CUSTOMERS

i. Samsung's Television Business

42. Samsung has maintained the number one position in global TV sales every year since 2006.³ Samsung had a 28.3-percent share of the global TV market in 2024, and derived approximately \$21.4-billion in revenue from television sales.⁴

43. Despite this 11-figure yearly revenue, Samsung has increasingly sought to increase the profitability of its television business through the collection and monetization of customer data.

As one commentator explains:

³ 2025 *Interim Business Report*, SAMSUNG (May 15, 2025), at p. 25, available online at: https://images.samsung.com/is/content/samsung/assets/global/ir/docs/2025_1Q_Interim_Report.pdf.

⁴ *Id.* at pp. 12, 25.

[T]he entry of Chinese manufacturers including Hisense and TCL into the TV business in the 2000s [led] to unprecedented price competition [for Samsung and other major TV retailers]. As the retail price of TVs fell, the margins of TV manufacturers became wafer-thin. Average margins in TV hardware are now less than 1%, whereas margins in connected TV advertising are 50% or more. Faced with these shrinking hardware margins, manufacturers have increasingly turned to services – advertising, content sales, and data brokerage – to improve their bottom lines. Just as Apple’s App Store established a lucrative services business alongside Apple’s hardware business, TV manufacturers are similarly keen to move up the value chain to higher margin activities.⁵

44. In pursuit of this goal, Samsung established Samsung Ads in 2015. By leveraging the massive amounts of consumer data that it harvests from its customers, Samsung touts its ability to serve targeted television, mobile phone, and internet advertising to over 160-million U.S. consumers, through over 600 audience segments “[p]owered by AI and Samsung’s TV and mobile data.”⁶

ii. Samsung’s Use of ACR Tools to Surveil Plaintiffs and Class Members

45. Samsung’s massive advertising enterprise would not be possible without the data collected through use of the ACR Tools. As Samsung explains, “ACR, or automatic content recognition, is a type of data technology that identifies content played on a digital media device.”⁷ Samsung TVs use both Samsung-specific ACR technology, as well as Samba TV, a leading ACR software tool present on over twenty TV brands with access to data from over 11-million U.S. households.⁸

⁵ Ramon Lobato, *Automated content recognition (ACR), smart TVs, and ad-tech infrastructure*, 31(6) CONVERGENCE: THE INT’L JOURNAL OF RESEARCH INTO NEW MEDIA TECHS. (July 15, 2025), at 1806, available online at: <https://journals.sagepub.com/doi/10.1177/13548565251327885>.

⁶ Samsung Ads, SAMSUNG, <https://www.samsung.com/us/business/samsungads/solutions/consumer-reach/> (last accessed Dec. 26, 2025).

⁷ *Understanding Automatic Content Recognition (ACR): A Samsung Ads Guide for Advertisers*, SAMSUNG, available online at: <http://samsungads.events/acrguide-pr>.

⁸ Katie North-Fisher, *A Closer Look at Samba TV’s Partnership with Publicis Groupe’s Epsilon*, SAMBA TV (Apr. 25, 2023), <https://www.samba.tv/resources/a-closer-look-at-samba-tvs-partnership-with-publicis-groupe-epsilon> (last accessed Dec. 26, 2025).

46. Samsung's ACR Tools operate by recording the image and audio played by the Samsung TV screen every **500 milliseconds** whenever the TV is in-use.⁹ Then, this output is analyzed by deep learning software programs to identify whatever visual elements are present on the screen, such as a specific face, product, brand name, or object.¹⁰ The resulting "video footprint" created by the ACR Tools is then compared to a content database to determine the specific program being viewed by the Samsung TV user.¹¹

47. However, Samsung's ACR Tools track far more than simply the television programs enjoyed by its customers. Rather:

ACR takes in everything on your screen, not just TV shows... ACR is capturing anything that appears on your screen, including YouTube videos, personal photos, security or doorbell camera streams, and video or photos you send via Apple AirPlay or Google Cast. ACR can even snag content from other devices connected to your TV by HDMI, including personal laptops, video game consoles, and Blu-ray players.¹²

48. This information is then linked to other information collected about the television user from other sources. As Samba TV explains, by "leverag[ing] a multi-identifier approach, using various types of digital identifiers as well as first party TV data[, Samba TV's ACR software] can identify at 90%+ accuracy which phones, tablets, PCs, and TVs belong to an individual[.]"¹³ As a result, Samsung is able to coordinate advertising delivered on a consumer's ACR-enabled television

⁹ *An Advertiser's Guide to Samsung Ads' ACR*, SAMSUNG, available online at: <https://samsungads.events/acrguide-pr>.

¹⁰ See *Understanding Video-based Automatic Content Recognition*, SAMBA TV, at 8, available online at: <https://www.samba.tv/resources/understanding-video-based-automatic-content-recognition-acr>.

¹¹ *Id.* at 6.

