Melisa A. Rosadini-Knott
mrosadini@peifferwolf.com
(California Bar No. 316369)
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010-1923
323-982-4109

[Additional counsel listed on signature page]
Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

STACEE SEVERINO, JILL COHEN, KENNEY REESE, SHARI ETCHEBARREN, and BRANDY MINNER, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

HISENSE USA CORPORATION,

Defendant.

Case No.: 3:26-cv-04379-MMC

AMENDED CLASS ACTION COMPLAINT FOR PUBLIC INJUNCTION, DAMAGES, AND DECLARATORY RELIEF, AND DEMAND FOR JURY TRIAL

Plaintiffs Stacee Severino, Jill Cohen, Kenney Reese, Shari Etchebarren, and Brandy Minner (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant Hisense USA Corporation ("Hisense" or "Defendant") 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. This case is about commercial surveillance and the systematic, ongoing, and unlawful export of bulk sensitive personal data of millions of Americans—captured continuously, in real time, from their living rooms—by a Chinese state-owned consumer-electronics conglomerate, in direct violation of federal law promulgated specifically to address such transfers as "unusual and extraordinary threats" to United States national security and foreign policy.

2. Defendant Hisense USA Corporation is the U.S. operating arm of Hisense Group Holdings Co., Ltd., a state-owned enterprise headquartered in Qingdao, People's Republic of China and majority-owned and controlled, directly and indirectly, by the Qingdao municipal government and other Chinese state-owned entities. Hisense's Smart TVs sit in millions of American living rooms, including the homes of military servicemembers, intelligence-community personnel, judges, elected officials, journalists, and dissidents. Through automatic content recognition ("ACR") technology embedded in these devices and operated by Hisense (directly and through its wholly-owned operating-system and ACR subsidiary VIDAA, USA, Inc.), Hisense and VIDAA capture every sound and image displayed on the screen as often as every 500 milliseconds, link that data to persistent device-, household-, and cross-device identifiers, and re-distribute the resulting bulk sensitive personal data to a network of downstream ad-tech, identity-graph, data-broker, and measurement partners—and, on information and belief, to Hisense's Chinese parents and affiliates, which are subject to Chinese law (including Article 7 of the PRC National Intelligence Law) compelling them to share that data with the Chinese government and the Chinese Communist Party ("CCP") on demand.

3. On April 8, 2025, the United States Department of Justice's Data Security Program—the "Rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," 28 C.F.R. Part 202, promulgated under Executive Order 14117 (the "DOJ Rule" or "Bulk Sensitive Data Transfer Rule")—took effect. The DOJ Rule prohibits U.S. persons from transferring, or facilitating access to, bulk U.S. sensitive personal data—including IP addresses, MAC addresses and other device identifiers, advertising identifiers, cookie data, and the granular viewing-behavior data with which they are linked—by "covered persons" in "countries of concern" (which expressly includes China). Willful violations are punishable as criminal offenses under the International Emergency Economic Powers Act (50 U.S.C. § 1705(c)), with penalties of up to $1 million in fines and 20 years' imprisonment per violation. Defendant's ongoing transfer of, and facilitation of access to, bulk Hisense ACR data by Hisense's Chinese parents and affiliates, without compliance with the strict CISA Security Requirements that apply to such transfers, is precisely the conduct that the DOJ Rule was designed to prevent.

4. The Texas Attorney General has already taken action. On December 15, 2025, Attorney General Ken Paxton filed an Original Petition and Application for Temporary and Permanent Injunctions against Hisense USA Corporation in Comal County, Texas, alleging that Hisense Smart TVs "aren't just entertainment devices—they're mass surveillance systems," and that "[t]he Chinese Communist Party — has access to all of the ACR data collected." Within days of filing, Attorney General Paxton secured a "first-of-its-kind" temporary restraining order against Hisense, prohibiting Hisense from any further collection, use, sale, sharing, disclosure, or transfer of ACR data about Texans during the pendency of the Texas action. Plaintiffs and Class Members in California (and across the United States) deserve no less protection. This action seeks to vindicate the privacy and national-security interests that Hisense and VIDAA continue to violate, and to recover the damages and equitable relief to which Plaintiffs and Class Members are entitled under federal and California law.

5. Modern televisions are no longer passive entertainment devices. Sitting in millions of American living rooms, today's "Smart TVs" operate as sophisticated surveillance systems—continuously monitoring what appears on the screen and transmitting detailed records of consumers' viewing behavior to manufacturers and advertising companies.

6. Hisense designs, manufactures, markets, distributes, and sells internet-connected televisions, including the Hisense-branded line of Smart TVs (running the proprietary VIDAA OS, Google TV, or Roku OS operating systems) used by millions of consumers across the United States.

7. Unbeknownst to consumers, Hisense Smart TVs incorporate ACR technology and related tracking systems (collectively, the "ACR Tools") that continuously monitor and analyze what appears on the television screen.

8. In other words, Hisense Smart TVs monitor *virtually everything displayed on the screen*, regardless of its source.

9. Hisense and its wholly-owned ACR provider VIDAA, together with Hisense's downstream advertising, analytics, and ad-tech partners, combine consumers' viewing activity with these identifiers—and with additional identifiers obtained from other sources, such as hashed email addresses and mobile advertising IDs—to link the television to other devices associated with the same individual or household, including smartphones, tablets, and computers.

10. The information collected and derived through these practices (the "Sensitive Information") includes: (i) consumers' video-viewing activity and the specific content they watch; (ii) information displayed on the television screen during use; (iii) device-level and network identifiers, including IP addresses and persistent device identifiers; (iv) cross-device identifiers and linkages, including identifiers that associate the television with other devices and accounts; and (v) inferences drawn from the foregoing, including consumers' interests, habits, and personal characteristics.

11. As a result, Plaintiffs and millions of Hisense Smart TV owners have had their viewing behavior secretly monitored and monetized without their knowledge or consent.

12. Hisense's conduct violates numerous federal and state privacy laws and constitutes an unlawful invasion of consumers' privacy.

13. Hisense's conduct also implicates urgent national-security concerns. Hisense is, at its corporate core, a Chinese state-owned enterprise. Hisense's ACR system collects bulk U.S. sensitive personal data—including IP addresses, device identifiers, advertising identifiers, cookie data, and granular records of in-home viewing behavior—and that data is, on information and belief, transferred to or made accessible by Hisense's Chinese parents and affiliates and by additional downstream ad-tech partners, in real time or near-real time, in violation of the DOJ Rule.

14. Hisense's ACR data collection and disclosure is not limited to internal Hisense systems. On information and belief, Hisense systematically discloses ACR-derived viewing data and persistent identifiers, in real time or near-real time, to multiple separate third-party ad-tech, data-broker, and identity-graph companies—including but not limited to VIDAA USA, Inc., Nexxen International Ltd., Roku, Inc. (on Hisense Smart TVs that use the Roku OS operating system), Amazon.com Services LLC and Amazon Advertising LLC (on Hisense Smart TVs that use the Amazon Fire TV operating system), and Alphonso, Inc. (now part of LG Ad Solutions)—each of which independently captures, processes, and uses Plaintiffs' and Class Members' intercepted communications for its own commercial purposes, including targeted advertising, audience segmentation, identity-graph construction, and measurement.

15. Moreover, Defendant's tracking of Hisense TV users violated 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.

16. 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 (vii) continued and ongoing risk to their Sensitive Information.

17. 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 – intrusion upon seclusion; invasion of privacy – public disclosure of private facts; invasion of privacy in violation of the California Constitution; violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631, 632, and 638.50–638.51; violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, et seq.; violation of the VPPA, 18 U.S.C. § 2710; negligence; violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.; violation of the California Consumers Legal Remedies Act (CLRA), Cal. Civ. Code § 1780(a)(2); unjust enrichment; and a public injunction on behalf of the general public.

II. THE PARTIES

A. Plaintiff Stacee Severino

18. Plaintiff Stacee Severino is a resident and citizen of Crescent City, California, in the Eureka—McKinleyville Division of the Northern District of California.