¹² Rachel Cericola, Jon Chase and Lee Neikirk, *Yes, Your TV Is Probably Spying on You. Your Fridge, Too. Here's What They Know*, NEW YORK TIMES (June 25, 2025), <https://www.nytimes.com/wirecutter/reviews/advice-smart-devices-data-tracking/> (last accessed Dec. 26, 2025).

¹³ *Bridgdatasets in the evolving identity world*, SAMBA TV, <https://www.samba.tv/business/identity> (last accessed Dec. 26, 2025).

with advertising delivered on the user's other devices, such as a second screen being used by the user simultaneously while watching a Samsung TV.¹⁴ Of course, the fact that Samsung can link Sensitive Information collected through the ACR Tools to data collected from the user's other devices necessarily means that the data collected from the ACR Tools is personally identifiable.

49. As Samsung's ACR Tools collect and analyze all of the information displayed on the user's Samsung TV screen at all times, some of the information captured necessarily includes highly sensitive, personally identifiable information. For example, when a user logs in to a streaming app or video game platform (e.g., Netflix, Hulu, PlayStation Plus), the ACR Tools may capture the e-mail address associated with the user's account. If the user accesses an account information page in a streaming application, the ACR Tools may capture the user's account information, including the user's full name, address, and billing information. Moreover, as Samsung TVs can be used as a computer monitor, the ACR Tools could even capture extensive, highly sensitive information accessed by the user online, such as information from medical provider online portals, banking provider financial portals, and communicated through social media and e-mail messages.

50. Through this highly invasive data collection, Samsung is able to surreptitiously amass a wealth of intimate knowledge about its customers, allowing its advertising clients to target consumers based on highly sensitive attributes such as religion, political affiliation, sexual orientation, and medical attributes.¹⁵

¹⁴ See *Understanding Video-based Automatic Content Recognition*, SAMBA TV, at 9, available online at: <https://www.samba.tv/resources/understanding-video-based-automatic-content-recognition-acr>.

¹⁵ *Audience Segments*, SAMSUNG, <https://help.dsp.samsungads.com/docs/linear-ads> (last accessed Dec. 26, 2025).

51. Further, as if this mass surveillance were not bad enough already, Samsung's misuse of its customer's Sensitive Information is not limited to merely its own advertising operations. Rather, the raw data collected by the ACR Tools is shared with third-party advertising companies including Google, Catalina, Kantar Milward Brown, and Twitter, without the Samsung TV owner's knowledge or consent.¹⁶

52. Through the use of tracking cookies that Google and Twitter's applications and web services automatically install on user devices, Google and Twitter are generally able to identify data pertaining to their accountholders regardless of its source.¹⁷ Thus, Plaintiffs allege upon information and belief that all Sensitive Information transmitted by Samsung to Google and Twitter was automatically linked to any Google and/or Twitter account held by the relevant Plaintiff or Class Member.¹⁸

B. PLAINTIFFS AND CLASS MEMBERS DID NOT CONSENT TO SAMSUNG'S COLLECTION AND MONETIZATION OF THEIR SENSITIVE INFORMATION THROUGH THE ACR TOOLS

i. Plaintiffs' and Class Members' Reasonable Expectation of Privacy

53. At all times when Plaintiffs and Class Members provided their Sensitive Information to Defendant, they each had a reasonable expectation that the information would

¹⁶ Data, SAMBA TV, <https://www.samba.tv/business/data> (last accessed Dec. 26, 2025).

¹⁷ Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (2019), available online at: https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf.

¹⁸ A remarkable number of Americans possess a Google or Twitter accounts. One-third of Americans have accounts with Google's Gmail e-mail client, and over 80-percent of Americans use YouTube, Google's video client. See Harsha Kiran, *49 Gmail Statistics To Show How Big It Is In 2024*, TECHJURY (Jan. 3, 2024), <https://techjury.net/blog/gmail-statistics/> (last accessed Oct. 23, 2025); Jeffrey Gottfried, *Americans' Social Media Use*, PEW RESEARCH (Jan. 31, 2024). And, approximately one in five Americans report using Twitter. See Jeffrey Gottfried, *Americans' Social Media Use*, PEW RESEARCH (Jan. 31, 2024), <https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/> (last visited Oct. 23, 2025).

remain confidential and that Defendant would not share the Sensitive Information with third parties for a commercial purpose, unrelated to providing them with video content.

54. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative informed consent before a company collects and shares that individual's data to be one of the most important privacy rights.

55. For example, a recent Consumer Reports study shows that 92-percent of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.¹⁹

56. Personal data privacy and obtaining consent to share Sensitive Information are material to Plaintiffs and Class Members.

ii. Plaintiffs Did Not (and Could Not) Consent to Samsung's Surveillance Practices

57. In its Privacy Notice, Samsung deceptively labels its ACR collection practices as "Viewing Information Services." With regards to its "Viewing Information Services," the Privacy Notice accessible on Samsung's TVs informs its customers only that "if you opt-in on the Smart TV for Viewing Information Service, you allow us to *process* your viewing history." The Privacy Notice further states that "Samsung neither collects any video footage *nor any content displayed on the Device*."

58. These representations are misleading. Samsung does not merely *process* its customer's viewing history; instead, it collects, monetizes, and discloses that viewing history,

¹⁹ *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> (last visited Feb. 1, 2025).

along with data reflecting any other actions the customer takes using their Samsung TV. Moreover, contrary to its representation in the Privacy Notice, Samsung does in fact collect copious amounts of content displayed on the device, as explained above. No reasonable consumer could possibly infer from the euphemistic representations in the Privacy Notice that Samsung would capture all output from the consumer's Samsung TV every 500 milliseconds, correlate that data with additional user-specific data collected from the consumer's other devices, and then provide that data to advertisers in a manner allowing it to be linked to the consumer's identity.

59. Additionally, Samsung packages this disclosure with four other notices during the set-up process for its Samsung TVs—its *Terms & Conditions: Dispute Resolution Agreement*, *Smart Hub U.S. Policy Notice*, *Viewing Information Services*, and *Interest-Based Advertisements Service U.S. Privacy Notice*—with **only one button** prominently displayed: *I Agree to all*.

60. Opt-out rights for Samsung's data collection are further scattered across four or more separate menus requiring approximately 15+ cumulative clicks to access. To fully opt-out of just ACR and related ad tracking, Samsung TV owners must disable at least two settings—(1) Viewing Information Services, and (2) Interest-Based Ads—each of which appear in different parts of the setting UI.

61. Conversely, Samsung provides consumers with a one-click enrollment option to opt-**in** during the initial start-up process.

62. In short, Samsung deliberately designed both the form and content of its ACR disclosures to obfuscate its invasive surveillance of its customers.

63. Unfortunately, such gamesmanship appears to be working as intended. Indeed, according to one survey of 36,000 U.S. consumers, only 13-percent of smart TV owners knew they

were being monitored and remembered agreeing to their smart TV's terms of service, and that 75-percent of respondents did not know how they had given their consent in the first place.²⁰

C. SAMSUNG WAS ENRICHED BY ITS COLLECTION, MONETIZATION, AND UNAUTHORIZED DISCLOSURE OF PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION

i. Samsung Derived Significant Benefits from Its Collection and Use of Plaintiffs' and Class Members' Sensitive Information

64. As detailed above, Samsung's advertising enterprise is fueled by the data collected through the ACR Tools.

65. As a direct result of its surreptitious collection, use, and disclosure of Plaintiffs and Class Members' Sensitive Information, Samsung is able to amass hundreds of millions of dollars in yearly revenue attributable to its targeted advertising sales.

ii. Plaintiffs' and Class Members' Data Had Financial Value

66. Moreover, Plaintiffs' and Class Members' Sensitive Information had value, and Defendant's disclosure and interception of that Sensitive Information harmed Plaintiffs and the Class.

67. According to the financial statements of Facebook, a major data and advertisement broker, the value derived from user data has continuously risen. "In 2013, the average American's data was worth about \$19 per year in advertising sales to Facebook, according to its financial statements. In 2020, [it] was worth \$164 per year."²¹

²⁰ Katie McQuater, *US consumers lack awareness of consent around smart TVs, finds study*, RESEARCHLIVE (July 9, 2018), <https://www.research-live.com/article/news/us-consumers-lack-awareness-of-consent-around-smart-tvs-finds-study/id/5040713> (last visited Dec. 30, 2025).

²¹ Geoffrey A. Fowler, *There's no escape from Facebook, even if you don't use it*, THE WASHINGTON POST (Aug. 29, 2021), <https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/> (last visited Feb. 1, 2025).

68. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200 billion industry wide.

69. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

70. The unauthorized disclosure of Plaintiffs' and Class Members' private and Sensitive Information has diminished the value of that information, resulting in harm including Plaintiffs and Class Members.

D. SAMSUNG'S USE OF THE ACR TOOLS VIOLATES NUMEROUS STATE AND FEDERAL DATA PRIVACY REGULATIONS

i. The Video Privacy Protection Act ("VPPA")

71. The VPPA was passed in 1988 in response to Congress's concern that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599, at p. 7 (1988) (statement of Sen. Patrick Leahy).

72. In passing the VPPA, Congress was particularly alarmed about surveillance of Americans' media consumption, recognizing that:

Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy-of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye...These records are a window into our loves, lives, and dislikes.

Id. (statement of Rep. Al McCandless).

73. Although the VPPA was originally intended to protect the privacy of an individual's rental videotape selections, Congress has repeatedly reiterated that the VPPA is applicable to "on-

demand’ cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.” S. Rep. 112-258, at p. 2.²²

74. Under the VPPA, “[a] video tape service provider” is prohibited from “knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider” without the consumer’s “informed, written consent... in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer.” 18 U.S.C. § 2710(b).

75. The VPPA defines a “video tape service provider” as “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio-visual materials.” 18 U.S.C. § 2710(a)(4).