19. Plaintiff Severino purchased a Hisense Smart TV (model 55R6E) in approximately 2018, and has used it regularly since then while in her home in Crescent City, California. Plaintiff Severino's home internet service is provided by Spectrum. The Hisense Smart TV runs the Roku OS operating system, in which Hisense's ACR functionality is enabled by default.

20. Plaintiff Severino, along with the two other members of her household (totaling three people in her household), regularly uses the Hisense Smart TV to access video-viewing content, including through streaming services such as the Roku Channel and Amazon Prime Video, as well as through Hisense's native "Hisense TV+" / VIDAA Free streaming service. The video-viewing content Plaintiff Severino selected and watched within the privacy of her home constitutes private, Sensitive Information.

21. Because Plaintiff Severino's Hisense Smart TV is a Hisense Roku TV running the Roku OS operating system, the ACR-derived viewing communications captured by the device are transmitted to and processed by Roku, Inc. in real time and incorporated into Roku's OneView/dataxu identity graph as alleged herein. On information and belief, Defendant's ACR functionality also operates at the chipset and firmware level, such that Hisense's ACR data from this device is also transmitted to VIDAA, Hisense's Chinese parents and affiliates, and additional downstream ad-tech partners as alleged herein.

22. Plaintiff Severino set up her Hisense Smart TV herself. At no time was Plaintiff Severino presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing Hisense's or VIDAA's collection, interception, or use of her viewing activity or associated data.

23. Unbeknownst to Plaintiff Severino, Hisense's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the Hisense Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Severino never authorized Defendant Hisense or VIDAA to collect, intercept, analyze, monetize, or disclose her Sensitive Information, did not consent to the interception of her viewing activity or device identifiers, and did not consent to the creation of cross-device identity profiles or the use of her private viewing behavior for advertising or other commercial purposes.

B. Plaintiff Jill Cohen

24. Plaintiff Jill Cohen is a resident and citizen of Chino, California, in the Eastern District of California.

25. Plaintiff Cohen purchased a Hisense Smart TV (model 65QD65NF) in approximately 2025, and has used it regularly since then while in her home in Chino, California. Plaintiff Cohen's home internet service is provided by T-Mobile (T-Mobile Home Internet). The Hisense Smart TV runs the Amazon Fire TV operating system, in which Hisense's ACR functionality is enabled by default.

26. Plaintiff Cohen, along with her adult daughter (totaling two adults in her household), regularly uses the Hisense Smart TV to access video-viewing content, including through streaming services such as Paramount+, Netflix, Peacock, Amazon Prime Video, and Apple TV+, as well as through Hisense's native "Hisense TV+" / VIDAA Free streaming service. The video-viewing content Plaintiff Cohen selected and watched within the privacy of her home constitutes private, Sensitive Information.

27. Because Plaintiff Cohen's Hisense Smart TV is a Hisense Fire TV running the Amazon Fire TV operating system, the ACR-derived viewing communications captured by the device are transmitted to and processed by Amazon.com Services LLC and Amazon Advertising LLC (collectively, "Amazon") in real time and incorporated into Amazon's DSP, Twitch, and identity-graph systems as alleged herein. On information and belief, Defendant's ACR functionality also operates at the chipset and firmware level, such that Hisense's ACR data from this device is also transmitted to VIDAA, Hisense's Chinese parents and affiliates, and additional downstream ad-tech partners as alleged herein.

28. Plaintiff Cohen did not participate in the assembly, installation, or initial configuration of the Hisense Smart TV. Those steps were performed by Plaintiff Cohen's adult daughter, who performed the bulk of the device installation and setup. At no time was Plaintiff Cohen presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing Hisense's or VIDAA's collection, interception, or use of her viewing activity or associated data.

29. Unbeknownst to Plaintiff Cohen, Hisense's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the Hisense Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Cohen never authorized Defendant Hisense or VIDAA to collect, intercept, analyze, monetize, or disclose her Sensitive Information, did not consent to the interception of her viewing activity or device

identifiers, and did not consent to the creation of cross-device identity profiles or the use of her private viewing behavior for advertising or other commercial purposes.

C. Plaintiff Kenney Reese

30. Plaintiff Kenney Reese is a resident and citizen of Los Angeles, California, in the Central District of California.

31. Plaintiff Reese purchased a Hisense Smart TV (model 65A6H) in approximately 2022, and has used it regularly since then while in his home in Los Angeles, California. The Hisense Smart TV runs the Google TV operating system, in which Hisense's ACR functionality is enabled by default.

32. Plaintiff Reese, along with his wife (totaling two adults in his household), regularly uses the Hisense Smart TV to access video-viewing content, including through streaming services such as Netflix, Tubi, YouTube, and Hulu, as well as through Hisense's native "Hisense TV+" / VIDAA Free streaming service. The video-viewing content Plaintiff Reese selected and watched within the privacy of his home constitutes private, Sensitive Information.

33. Because Plaintiff Reese's Hisense Smart TV is a Hisense Google TV running the Google TV operating system, the ACR-derived viewing communications captured by the device are transmitted to and processed by Google LLC in real time and incorporated into Google's ad-tech and identity-graph systems as alleged herein. On information and belief, Defendant's ACR functionality also operates at the chipset and firmware level, such that Hisense's ACR data from this device is also transmitted to VIDAA, Nexxen, Hisense's Chinese parents and affiliates, and additional downstream ad-tech partners as alleged herein.

34. Plaintiff Reese set up his Hisense Smart TV himself. At no time was Plaintiff Reese presented with, or did he knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing Hisense's or VIDAA's collection, interception, or use of his viewing activity or associated data.

35. Unbeknownst to Plaintiff Reese, Hisense's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed his Sensitive Information

during his use of the Hisense Smart TV (including the specific programs and content he viewed, applications he accessed, device-level identifiers, and his IP address). Plaintiff Reese never authorized Defendant Hisense or VIDAA to collect, intercept, analyze, monetize, or disclose his Sensitive Information, did not consent to the interception of his viewing activity or device identifiers, and did not consent to the creation of cross-device identity profiles or the use of his private viewing behavior for advertising or other commercial purposes.

D. Plaintiff Shari Etchebarren

36. Plaintiff Shari Etchebarren is a resident and citizen of Diamond Bar, California, in the Central District of California.

37. Plaintiff Etchebarren purchased a Hisense Smart TV (model 32H4030F4) in approximately 2025, and has used it regularly since then while in her home in Diamond Bar, California. The Hisense Smart TV runs the Roku OS operating system, in which Hisense's ACR functionality is enabled by default.

38. Plaintiff Etchebarren, along with the two other members of her household, including at least one minor child (totaling three people in her household), regularly uses the Hisense Smart TV to access video-viewing content, including through streaming services such as Netflix, Amazon Prime Video, Paramount+, YouTube, Tubi, and Peacock, as well as through Hisense's native "Hisense TV+" / VIDAA Free streaming service. The video-viewing content Plaintiff Etchebarren selected and watched within the privacy of her home constitutes private, Sensitive Information.

39. Because Plaintiff Etchebarren's Hisense Smart TV is a Hisense Roku TV running the Roku OS operating system, the ACR-derived viewing communications captured by the device are transmitted to and processed by Roku, Inc. in real time and incorporated into Roku's OneView/dataxu identity graph as alleged herein. On information and belief, Defendant's ACR functionality also operates at the chipset and firmware level, such that Hisense's ACR data from this device is also transmitted to VIDAA, Hisense's Chinese parents and affiliates, and additional downstream ad-tech partners as alleged herein.

40. Plaintiff Etchebarren set up her Hisense Smart TV herself. At no time was Plaintiff Etchebarren presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing Hisense's or VIDAA's collection, interception, or use of her viewing activity or associated data.

41. Unbeknownst to Plaintiff Etchebarren, Hisense's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the Hisense Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Etchebarren never authorized Defendant Hisense or VIDAA to collect, intercept, analyze, monetize, or disclose her Sensitive Information, did not consent to the interception of her viewing activity or device identifiers, and did not consent to the creation of cross-device identity profiles or the use of her private viewing behavior for advertising or other commercial purposes.

E. Plaintiff Brandy Minner

42. Plaintiff Brandy Minner is a resident and citizen of Stockton, California, in the Eastern District of California.

43. Plaintiff Minner purchased a Hisense Smart TV (model 43H4030F4) in or around September 2025, and has used it regularly since then while in her home in Stockton, California. Plaintiff Minner's home internet service is provided by Xfinity. The Hisense Smart TV runs the Roku OS operating system, in which Hisense's ACR functionality is enabled by default.

44. Plaintiff Minner, along with the two other members of her household (totaling three people in her household), regularly uses the Hisense Smart TV to access video-viewing content, including through various streaming services, as well as through Hisense's native "Hisense TV+" / VIDAA Free streaming service. The video-viewing content Plaintiff Minner selected and watched within the privacy of her home constitutes private, Sensitive Information.

45. Because Plaintiff Minner's Hisense Smart TV is a Hisense Roku TV running the Roku OS operating system, the ACR-derived viewing communications captured by the device are transmitted to and processed by Roku, Inc. in real time and incorporated into Roku's

OneView/dataxu identity graph as alleged herein. On information and belief, Defendant's ACR functionality also operates at the chipset and firmware level, such that Hisense's ACR data from this device is also transmitted to VIDAA, Hisense's Chinese parents and affiliates, and additional downstream ad-tech partners as alleged herein.

46. Plaintiff Minner set up her Hisense Smart TV herself. At no time was Plaintiff Minner presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing Hisense's or VIDAA's collection, interception, or use of her viewing activity or associated data.

47. Unbeknownst to Plaintiff Minner, Hisense's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the Hisense Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Minner never authorized Defendant Hisense or VIDAA to collect, intercept, analyze, monetize, or disclose her Sensitive Information, did not consent to the interception of her viewing activity or device identifiers, and did not consent to the creation of cross-device identity profiles or the use of her private viewing behavior for advertising or other commercial purposes.

48. Prior to purchase, each Plaintiff was exposed to and relied upon Hisense's branding, packaging, and marketing representing the Hisense Smart TV as a premium personal entertainment device offering a personalized viewing experience, and was unaware—because Hisense concealed these facts—of the ACR surveillance, third-party disclosures, and PRC data-transfer practices alleged herein. Had these facts been disclosed, each Plaintiff would not have purchased the television at the price paid, or would not have purchased it at all.

49. Each named Plaintiff continues to own and use his or her Hisense Smart TV, which remains operational and connected, such that each Plaintiff's viewing activity and associated identifiers remain subject to Defendant's ongoing, continuous ACR interception, collection, transmission, and disclosure. Absent injunctive relief, Defendant's unlawful conduct will continue to capture and disclose Plaintiffs' Sensitive Information. Plaintiffs therefore face a real and

immediate threat of continuing and future injury, and monetary damages—which can redress only past collection—cannot remedy this ongoing and prospective harm.

F. Defendant Corporations

50. Defendant Hisense USA Corporation ("Hisense USA" or "Hisense") is a Georgia corporation regularly transacting, soliciting, and conducting business in California, with its principal place of business at 5995 Windward Parkway, Suite 500-A, Alpharetta, Georgia 30005. Hisense USA may be served through its registered agent for service of process in California, Chris Gardner, c/o Moreno Valley Logistic Center 4, 22750 Cactus Avenue, Moreno Valley, CA 92553, or through its registered agent in Georgia. Plaintiff requests service at this time.

51. Hisense USA Corporation is the principal U.S. arm of the Chinese global consumer-electronics manufacturer Hisense Group Holdings Co., Ltd. (and its publicly traded affiliate Hisense Co., Ltd.), a state-owned enterprise headquartered in Qingdao, People's Republic of China. Hisense designs, manufactures, markets, distributes, and sells televisions, appliances, and other consumer electronics in the United States, including the Hisense Smart TVs at issue in this Complaint. Hisense, directly and through its wholly-owned operating-system and ACR subsidiary VIDAA, USA, Inc., designs, develops, deploys, and operates the VIDAA smart-television operating system and the ACR functionality embedded in Hisense Smart TVs (and contracts with Roku, Inc., Amazon.com Services LLC, Alphonso, Inc., and Nexxen International Ltd. for additional ACR and ad-tech functionality on certain Hisense Smart TVs).

52. Hisense knowingly and intentionally incorporated ACR Tools, such as VIDAA, into their televisions to track Plaintiffs' and Class Members' video-viewing history and other activities.

53. Hisense developed a persistent, unique identifier designed to accurately link Plaintiffs' and Class Members' video-viewing history and online activity to their individual identities.

54. Hisense knew that its unique identifier and identity graph solution were inconsistent with expectations of privacy because it had publicly stated that tracking individuals in such a manner raised privacy concerns.

55. Hisense knowingly and intentionally used its identifiers, and video-viewing data associated with it, to facilitate targeted advertisements for profit

III. JURISDICTION AND VENUE

56. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class contains more than 100 members; and minimal diversity exists because at least one Class Member is a citizen of a state different from Defendant.

57. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because this action arises under federal law, including the VPPA, 18 U.S.C. § 2710, and the ECPA, 18 U.S.C. § 2510 et seq.

58. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367, because those claims arise from the same common nucleus of operative facts as the federal claims.

59. This Court has personal jurisdiction over Defendant Hisense USA Corporation because it has purposefully availed themselves of the privilege of conducting business in California and within this District. Defendant designs, markets, distributes, and sell millions of Hisense Smart TVs to California residents through nationwide retailers (including Amazon, Best Buy, Costco, Sam's Club, Target, and Walmart) and through e-commerce channels directed at California consumers; they remotely deliver firmware, software, and over-the-air updates to Smart TVs operating in this District; and they continuously and systematically intercept, collect, transmit, and monetize data from Hisense Smart TVs located in this District. Defendant's alleged tortious and statutory violations were expressly aimed at, occurred within, and caused harm in this District.

60. Defendant designs, manufactures, markets, distributes, and sells Smart TVs throughout California, including within this District.

61. Defendant derives substantial revenue from the sale of Smart TVs in California and from the monetization of consumer data collected from those devices.

62. Defendant also directs advertising, software updates, and data collection services toward Smart TVs located in California, including those owned by Plaintiffs and members of the proposed Class.

63. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

64. Specifically, Hisense Smart TVs equipped with ACR technology were sold, installed, and used by consumers within this District.

65. The unlawful collection and transmission of viewing data described in this Complaint occurred on devices located within this District.

66. Venue is proper in the Eureka—McKinleyville Division of the Northern District of California pursuant to Civil Local Rule 3-2(d) because Plaintiff Severino resides in this Division, used the Hisense Smart TV at issue in her home located within this Division, and a substantial part of the conduct giving rise to her claims occurred within this Division.

IV. ARTICLE III STANDING

67. Each named Plaintiff has Article III standing to bring the claims asserted herein. Each Plaintiff has suffered a concrete and particularized injury-in-fact that is fairly traceable to Defendant's conduct and that is redressable by a favorable judicial decision. *See, e.g.*, *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021); *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016).

68. First, each Plaintiff has suffered an actual, concrete invasion of privacy—the kind of harm that has long been recognized as actionable both at common law and under California and federal statutory law. The interception, recording, real-time disclosure, identification, and re-distribution of an individual' in-home audiovisual viewing communications by an internet-connected Smart TV is precisely the sort of intrusion that the common-law privacy torts of

intrusion upon seclusion and public disclosure of private facts, the California Constitution's right of privacy (Art. I, § 1), the California Invasion of Privacy Act, the federal Wiretap Act, and the Video Privacy Protection Act were enacted to address. *See TransUnion*, 594 U.S. at 425 (intangible harms with "a close historical or common-law analogue" satisfy concreteness).