76. The VPPA additionally defines “personally identifiable information” as “information which identifies a person as having requested or obtained specific video materials or services from a video service provider.” 18 U.S.C. § 2710(a)(3).

77. Samsung is a video tape services provider under the meaning of the VPPA, as it provides on-demand access to video content through both third-party apps offered in its TV’s “Smart Hub” as well as its own content provided to Samsung TV owners through the Samsung TV Plus on-demand video platform. Accordingly, Defendant’s disclosure of the specific videos viewed by its customers through on-demand streaming services constitutes a violation of VPPA. *See, e.g.,*

²² *See also The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW (Jan. 31, 2012), available online at https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (statement by Senator Leahy, who originally introduced the VPPA in the Senate: “Now, it is true that technology has changed...but I think we should all agree that we have to be faithful to our fundamental right to privacy and freedom. Today the social networking, video streaming, the cloud, mobile apps, and other new technologies have revolutionized the availability of Americans’ information.”).

Fan v. NBA Props. Inc., No. 23-cv-05069-SI, 2024 U.S. Dist. LEXIS 57205, at *9 (N.D. Cal. Mar. 26, 2024) (“in enacting the VPPA, ‘Congress[] inten[ded] to cover new technologies for pre-recorded video content’” and “used ‘similar audio visual materials’ to ensure that VPPA’s protections would retain their force even as technologies evolve”).²³

ii. Maryland Online Data Privacy Act (“MODPA”), 2024 Md. Laws 454 § 14-4601, *et seq.*

78. Under the MODPA, entities like Samsung are required to:

- a. limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;
- b. not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer’s consent;[...]
- c. not process sensitive data concerning a consumer without first obtaining the consumer’s consent, or, in the case of the processing of personal data concerning a known child, without processing such data in accordance with COPPA;
- d. [...and] specify the express purposes for which personal data are processed.

2024 Md. Laws 454 § 14-4607.

79. Additionally, entities like Samsung are to “not conduct processing that presents a heightened risk of harm to a consumer. 2024 Md. Laws 454 § 14-4610. Under the MODPA, a “heightened risk” includes:

- a. the processing personal data for the purposes of targeted advertising;

²³ *How ACR Data Helps Samsung Clients Get A Better Grasp Of Their Target Audience*, TVREV (FEB 7, 2022), <https://www.tvrev.com/news/how-samsung-helps-clients-get-a-better-grasp-of-their-target-audience> (last visited Dec. 30, 2025) (Global Head of Analytics & Insights at Samsung Ads: “ACR is one of the few places where you can access a single source view of television where you have one data set that covers linear and streaming”).

- b. the sale of personal data;
- c. the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and
- d. the processing of sensitive data.

Id.

80. Moreover, under these statutes, consent means: [A] clear affirmative act signifying a consumer’s freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. 2022 Ct. P.A. 15 § 1(6); 2024 Md. Laws 454 § 14-4601(G).

81. The MODPA further specifies that:

“Consent” may include a written statement, including by electronic means, or any other unambiguous affirmative action. Consent shall not include: (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (B) hovering over, muting, pausing, or closing a given piece of content; or (C) agreement obtained through the use of dark patterns.

Id.

82. Samsung’s practices described in this Complaint violated the MODPA.

iii. New Jersey Data Privacy Law (“NJDPL”), N.J. Stat. § § 56:8-166.4

83. Effective January 15, 2025, the NJDPL is a comprehensive data privacy statute that regulates some of the data collected by Defendant through the Samsung TVs.

84. Under the NJDPL, businesses like Defendant are required to:

- a. limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;
- b. not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes for which such personal data is

processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;[...]

- c. not process sensitive data concerning a consumer without first obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without processing such data in accordance with COPPA;
- d. [...and] specify the express purposes for which personal data are processed.

N.J. Stat. § 56:8-166.12.

85. Additionally, under the New Jersey law, entities like Samsung are to “not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired [after January 15, 2025] that present a heightened risk of harm to a consumer.” N.J.

Stat. § 56:8-166.12(a)(9). Under these statutes, a “heightened risk” includes:

- a. processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers; financial or physical injury to consumers; a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or other substantial injury to consumers;
- b. selling personal data; and
- c. processing sensitive data.

N.J. Stat. § 56:8-166.12.

86. Moreover, under this statute, consent means:

[A] clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer.

“Consent” may include a written statement, including by electronic means, or any other unambiguous affirmative action. Consent shall not include: acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; hovering over, muting, pausing, or closing a given piece of content; or agreement obtained through the use of dark patterns.

N.J. Stat. § 56:8-166.4.

87. Samsung's practices described in this Complaint violated the NJDPL.

V. TOLLING AND ESTOPPEL

88. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its installation of the ACR Tools onto Samsung TVs.

89. The ACR Tools installed on the Samsung TVs were and are invisible to the average TV user.

90. Through no fault or lack of diligence, Plaintiffs and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

91. Plaintiffs were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

92. Defendant had exclusive knowledge that the ACR Tools were installed on the Samsung TVs and yet failed to disclose to customers, including Plaintiffs and Class Members, that by using a Samsung TV, Plaintiffs' and Class Members' Sensitive Information would be collected and disclosed or released to unauthorized third parties.

93. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of their collection and treatment of its customers' Sensitive Information. Accordingly, Defendant is estopped from relying on any statute of limitations.

94. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

95. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

VI. CLASS ALLEGATIONS

96. This action is brought by the named Plaintiffs both individually, and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

97. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

The Nationwide Class

All natural persons who have owned a Samsung Smart TV, and whose Sensitive Information was collected without their actual and/or constructive knowledge.

98. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of separate California, New York, Vermont, and Maryland Subclasses, which are defined as follows:

California Subclass

All natural persons residing in California who own or have owned a Samsung Smart TV, and whose Sensitive Information was collected without their actual and/or constructive knowledge.

New York Subclass

All natural persons residing in New York who own or have owned a Samsung Smart TV, and whose Sensitive Information was collected without their actual and/or constructive knowledge.

Vermont Subclass

All natural persons residing in Vermont who own or have owned a Samsung Smart TV, and whose Sensitive Information was collected without their actual and/or constructive knowledge.

Maryland Subclass

All natural persons residing in Maryland who own or have owned a Samsung Smart TV, and whose Sensitive Information was collected without their actual and/or constructive knowledge.

99. The Nationwide Class, California Subclass, New York Subclass, Vermont Subclass, and Maryland Subclass are collectively referred to herein as the “Class.” Excluded from the proposed Class are any claims for personal injury, wrongful death, or other property damage sustained by the Class; Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns; and any Judge conducting any proceeding in this action and members of their immediate families.

100. Plaintiffs reserve the right to amend the definitions of the Class or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

101. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 100,000 individuals that have been impacted by Defendant’s actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

102. **Commonality.** Common questions of law or fact arising from Defendant’s conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

- a) Whether and to what extent Defendant had a duty to protect the Sensitive Information of Plaintiffs and Class Members;
- b) Whether Defendant had duties not to collect and/or disclose the Sensitive Information of Plaintiffs and Class Members to unauthorized third parties;
- c) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Sensitive Information would be collected and disclosed to third parties;

- d) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Sensitive Information was being collected and disclosed without their consent;
- e) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized collection and disclosure of patients' Sensitive Information;
- f) Whether Defendant violated the Video Privacy Protection Act, as alleged in this Complaint;
- g) Whether Defendant violated the statutes mentioned in this Complaint;
- h) Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; and
- i) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's collection and disclosure of their Sensitive Information.

103. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the ACR Tools.

104. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

105. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including third parties, like Google, in the same

way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

106. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

107. Defendant acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

108. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a) Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Sensitive Information and not disclosing it to unauthorized third parties;

- b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;
- c) Whether Defendant failed to comply with applicable laws, regulations, and industry standards relating to data security;
- d) Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Sensitive Information would be collected disclosed to third parties;
- e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information collected and disclosed to third parties; and
- f) Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

109. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the unauthorized disclosures that have taken place.

COUNT I

COMMON LAW INVASION OF PRIVACY

(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California, New York, Vermont, and Maryland Subclass(es))

110. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 109 as if fully set forth herein.

111. Plaintiffs and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, highly personal Sensitive Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various television platforms or services without being subjected to the exfiltration of their communications without Plaintiffs' and Class Members' knowledge or consent.

112. Plaintiffs and Class Members had a reasonable expectation of privacy in the

information transmitted and received through use of their Samsung TVs and the communications platforms and services therein.

113. Defendant's interception and disclosure of the substance and nature of those communications without the knowledge and informed consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

114. Plaintiffs and Class Members have a general expectation that their communications regarding sensitive, highly personal information would be protected from surreptitious disclosure to third parties.

115. Defendant's disclosure of Plaintiffs' and Class Members' Sensitive Information coupled with individually identifying information is highly offensive to the reasonable person.

116. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

117. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to compensatory and/or nominal damages.

118. Plaintiffs and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of the intrusions upon their privacy.

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

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

COUNT II
NEGLIGENCE

(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California, New York, Vermont, and Maryland Subclass(es))

121. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 120 as if fully set forth herein.

122. Through using their Samsung TVs, Plaintiffs and Class Members provided Defendant with their Sensitive Information.

123. By collecting and storing data related to Plaintiffs and Class Members use of their Samsung TVs, Defendant had a duty of care to use reasonable means to secure and safeguard it from unauthorized disclosure to third parties.

124. Defendant negligently, recklessly, and/or intentionally failed to take reasonable steps to protect Plaintiffs' and Class Members' Sensitive Information from being disclosed to third parties, without their consent, including to major advertising companies like Google and Twitter.

125. Defendant further negligently, recklessly, and/or intentionally omitted to inform Plaintiffs and the Class that it would collect and use their Sensitive Information for marketing purposes, or that their Sensitive Information would be transmitted to third parties.