69. Second, each Plaintiff has suffered loss of control over "covered personal identifiers" and bulk U.S. sensitive personal data within the meaning of 28 C.F.R. Part 202, including the unauthorized export of, or facilitation of access to, that data by Hisense' Chinese parents and affiliates in violation of federal national-security law. That harm is concrete and particularized as to each Plaintiff, whose specific household-level identifiers, IP addresses, MAC addresses, advertising identifiers, and viewing-behavior data were captured by Hisense' ACR pipeline.

70. Third, each Plaintiff has suffered economic injury, including (i) the loss of the benefit of the bargain (Plaintiffs would not have purchased their Hisense Smart TVs at the prices paid, and on information and belief would have paid less or nothing at all, had Defendant disclosed the true nature, scope, and downstream uses of the ACR-derived data collection at the point of sale) and (ii) the diminution in value of, and loss of ability to control or monetize, their personal information.

71. Fourth, where applicable, each Plaintiff is entitled to statutory damages under CIPA (Cal. Penal Code § 637.2 ($5,000 per violation)), the federal Wiretap Act (18 U.S.C. § 2520(c)(2)), the VPPA (18 U.S.C. § 2710(c)(2)), and the CDAFA (Cal. Penal Code § 502(e)). Statutory-damages remedies for the intangible privacy injuries of the kind asserted here independently confer Article III standing under TransUnion and its progeny.

72. Nothing in Section 230 of the Communications Decency Act, 47 U.S.C. § 230, immunizes any of the conduct alleged here. Section 230 protects interactive computer service providers from being treated as the publishers or speakers of third-party content. Plaintiffs do not seek to hold Defendant liable as publishers or speakers of third-party content; they seek to hold Defendant liable for their own first-party conduct in designing, configuring, and operating Hisense

Smart TVs and the ACR systems embedded therein, capturing and re-distributing Plaintiffs' in-home audiovisual viewing communications and associated identifiers, and doing so without informed consent and in violation of federal and California law. The Ninth Circuit has repeatedly held that § 230 does not immunize defendants from liability for their own first-party data-collection and data-disclosure conduct.

V. HISENSE'S SMART TV BUSINESS

73. Hisense manufactures and sells Smart TVs in the United States under the Hisense Smart TV brand.

74. Hisense's Smart TVs are internet-connected devices capable of running streaming applications, connecting to external media devices, and interacting with other smart devices within a consumer's home.

75. Hisense markets these televisions as convenient, centralized platforms for accessing digital media and streaming services.

76. Hisense sells millions of Smart TVs in the United States each year and has placed such devices in millions of American households.

77. Because televisions are typically located in shared household spaces—such as living rooms and bedrooms—a single Hisense Smart TV is regularly used by multiple individuals within a household, including family members and guests.

78. As a result, each Hisense Smart TV provides Hisense with access to detailed behavioral and viewing information concerning multiple individuals within the same household.

79. This household-level surveillance allows Hisense to collect and monetize viewing data not only from the purchaser of the television, but from all individuals who use it—regardless of whether those individuals received notice of or consented to such data collection.

VI. AUTOMATIC CONTENT RECOGNITION TECHNOLOGY

80. Automatic Content Recognition (ACR) is a technology designed to identify what media content is displayed on a television.

81. ACR operates by continuously capturing portions of the audio and video output from the television and converting those fragments into unique digital "fingerprints."

82. The identified viewing data is then transmitted to remote servers, where it is aggregated, analyzed, and linked to device- and household-level identifiers.

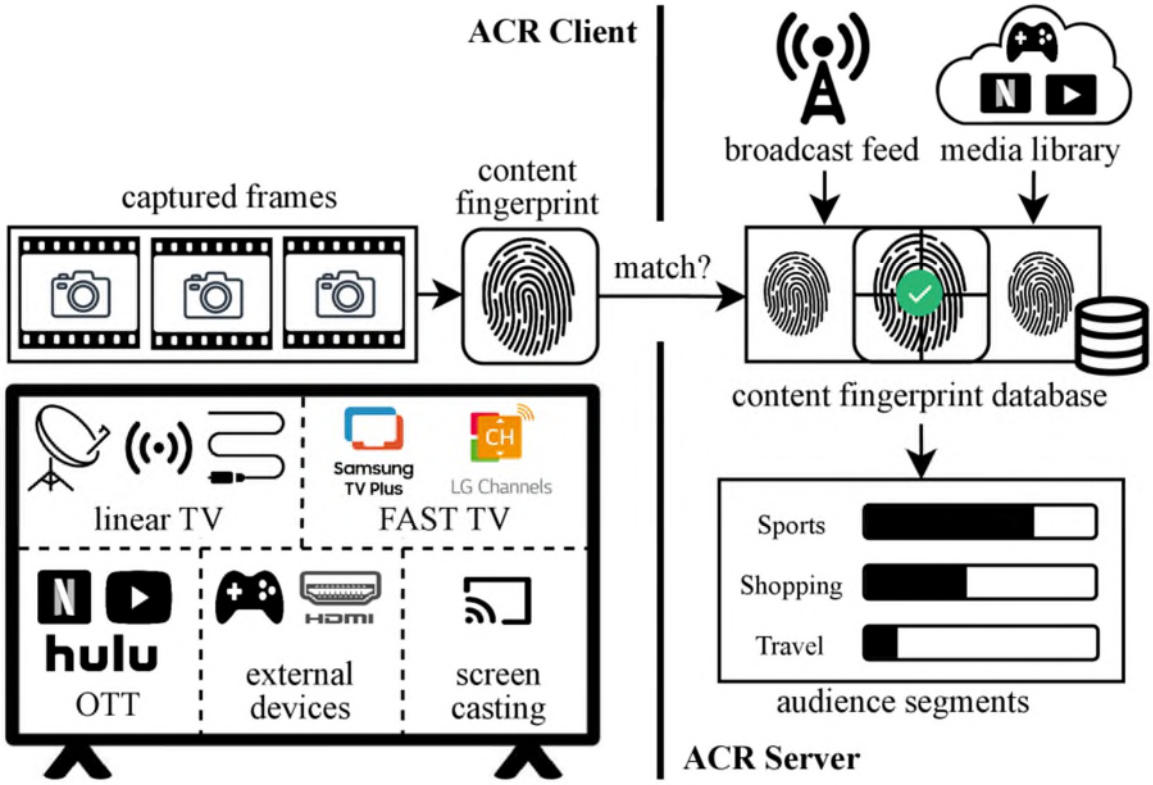

Figure 1: Overview of ACR tracking in Smart TVs

Source: Gianluca Anselmi et al., *Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs* (Sept. 10, 2024), https://arxiv.org/html/2409.06203v1.

83. Regulators have specifically recognized the intrusive nature of Hisense's ACR practices. On December 15, 2025, the Texas Attorney General filed an Original Petition and Application for Temporary and Permanent Injunctions against Hisense USA Corporation in Comal County, Texas, alleging that Hisense Smart TVs "aren't just entertainment devices—they're mass surveillance systems" and that, through ACR technology, Hisense "secretly monitors what

consumers watch across streaming apps, cable, and even connected devices like gaming consoles or Blu-ray players." Texas further explained that ACR technology works by capturing "audio and visual data of what you're watching on TV … to build a 'fingerprint' of the content" and matching it against a database to identify precisely what is viewed.[1]

84. The Texas Attorney General's petition specifically alleges that Hisense Smart TVs capture audio and video data "every 500 milliseconds—7,200 images per hour," build household-level profiles for cross-device advertising, and use deceptive labeling (such as "Enhanced Viewing Service") and dark-pattern interfaces (described in privacy literature as "Privacy Zuckering" and "Roach Motel" designs) to extract purported "consent" that is neither informed nor meaningful. Hisense's ACR opt-out controls, when they exist at all, are scattered across "four or more separate menus which require[] over 200 clicks to read through in full on the TV."

85. Within days of filing the petition, Attorney General Paxton secured what his office publicly described as a "first-of-its-kind" temporary restraining order against Hisense USA Corporation in the same action. The temporary restraining order prohibits Hisense, during the pendency of the Texas action, from (i) collecting any further ACR-derived personal data from Hisense Smart TVs in Texas, and (ii) using, selling, sharing, disclosing, or transferring any ACR-derived personal data already collected from Texas consumers. In announcing the order, the Texas Attorney General specifically described Hisense as a "CCP-aligned smart TV company" and emphasized that "[t]he Chinese Communist Party — has access to all of the ACR data collected." The temporary restraining order against Hisense thus reflects an independent governmental finding that Hisense's ACR-data collection and disclosure practices are sufficiently unlawful, deceptive, and dangerous to warrant immediate injunctive relief.[2]

---

[1] *See State of Texas v. Hisense USA Corp.*, No. 1 (Comal Cnty. Dist. Ct. filed Dec. 15, 2025) (the "Texas Petition"), available at https://www.texasattorneygeneral.gov/sites/default/files/images/press/Hisense%20TV%20Petition%20Filed.pdf.

[2] *See* Press Release, Off. of the Tex. Att'y Gen., Attorney General Ken Paxton Secures Court Order Stopping CCP-Aligned Smart TV Company from Spying on Texans, available at

86. Notably, in a separate enforcement action, Texas previously secured an agreement requiring Samsung to "promptly update its smart TVs and implement disclosures and consent screens that are clear and conspicuous to ensure that Texans can make an informed decision regarding whether their data is collected and how it's used."[3] Shortly thereafter, Texas secured a similar agreement from LG.[4]

87. Federal regulators have likewise long recognized the deceptive and unfair nature of undisclosed ACR data collection. In February 2017, the Federal Trade Commission and the New Jersey Attorney General announced a $2.2 million settlement with Vizio, Inc. arising from Vizio's collection of viewing data on approximately 11 million Vizio Smart TVs through ACR technology without consumers' informed consent. *See United States v. VIZIO, Inc*., No. 2:17-cv-00758 (D.N.J.). The FTC found that Vizio used the ACR data to build "highly specific viewing-behavior databases" and shared those databases with third parties for advertising and analytics purposes. By 2021, public reporting indicated that Vizio earned more in profit from the sale of ACR-derived viewer data than from the sale of its televisions themselves. Hisense's ACR practices are materially the same as the practices for which Vizio was sanctioned, and Hisense's business model—selling televisions at competitive prices and recouping margin through the monetization of consumer ACR data—is the same business model that the FTC and the New Jersey Attorney General determined to be unlawful and unfair.

VII. HISENSE'S ACR SURVEILLANCE PROGRAM

88. Hisense has incorporated ACR technology into its Smart TVs since at least 2019.

89. Hisense implements this functionality through its wholly-owned operating system and ACR provider, VIDAA, which is integrated directly into the Hisense Smart TV platform and

---

https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-court-order-stopping-ccp-aligned-smart-tv-company-spying-texans.

[3] https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-secures-major-agreement-samsung-ensure-texans-are-protected-smart-tvs

[4] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-major-agreement-lg-protect-texans-privacy-and-stop-data-being

which captures, transmits, and analyzes viewing activity. Hisense Smart TVs ship with one of three operating systems—the proprietary VIDAA OS, Google TV, or Roku OS—each of which is configured by Hisense to enable ACR-based monitoring and to transmit viewing data to Hisense, VIDAA, and their advertising and analytics partners.

90. Within Hisense Smart TVs, this ACR functionality is presented to consumers during device setup and in subsequent menus under benign-sounding labels such as "Enhanced Viewing Service"—a deceptive label that does not communicate that the feature operates as continuous, frame-by-frame surveillance of every sound and image displayed on the consumer's television.

91. Hisense describes this feature as providing personalization, recommendations, or enhanced viewing experiences.

92. In reality, the feature operates as a continuous surveillance mechanism that monitors and records the media displayed on the television.

93. When enabled, Hisense's ACR system continuously captures audio and video data from the television screen during ordinary use.

94. The system identifies the content being displayed and records detailed information about each viewing session.

95. This data includes, but is not limited to:

- the specific programs and videos watched;
- the advertisements viewed;
- the applications used;
- the timing and duration of viewing sessions; and
- information about devices connected to the television.

96. Hisense aggregates this data to create household-level viewing profiles.

97. These profiles are used by Hisense and its advertising partners to deliver targeted advertising across televisions and other connected devices.

VIII. HISENSE'S COLLECTION OF HIGHLY SENSITIVE VIEWING DATA

98. The viewing information captured through Hisense's ACR system is highly sensitive and revealing.

99. For example, viewing behavior can reveal information relating to:

- political preferences and affiliations;
- religious beliefs and practices;
- sexual orientation;
- health conditions and medical concerns;
- family composition, including the presence and ages of children; and
- age, socioeconomic status, and other demographic characteristics.

100. Hisense aggregates this viewing data into consumer profiles used for targeted advertising and behavioral segmentation.

101. These profiles are linked to persistent identifiers and, upon information and belief, are associated with identifiers tied to other devices belonging to the same individual or household.

102. Through this linkage, Hisense correlates viewing activity from Smart TVs with data collected from smartphones, tablets, and computers.

103. This cross-device tracking enables Hisense and its advertising partners to construct detailed identity graphs and comprehensive behavioral profiles of consumers across contexts and devices.

IX. VIDAA'S SURVEILLANCE AND IDENTITY-RESOLUTION BUSINESS

104. VIDAA is not merely a passive operating-system supplier to Hisense. It is an integrated smart-television operating system, automatic-content-recognition, and ad-tech business whose commercial model is built around capturing, identifying, matching, and monetizing television-viewing data across devices. VIDAA, USA, Inc. and its corporate affiliates develop, distribute, and operate the VIDAA OS smart-television operating system that ships pre-installed on millions of Hisense Smart TVs in the United States and globally; develop and distribute the

ACR software embedded in those devices; and operate the cloud infrastructure that receives, processes, monetizes, and re-distributes the resulting viewing data and associated identifiers.

105. Although VIDAA is corporately affiliated with Hisense, it is, on information and belief, a legally distinct corporate person from Hisense USA Corporation, with its own board, contracting authority, infrastructure, and downstream commercial relationships. VIDAA holds itself out publicly as the operator of one of the world's fastest-growing CTV operating-system platforms, with tens of millions of CTV devices powered by VIDAA OS across multiple OEM brands (including Hisense, Toshiba, and others). VIDAA enters into independent commercial agreements with ad-tech, identity-graph, and data-broker companies in its own name, including the multi-year exclusive ACR-data-access and ad-monetization agreement with Nexxen International Ltd. described below.

106. VIDAA's ACR functionality serves as the anchor of an end-to-end surveillance and identity-resolution system. The ACR software embedded in Hisense Smart TVs continuously captures information about what is displayed on the television screen—as the Texas Attorney General has alleged in its enforcement action against Hisense, capturing audio and visual data "every 500 milliseconds"—and transmits that information, along with persistent device, household, and network-level identifiers, to VIDAA-operated servers. VIDAA collects and processes this information regardless of source: native VIDAA OS streaming applications, cable and broadcast television signals, content from external HDMI-connected devices (including video-game consoles, streaming sticks, Blu-ray players, and personal computers), and content cast or mirrored to the television over Wi-Fi.

107. In connection with this viewing data, VIDAA collects and receives multiple categories of identifying signals, including IP addresses, MAC addresses and other device-based identifiers, advertising identifiers, application-level identifiers, household identifiers, timestamps of viewing activity, location and network information, device type, make, and model, and operating-system information. These identifiers are transmitted together with viewing data,

allowing VIDAA to associate specific viewing activity with particular devices, households, and network environments.

108. VIDAA applies both deterministic and probabilistic matching techniques to these signals in order to determine which devices belong to the same household or individual. These techniques include comparing shared IP-address patterns, correlating device activity over time, and reconciling identifiers obtained from televisions, mobile applications, third-party data partners, and identity-resolution providers. Through this process, VIDAA is able to infer relationships between Hisense Smart TVs and other devices—including smartphones, tablets, and computers—used within the same household or by the same user.