126. Defendant knew, or reasonably should have known, that Plaintiffs and the Class would not have provided their Sensitive Information to Defendant had Plaintiffs and the Class known that Defendant intended to use that information for unlawful purposes.

127. Defendant's conduct has caused Plaintiffs and the Class to suffer damages by having their highly confidential, personally identifiable Sensitive Information accessed, stored, and disseminated without their knowledge or consent.

128. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages.

129. Defendant's negligent conduct is ongoing, in that they still hold the Sensitive

Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) cease collection and dissemination of the Samsung TV users' Sensitive Information to third parties; and (iii) submit to future annual audits of those systems and monitoring procedures.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California, New York, Vermont, and Maryland Subclass(es))

130. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 129 as if fully set forth herein.

131. When Plaintiffs and Class Members provided their Sensitive Information to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Sensitive Information without consent.

132. Plaintiffs and Class Members accepted Defendant's offers and provided their Sensitive Information to Defendant.

133. Plaintiffs and Class Members would not have entrusted Defendant with their Sensitive Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Sensitive Information without consent.

134. Defendant breached these implied contracts by accessing and disclosing Plaintiffs' and Class Members' Sensitive Information to third parties like Google and Twitter.

135. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

136. Plaintiffs and Class Members would not have bought a Samsung TV if they had known that their Sensitive Information would be accessed and disclosed.

137. Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT IV
UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Nationwide Class or, alternatively, the California, New York, Vermont, and Maryland Subclass(es))

138. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 137 as if fully set forth herein.

139. Plaintiffs plead this claim in the alternative to their breach of implied contract claim.

140. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of (a) payment for their Samsung TVs, and (b) providing their inherently valuable Sensitive Information to Defendant, which Defendant used to profit through the targeted advertising sales, described *supra*.

141. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from the Sensitive Information of Plaintiffs and Class Members by using it for marketing and advertising.

142. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize their own profits over the privacy of their Sensitive Information.

143. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, obtained by its surreptitious collection and transmission of their Sensitive Information.

144. If Plaintiffs and Class Members knew that Defendant would be disclosing their Sensitive Information to unauthorized third parties, they would not have agreed to provide their

Sensitive Information to Defendant.

145. Plaintiffs and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damage.

146. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury.

147. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them and from the collection and unauthorized distribution of the Sensitive Information, or to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
VIOLATIONS OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

148. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 147 as if fully set forth herein.

149. The VPPA provides that “a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person[.]” 18 U.S.C. § 2710(b)(1).

150. “Personally-identifiable information” is defined to include “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3).

151. A “video tape service provider” is “any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

152. Defendant is a “video tape service provider” because their primary business is the monetization of Samsung TVs, which host thousands of videos, thereby “engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4).

153. Defendant violated the VPPA by knowingly disclosing Plaintiffs’ and Class Members’ personally identifiable Sensitive Information to third party advertising partners, including Google, Catalina, Kantar Milward Brown, and Twitter, without obtaining informed, written consent.

154. As a result of Defendant’s violations of the VPPA, Plaintiffs and the Class are entitled to all damages available under the VPPA including declaratory relief, injunctive and equitable relief, statutory damages of \$2,500 for each violation of the VPPA, and attorney’s fees, filing fees, and costs.

COUNT VI
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
(“ECPA”), 18 U.S.C. § 2511(1), *et seq.*
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiffs and the Nationwide Class)

155. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 154 as if fully set forth herein.

156. The ECPA protects both sending and receipt of communications.

157. 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.

158. The transmissions of Plaintiffs’ Sensitive Information while using their Samsung TVs qualify as “communications” under the ECPA’s definition of 18 U.S.C. § 2510(12).

159. Electronic Communications. The transmission of Sensitive Information between Plaintiffs and Class Members and Defendant's Samsung TVs 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).

160. Content. 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) (emphasis added).

161. Interception. 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).

162. Electronic, Mechanical or Other Device. 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. Plaintiffs' and Class Members' Samsung TVs;
- b. Defendant's web-servers; and
- c. The ACR software code(s) deployed by Defendant to effectuate the sending and acquisition of patient communications.

163. By utilizing and embedding the ACR Tools on the Samsung TVs, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

164. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the ACR Tools, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Sensitive Information to third parties such as Google and Twitter.

165. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Sensitive Information.

166. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs 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).

167. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs 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).

168. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' 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, among others.

169. The ECPA provides that a “party to the communication” may liable where a “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C § 2511(2)(d).

170. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication,

forwarding, and interception of Plaintiffs' and Class Members' Sensitive Information does not qualify for the party exemption.