109. VIDAA's business model is to collect viewing data from televisions, combine that data with persistent identifiers and partner data, and transform it into advertising products, audience segments, and measurement outputs sold or licensed to brands, agencies, ad-tech intermediaries, identity-resolution providers, and other market participants. VIDAA's commercial relationships demonstrate the depth of this business: pursuant to a multi-year strategic partnership most recently renewed and expanded in August 2025, VIDAA has granted Nexxen International Ltd. exclusive global access to VIDAA's ACR data and exclusive rights to monetize CTV and native display advertising on VIDAA media in North America through at least the end of 2029, in exchange for an aggregate equity investment by Nexxen of approximately $60 million.

110. Through that partnership, the ACR data collected by VIDAA from approximately 1.2 million or more VIDAA-operated Hisense Smart TVs in the United States is curated by Nexxen into proprietary "TV retargeting segments" and used by Nexxen to power advanced audience targeting, insights, and measurement capabilities across the United States, Canada, the United Kingdom, Australia, and Germany. The arrangement reflects the core commercial function of VIDAA's business: taking television-derived viewing data and turning it into matched household audiences, cross-device advertising targets, identity-graph nodes, and attribution products that can be used across the digital advertising ecosystem.

111. Hisense Smart TVs fit directly into that apparatus. Hisense's manufacture, sale, configuration, software-updating, and ongoing operational support of those devices is the indispensable input layer for VIDAA's larger surveillance and identity-resolution system. Through Hisense televisions placed in consumers' living rooms and bedrooms, VIDAA is able to obtain granular viewing data from the "first screen" in the home, associate that data with device and household identifiers, and then deploy the resulting identity graph to support audience construction, targeting, retargeting, attribution, and cross-device advertising products that reach far beyond the television itself.

112. VIDAA's role in the Hisense ecosystem is therefore central, not incidental. Hisense designs, configures, sells, and remotely supports the Smart TVs that capture viewing activity; VIDAA receives or directs the receipt of content-derived data and associated identifiers; VIDAA then matches, links, and aggregates this data into unified profiles, enriches those profiles with partner data, and deploys the resulting identity graph to power audience segmentation, cross-device targeting, retargeting, and attribution systems that extend across connected televisions, mobile devices, computers, and other digital platforms—and ultimately, on information and belief, into the hands of Hisense's Chinese parents and affiliates, as alleged in the China-data-transfer section that follows.

X. HISENSE'S AND VIDAA'S INTEGRATED SURVEILLANCE ARCHITECTURE

113. Hisense's Smart TVs and VIDAA's data-processing systems operate together as an integrated surveillance and advertising architecture designed to capture, identify, and monetize consumers' in-home viewing activity.

114. Upon receipt, VIDAA matches these fingerprints to identify viewed content and associates that information with device- and household-level identifiers. In doing so, VIDAA correlates content-derived signals with persistent identifiers such as IP address, MAC address, advertising identifiers, and a VIDAA-issued unique household identifier, enabling it to link specific viewing activity to particular devices, households, and network environments. These transmissions include content-derived information sufficient to identify the specific programs,

advertisements, or audiovisual material viewed, thereby conveying the substance of Plaintiffs' and Class Members' video-viewing activity to VIDAA in real time or near-real time.

115. VIDAA integrates this viewing data into broader identity-resolution systems that link Hisense Smart TVs to other devices associated with the same household or user, including smartphones, tablets, and computers. These systems use deterministic and probabilistic matching techniques to associate identifiers observed from the Smart TV with identifiers obtained from other devices and data sources, including identifiers obtained from third-party identity-resolution providers (such as LiveRamp), demand-side and supply-side platforms, and Nexxen's identity and audience-resolution infrastructure.

116. Through these systems, Defendant and the third-party recipients create cross-device identity graphs that connect in-home television viewing activity with digital activity occurring on other devices and platforms, forming unified profiles that persist over time and are updated as additional data is collected. This process results in the assignment or maintenance of persistent identifiers—whether internally defined or derived from combined signals—that function as stable reference points for tracking a household or user across devices and over time.

117. The Hisense Smart TV serves as a primary data-collection endpoint—and the anchor of the system's identity-resolution architecture—capturing viewing activity from the "first screen" in the home, while VIDAA functions as a central processing and monetization layer that transforms that data into actionable advertising products. In sequence, Defendant and its third-party ACR partners (1) capture viewing data on the device, (2) convert it into identifiable signals, (3) transmit those signals to VIDAA in real time or near-real time, (4) match them to known content, (5) associate them with persistent identifiers, (6) incorporate them into identity graphs used for advertising and analytics, and (7) re-distribute the resulting datasets to Nexxen, Roku, Alphonso, and other downstream ad-tech, identity-graph, data-broker, and measurement partners as alleged herein.

118. Recent academic forensics support the existence and operational behavior of these data flows. In a 2024 ACM Internet Measurement Conference paper, researchers from University

College London, the University of California, Davis, and Universidad Carlos III de Madrid documented that ACR-enabled Smart TVs continuously capture content displayed on the screen, generate fingerprints, and transmit those fingerprints to ACR-vendor-controlled domains (e.g., "eu-acrX.alphonso.tv" and "tkacrX.alphonso.tv" for Alphonso-integrated devices in the LG ecosystem). The researchers further found ACR transmissions occurred even when the Smart TV was used as a "dumb" HDMI display for laptops, gaming consoles, and other personal devices. *See* Gianluca Anselmi et al., Watching TV with the Second-Party: A First Look at Automatic Content Recognition Tracking in Smart TVs (Sept. 10, 2024), https://arxiv.org/html/2409.06203v1. On information and belief, Hisense Smart TVs transmit ACR fingerprints and associated identifiers to materially identical VIDAA-, Nexxen-, Roku-, Amazon-, and Alphonso-controlled server endpoints in real time and near-real time during use; Plaintiffs reserve the right to identify the specific endpoints in discovery.

XI. HISENSE'S CORPORATE TIES TO THE PEOPLE'S REPUBLIC OF CHINA AND UNDISCLOSED DATA-TRANSFER OBLIGATIONS

119. Hisense's ACR surveillance is not merely a domestic privacy problem. Hisense is, at its corporate core, a Chinese state-owned enterprise under the control of the Qingdao municipal government in the People's Republic of China ("PRC").

120. The ultimate parent of Defendant is Hisense Group Holdings Co., Ltd., a state-owned holding company headquartered in Qingdao, China, whose shares are held, directly and indirectly, by Chinese government entities. Hisense Group has received billions of dollars in PRC government subsidies to support its global expansion in the consumer-electronics market.

121. Under Article 7 of the PRC National Intelligence Law (effective 2017, as amended in 2018), "[a]ny organization or citizen shall support, assist, and cooperate with state intelligence work" in accordance with Chinese law, and shall "protect the secrets of the national intelligence work known to the public." In practical effect, Hisense and its corporate parents and affiliates can be compelled to turn over any data they hold—including data collected from Hisense Smart TVs in the United States—to the Chinese government and the Chinese Communist Party on demand.

122. Hisense itself acknowledges, in its End User Terms and Conditions, that it "may transfer" its users' personal information to the People's Republic of China.

123. Nowhere, however, does Hisense disclose to consumers in California—or elsewhere in the United States—that, as a matter of Chinese law, Hisense is obligated to share data collected from American consumers, including data harvested through ACR surveillance, with the Chinese government and the CCP upon request.

124. Nor does Hisense disclose that every image and sound captured by ACR on a Hisense Smart TV—whether the consumer is watching a streaming service, a cable broadcast, a video-game console, or content from a personal computer or phone connected via HDMI, AirPlay, or Google Cast—may be collected, stored, and ultimately transferred to the PRC.

125. The combination of (i) Hisense's continuous, frame-by-frame ACR capture of audiovisual content within the home, (ii) Hisense's aggregation of that data with persistent and cross-device identifiers, (iii) Hisense's status as a Chinese state-owned enterprise, and (iv) Hisense's express acknowledgment that user data "may transfer" to the PRC, exposes Plaintiffs and Class Members to a foreseeable, material, and undisclosed risk that the most intimate details of their viewing habits and household life will be made available to a foreign government.

126. Reasonable consumers, including Plaintiffs, would consider it material to their decision to purchase or use a Hisense Smart TV that the device's manufacturer is a Chinese state-owned enterprise legally obligated to share their viewing data with a foreign government on demand. Had Plaintiffs known these facts, they would not have purchased the Hisense Smart TV, or would have paid substantially less for it.

127. Hisense's knowing failure to disclose its data-transfer obligations to the PRC is independently deceptive and unfair under California law, including under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, and related common-law doctrines pleaded herein.

XII. DEFENDANT'S VIOLATIONS OF THE U.S. BULK SENSITIVE DATA TRANSFER RULE

128. This case sits at the intersection of consumer-privacy law, ad-tech surveillance, and federal national-security regulation. On April 8, 2025, the U.S. Department of Justice's Data Security Program—codified at 28 C.F.R. Part 202 and known as the "Rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (the "Bulk Sensitive Data Transfer Rule" or the "DOJ Rule")—took effect. The DOJ Rule was promulgated pursuant to Executive Order 14117 to address what the United States government has formally determined to be an "unusual and extraordinary threat" to U.S. national security: the bulk export of Americans' behavioral data to hostile foreign regimes and entities under their jurisdiction.

129. The DOJ Rule prohibits U.S. persons from knowingly engaging in "covered data transactions" involving "data brokerage" with any "country of concern" or "covered person." 28 C.F.R. § 202.301. The DOJ Rule further restricts U.S. persons from engaging in covered data transactions involving vendor, employment, or investment agreements with any country of concern or covered person unless the U.S. person complies with the Cybersecurity and Infrastructure Security Agency ("CISA") Security Requirements for Restricted Transactions issued under Executive Order 14117. Id. § 202.401; § 202.248.

130. "Bulk U.S. sensitive personal data" means a collection of sensitive personal data on more than 100,000 U.S. persons in any 12-month window. 28 C.F.R. §§ 202.205, 202.206, 202.212. "Listed identifier" expressly includes device-based and hardware-based identifiers (IMEI, MAC address, SIM); advertising identifiers (Google Advertising ID, Apple ID for Advertisers, MAID); and network-based identifiers (IP address, cookie data). Id. § 202.234. "Covered personal identifiers" means any listed identifier combined with another listed identifier or with other data linkable to listed identifiers. Id. § 202.212.

131. The Hisense ACR data at issue in this Complaint—including, in real time and in combination with each other, IP addresses, MAC addresses and other device-level identifiers,

advertising identifiers, cookie data, household identifiers, cross-device identifiers, and granular records of consumers' viewing behavior—falls squarely within the DOJ Rule's definition of "covered personal identifiers" and, given the millions of U.S. households whose Hisense Smart TVs feed Defendant's ACR pipeline, plainly meets the "bulk" threshold under 28 C.F.R. § 202.205.

132. The "bulk" threshold under the DOJ Rule (data collected about or maintained on more than 100,000 U.S. persons in any 12-month window, 28 C.F.R. § 202.205) is met by orders of magnitude here. Hisense holds, on information and belief, approximately 6% of the U.S. Smart TV installed base. Hisense ranked No. 2 globally in TV shipments in 2022 and shipped more than 29.14 million televisions worldwide in 2024 (a 14% global market share). Public reporting indicates that approximately 68% of U.S. households now own a Smart TV, and that Hisense's share of those households translates to multiple millions of U.S. households running Hisense Smart TVs at any given time. The Texas Attorney General has alleged that approximately 470,000 Texas households alone own Hisense Smart TVs, equivalent to nearly 1.27 million Texans (assuming a 2.7-person average household)—in a single state. Hisense's ACR pipeline therefore captures and transmits covered personal identifiers about, at a minimum, multiple millions of U.S. persons in any 12-month period, multiples above the DOJ Rule's 100,000-person bulk threshold. By any reasonable measure, the data Hisense's ACR system collects and disseminates is bulk U.S. sensitive personal data within the meaning of 28 C.F.R. § 202.206.

133. Defendant Hisense USA Corporation is a "U.S. person" under the DOJ Rule because it is "an[] entity organized solely under the laws of the United States or any jurisdiction within the United States." 28 C.F.R. § 202.256.

134. Hisense's ultimate corporate parents and affiliates—including Hisense Group Holdings Co., Ltd. and Hisense Co., Ltd., each headquartered in Qingdao, People's Republic of China and majority-owned and controlled, directly and indirectly, by the Qingdao municipal government and other Chinese state-owned entities—are each "covered persons" under the DOJ

Rule because each is a foreign entity organized under the laws of, and with its principal place of business in, the People's Republic of China. 28 C.F.R. § 202.211.

135. Hisense's own End User Terms and Conditions—specifically the End User Terms and Conditions effective February 1, 2019 and the End User License Agreement effective April 30, 2023—expressly admit that Hisense's collection of users' personal information "may transfer" that information to the People's Republic of China. That admission is dispositive: Hisense's own statements confirm that the very ACR-derived data at issue in this Complaint flows, or may flow, to a country of concern under the DOJ Rule. As a matter of Chinese law—including Article 7 of the PRC National Intelligence Law, the PRC Cybersecurity Law, and the PRC Data Security Law—Hisense's Chinese parents and affiliates can be compelled to grant the Chinese government and the Chinese Communist Party access to any data they hold, including ACR data harvested from American households.

136. Hisense USA does not, and cannot, demonstrate compliance with the CISA Security Requirements for Restricted Transactions under Executive Order 14117 with respect to the ACR data it permits to be transferred to, or accessed by, its Chinese parents and affiliates. Hisense USA does not implement the required organizational cybersecurity policies, logical and physical access controls, risk-assessment and mitigation strategies, data-minimization or data-masking protocols, or encryption requirements designed to prevent covered persons or countries of concern from gaining access to covered data.

137. Defendant's conduct therefore constitutes both (i) a Prohibited Data Transaction under 28 C.F.R. § 202.301 (data brokerage with a country of concern or covered person) and/or (ii) a Restricted Data Transaction under 28 C.F.R. § 202.401 (vendor, employment, or investment-agreement transfers without the requisite CISA security requirements). On information and belief, Defendant knowingly engaged in this conduct on and after the April 8, 2025 effective date of the DOJ Rule.

138. Willful violations of the DOJ Rule are punishable as criminal offenses. The DOJ Rule is promulgated under the International Emergency Economic Powers Act ("IEEPA"), 50

U.S.C. § 1701 et seq., which provides that any person who "willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act" under IEEPA "shall, upon conviction, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both." 50 U.S.C. § 1705(c). Hisense's knowing transfer of, or knowing facilitation of access to, bulk U.S. sensitive personal data by its Chinese parents and affiliates constitutes a willful violation of the DOJ Rule and therefore a criminal offense under federal law.

XIII. HISENSE'S REAL-TIME AND NEAR-REAL-TIME DISCLOSURE OF ACR DATA TO VIDAA, NEXXEN, ROKU, ALPHONSO, AND OTHER DOWNSTREAM AD-TECH PARTNERS

139. VIDAA. VIDAA, USA, Inc. and its corporate affiliates (collectively, "VIDAA") operate the VIDAA smart-TV operating system embedded in Hisense Smart TVs. VIDAA is the primary technical conduit for Hisense's ACR data collection: it captures the ACR fingerprints from the screen, transmits them to remote servers in real time, and integrates them with persistent device, household, and cross-device identifiers (including a VIDAA-issued unique ID) to construct household-level viewing profiles. Although VIDAA is corporately affiliated with Hisense, it is, on information and belief, a legally distinct corporate person from Hisense USA Corporation, with its own board, contracting authority, infrastructure, and downstream commercial relationships, such that Hisense's causing, aiding, agreeing with, employing, and conspiring with VIDAA to capture, intercept, and transmit consumers' communications constitutes the aiding of a third party for purposes of CIPA § 631(a) and the federal Wiretap Act.