171. Defendant's acquisition of sensitive communications that were used and disclosed to Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

- a. Invasion of privacy;
- b. Breach of implied contract;
- c. Violations of the Video Privacy Protection Act, 18 U.S.C. §§ 2710, *et seq.*;
- d. Violations of N.Y. Gen. Bus. Law § 349;
- e. Violations of the California Invasion of Privacy Act, Cal. Pen. Code §§ 360, *et seq.*;
- f. Violations of the California Unfair Competition Law, Cal. Bus. & Prof. Code, §§ 17200, *et seq.*
- g. Violations of the Vermont Consumer Fraud Act, Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*;
- h. Violations of the New Jersey Consumer Fraud Act, N.J. Stat. Ann. 56:8-1, *et seq.*;
- i. Violations of the New Jersey Data Protection Law, N.J. Stat. §§ 56:8-166.4, *et seq.*; and
- a. Violations of the Maryland Online Data Privacy Act, 2024 Md. Laws 454 §§ 14-4601, *et seq.*

172. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it used and caused to be used personally identifiable data associated with specific users, including Plaintiffs and Class Members, without user authorization; and disclosed individually identifiable Sensitive Information to Google and Twitter without user authorization.

173. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Sensitive Information through their Samsung TV, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Sensitive Information with Google, Twitter, and other third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their Sensitive Information, and that Plaintiffs and Class Members did not consent to receive their Sensitive Information.

174. As such, Defendant cannot viably claim any exception to ECPA liability.

175. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their Sensitive Information for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' Sensitive Information without providing any value or benefit to Plaintiffs or Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' Sensitive Information, such as understanding how people use their Samsung TVs and determining what ads people see when using their Samsung TVs, without providing any value or benefit to Plaintiffs or Class Members; and
- d. The diminution in value of Plaintiffs' and Class Members' Sensitive Information and/or the loss of privacy due to Defendant making such Sensitive Information, which Plaintiffs and Class Members intended to remain private, no longer private.

176. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the ACR Tools to track and utilize Plaintiffs' and Class Members' Sensitive Information for financial gain.

177. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

178. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the ACR Tools.

179. Any purported consent that Defendant may claim to have received from Plaintiffs and Class Members was not valid.

180. In sending and acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Samsung TVs, Defendant's purpose was

tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

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

COUNT VII
**VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW – DECEPTIVE ACTS
OR PRACTICES**
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff Rood and the New York Subclass)

182. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 181 as if fully set forth herein.

183. N.Y. Gen. Bus. Law § 349 prohibits use of “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service[.]”

184. Defendant violated N.Y. Gen. Bus. Law § 349 by using the ACR Tools to record, monetize and transmit Plaintiff Rood and New York Subclass Members' Sensitive Information without their knowledge of consent.

185. Defendant intended to mislead Plaintiff Rood and New York Subclass Members and intended to induce Plaintiff Rood and New York Subclass Members to rely on its misrepresentations and omissions.

186. As a result of Defendant's violation of N.Y. Gen. Bus. Law. § 349, Plaintiff Rood and New York Subclass Members are entitled to actual damages, treble damages, and attorneys' fees, filing fees, and costs.

COUNT VIII
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”)
Cal. Pen. Code §§ 360, *et seq.*
(On Behalf of Plaintiffs DiGiacinto and Tillery, and the California Subclass)

187. Plaintiffs DiGiacinto and Tillery repeat and reallege the allegations contained in paragraphs 1 through 186 as if fully set forth herein.

188. The California Legislature enacted CIPA in response to “advances in science and technology” that “have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications[.]” recognizing 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. Pen. Code. § 630.

189. Under CIPA, it is unlawful to:

- a. “[W]illfully and ***without the consent of all parties to the communication***, or in any unauthorized manner, read[], or attempt[] 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
- b. “[U]se, or attempt[] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained[;]” or
- c. [A]id, agree[] with, employ[], or conspire[] with any person or persons to unlawfully do, or permit, or cause to be done any of the acts [prohibited by CIPA.]”

Cal. Penal Code § 631(a) (emphasis added).

190. At all relevant times, Defendant tracked and intercepted Plaintiff DiGiacinto's, Plaintiff Tillery's, and California Subclass Members' internet communications made through their Samsung TVs by installing and configuring the ACR Tools without their knowledge.

191. The content of those conversations included Sensitive Information. Through Defendant's installation and configuration of the ACR Tools on the Samsung TVs, these communications were intercepted by Samsung and disclosed to unauthorized third parties without the knowledge, authorization, or consent of Plaintiff DiGiacinto, Plaintiff Tillery, and California Subclass Members.

192. Defendant intentionally installed an electronic device onto the Samsung TVs that, without the knowledge and consent of Plaintiff DiGiacinto, Plaintiff Tillery, and California Subclass Members, collected and transmitted the substance of their confidential communications.

193. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the ACR Tools falls under the broad catch-all category of "any other manner":

- a. The ACR software code;
- b. Plaintiff DiGiacinto's, Plaintiff Tillery's, and the California Subclass Members' web-enabled Samsung TVs;
- c. Plaintiff DiGiacinto's, Plaintiff Tillery's, and the California Subclass Members' computing and mobile devices; and
- d. Samsung's web and ad servers.

194. As demonstrated hereinabove, Defendant violated CIPA intercepting and disclosing Plaintiff DiGiacinto's, Plaintiff Tillery's, and California Subclass Members' Sensitive Information in real time through the ACR Tools without their consent.

195. By disclosing Plaintiff DiGiacinto's, Plaintiff Tillery's, and the California Subclass Members' Sensitive Information, Defendant violated Plaintiff DiGiacinto's, Plaintiff Tillery's, and California Subclass Members' statutorily protected right to privacy.

196. As a result of Defendant's violation of the CIPA, Plaintiff DiGiacinto, Plaintiff Tillery, and the California Subclass Members are entitled to treble actual damages related to their loss of privacy in an amount to be determined at trial, statutory damages, attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages.

COUNT IX
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code, §§ 17200, *et seq.*
(On Behalf of Plaintiffs DiGiacinto and Tillery, and the California Subclass)

197. Plaintiffs DiGiacinto and Tillery repeat and reallege the allegations contained in paragraphs 1 through 196 as if fully set forth herein.

198. The UCL prohibits any "unlawful, unfair or fraudulent business act or practice" and any "unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

199. Defendant violated the "unlawful" prong of the UCL by violating Plaintiff DiGiacinto's, Plaintiff Tillery's, and the California Subclass Members' right to privacy, as well as by violating the statutory counts alleged herein.

200. Defendant violated the unfair prong of the UCL by:

- a. Using the ACR Tools to record and transmit the sensitive communications made by and to Plaintiff DiGiacinto, Plaintiff Tillery, and the California Subclass Members through their Samsung TVs; and
- b. Disclosing the sensitive communications made by and to Plaintiff DiGiacinto, Plaintiff Tillery, and the California Subclass Members through their Samsung TVs to third parties, including Google and Twitter.

201. As a result of Defendant's violations of the UCL, Plaintiff DiGiacinto, Plaintiff Tillery, and the California Subclass Members have suffered the diminution of the value of their Sensitive Information, as alleged above.

202. As a result of Defendant's violation of the UCL, Plaintiff DiGiacinto, Plaintiff Tillery, and the California Subclass Members are entitled to injunctive relief, as well as restitution necessary to restore to them in interest any money or property, real or personal, acquired through Defendant's unfair competition practices.

COUNT X
VIOLATIONS OF THE VERMONT CONSUMER FRAUD ACT
Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*
(On Behalf of Plaintiff Baker and the Vermont Subclass)

203. Plaintiff Baker repeats and realleges the allegations contained in paragraphs 1 through 202 as if fully set forth herein.

204. Plaintiff Baker is a "consumer," as defined by Vt. Stat. Ann. tit. 9, § 2451a(1).

205. Defendant is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(3).

206. The Samsung TVs are "goods," as defined by Vt. Stat. Ann. tit. 9, § 2451a(2).

207. Vt. Stat. Ann. tit. 9, § 2453 prohibits "unfair or deceptive acts or practices in commerce."

208. Defendant violated the Vermont Consumer Fraud Act by collecting, monetizing, and disclosing Plaintiff Baker's and Vermont Subclass Members' Sensitive Information, as detailed above, without their knowledge or consent.

209. Defendant intended to mislead Plaintiff Baker and Vermont Subclass Members and intended to induce Plaintiff Baker and Vermont Subclass Members to rely on its misrepresentations and omissions.

210. Plaintiff Baker and Vermont Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages equal to three times the value of the consideration given by them to Defendant, and attorneys' fees, filing fees, and costs

COUNT XI
VIOLATIONS OF NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. 56:8-1, et seq.
(On Behalf of Plaintiffs and the Nationwide Class)

211. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 210 as if fully set forth herein.

212. Defendant is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

213. Defendant sells and advertises "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

214. N.J. Stat. Ann. 56:8-2 prohibits:

The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby[.]

215. Defendant violated the New Jersey Consumer Fraud Act by failing to inform Plaintiffs and Class Members that they would collect, monetize and disclose Plaintiffs and Class Members' Sensitive Information, as detailed above.

216. Defendant intended to mislead Plaintiffs and Class Members and intended to induce Plaintiffs and Class Members to rely on its misrepresentations and omissions.

217. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of other Class Members, pray for judgment against Defendant as follows:

- A. an Order certifying the Nationwide Class, and California, New York, Vermont, and Maryland Subclasses, and appointing the Plaintiffs and their Counsel to represent the Classes;
- B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiffs and Class Members;
- C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
- D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;
- E. an award of attorney fees, costs, and litigation expenses, as allowed by law;
- F. prejudgment interest on all amounts awarded; and
- G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and other members of the proposed Class, hereby demand a jury trial on all issues so triable.

Dated: January 9, 2026

Respectfully submitted,

/s/ Alyssa Tolentino

Alyssa Tolentino (Bar No. 6195481)

Tyler J. Bean*

Sonjay C. Singh*

SIRI & GLIMSTAD LLP

745 Fifth Avenue, Suite 500

New York, New York 10151

Tel: (212) 532-1091

E: atolentino@sirillp.com

E: tbean@sirillp.com

E: ssingh@sirillp.com

**pro hac vice admission anticipated*

Attorneys for Plaintiffs and the Class