140. Nexxen. Nexxen International Ltd. and its U.S. operating affiliates (collectively, "Nexxen") are publicly traded ad-tech companies operating an end-to-end programmatic advertising platform. On information and belief, pursuant to a multi-year strategic partnership with VIDAA originally announced in 2024 and renewed and expanded in August 2025, Nexxen has been granted (i) exclusive global access to VIDAA's ACR data and (ii) exclusive rights to monetize CTV and native display advertising on VIDAA media in North America through at least

the end of 2029, in exchange for an aggregate equity investment of approximately $60 million. The exclusive ACR data Nexxen receives includes data sourced from approximately 1.2 million or more VIDAA-operated Hisense Smart TVs in the United States, which Nexxen curates into proprietary "TV retargeting segments" and uses to power audience targeting, insights, and measurement across the United States, Canada, the United Kingdom, Australia, and Germany.

141. Roku. Hisense's portfolio includes Hisense Smart TVs configured with Roku's Roku OS operating system (commonly marketed as "Hisense Roku TVs"). On information and belief, Roku, Inc. (a Delaware corporation headquartered in San Jose, California) (hereinafter, "Roku") operates its own ACR pipeline on Hisense Roku TVs in real time, and uses the resulting data to power its OneView ad-buying platform (which integrates the dataxu identity-and-attribution capabilities Roku acquired in November 2019); to operate Roku's proprietary identity and device graph (which Roku publicly states covers approximately four out of five U.S. households); and to enable cross-device addressable advertising, audience targeting, measurement, and attribution. Roku has publicly described its ACR-driven dataset as providing "real time, accurate aggregate insights into what viewers are watching" and as covering "one half of all smart TVs ad impressions."

142. Roku's receipt and use of ACR data from Hisense Roku TVs makes Roku a separate, third-party recipient of consumers' viewing communications, distinct from Hisense USA Corporation. Hisense's manufacture, sale, configuration, software updates, and ongoing operational support of Hisense Roku TVs—which it knows are designed to enable Roku's real-time interception, capture, and use of consumers' viewing communications—constitute aiding, agreeing with, employing, and conspiring with Roku to do so within the meaning of CIPA § 631(a) and the federal Wiretap Act.

143. Alphonso. Hisense USA has, since at least 2019, integrated ACR technology supplied by Alphonso, Inc. (now operating as part of LG Ad Solutions following its 2020 acquisition by LG Electronics) (collectively, "Alphonso") into certain Hisense Smart TVs. Hisense's integration of Alphonso's ACR technology was specifically alleged in the December

15, 2025 Original Petition filed by the Texas Attorney General against Hisense USA Corporation in Comal County, Texas. Alphonso has publicly described its TV-audience footprint as including ACR data from smart TVs and connected-TV devices in more than 15 million opted-in U.S. households, across brands including Hisense. As with VIDAA, Nexxen, and Roku, Alphonso receives, processes, and uses Hisense ACR data in real time or near-real time, and is a separate corporate person whose interception of consumers' viewing communications Hisense aids, agrees with, employs, and conspires with within the meaning of CIPA § 631(a) and the federal Wiretap Act.

144. Amazon (Fire TV). Hisense's portfolio also includes Hisense Smart TVs configured with Amazon's Fire TV smart-TV operating system (commonly marketed as "Hisense Fire TVs" or "Hisense Fire TV Edition" televisions, including the U6HF (2022); the U6K, U7K, and U8K Fire TV (2023); and the QD6, QD7, U6 Fire, U7 Fire, U8 Fire, and QD65NF series (2024–2025)). On information and belief, Amazon.com Services LLC, Amazon Advertising LLC, and their corporate affiliates (collectively, "Amazon", a Delaware-incorporated business with its principal place of business in Seattle, Washington) operate Amazon's own ACR pipeline on Hisense Fire TVs in real time and use the resulting data to power Amazon's DSP, Amazon Publisher Services, Amazon Marketing Cloud, the Twitch advertising network, and Amazon's proprietary identity and household-level device graph for cross-device addressable advertising, audience targeting, measurement, and attribution.

145. Amazon's receipt and use of ACR data from Hisense Fire TVs makes Amazon a separate, third-party recipient of consumers' viewing communications, distinct from Hisense USA Corporation. Hisense's manufacture, sale, configuration, software updates, and ongoing operational support of Hisense Fire TVs—which Hisense knows are designed to enable Amazon's real-time interception, capture, and use of consumers' viewing communications—constitutes aiding, agreeing with, employing, and conspiring with Amazon to do so within the meaning of CIPA § 631(a) and the federal Wiretap Act. Plaintiff Cohen owns a 65" Class QD65 Series QLED

4K UHD Smart Fire TV (model 65QD65NF) and is, accordingly, a member of the Hisense-Fire-TV Class of consumers whose Hisense Smart TVs feed Amazon's ACR pipeline.

146. Other ad-tech, data-broker, identity-resolution, and measurement partners. On information and belief, Hisense's and VIDAA's ACR data is further disclosed, sold, licensed, or otherwise made available to additional downstream identity-resolution providers (such as LiveRamp Holdings, Inc.), measurement and attribution providers (such as The Nielsen Company), demand-side and supply-side platforms (such as The Trade Desk, Inc.), real-time bidding exchanges, and other ad-tech ecosystem participants. Plaintiffs reserve the right to identify additional third-party recipients in discovery.

XIV. HISENSE'S MARKETING AND REPRESENTATIONS REGARDING SMART TV FUNCTIONALITY AND PRIVACY

145. Hisense markets its Smart TVs as premium entertainment devices designed to provide consumers with seamless access to content and a personalized viewing experience.

146. In its marketing materials and user-facing disclosures, Hisense represents that features such as "Enhanced Viewing Service" or "personalized recommendations" enhance the user experience by tailoring content suggestions to the viewer.

147. Hisense promotes these features as tools that help users "discover content," "enhance viewing," and "personalize" their entertainment experience.

148. These representations convey to reasonable consumers that any data collection associated with such features is limited, user-beneficial, and tied to improving on-screen recommendations.

149. Hisense does not disclose in its marketing materials that these features function by continuously capturing and analyzing the audio and video displayed on the television screen, including content viewed through third-party applications and external devices.

150. Nor does Hisense disclose that this viewing data is transmitted to third parties, including advertising and data analytics companies, for purposes unrelated to providing core television functionality.

151. Hisense further fails to disclose that the data collected through ACR is used to construct cross-device identity profiles and to facilitate targeted advertising across multiple devices and platforms.

152. To the extent Hisense provides disclosures regarding data collection, such disclosures are incomplete, obscured, and presented, if at all, during initial device setup—often to a different individual than the end users of the television.

153. Hisense's marketing and disclosures omit material facts necessary to prevent its representations regarding personalization and user control from being misleading.

154. Reasonable consumers, including Plaintiffs, would not expect that simply watching television in their homes would result in the continuous interception, analysis, and disclosure of their viewing activity and associated identifiers to third parties.

155. Had Plaintiffs known the true nature and scope of Hisense's data collection and sharing practices, they would not have purchased the Hisense Smart TV or would have paid substantially less for it.

XV. HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN.

156. Hisense does not meaningfully disclose its ACR surveillance practices to consumers.

157. Instead, Hisense presents the ACR feature during the television setup process using misleading terminology and opaque disclosures.

158. For example, Hisense labels the ACR feature "Enhanced Viewing Service" or "Enhanced Viewing Service," terminology that does not convey that the feature enables continuous monitoring of television viewing.

159. During the setup process, consumers are required to navigate through multiple screens containing dense legal text before reaching the screen Hisense characterizes as a consent screen.

160. Most consumers click through the setup screen-flow simply to complete the setup process and begin using the television.

161. Hisense intentionally presents its privacy policies during the initial setup process when consumers are most eager to begin using their new televisions.

162. Hisense's disclosures fail to explain that enabling the feature allows Hisense to continuously capture and analyze the audio and video displayed on the television screen.

163. Hisense also fails to disclose that the resulting viewing data will be used to create advertising profiles or identity graphs and shared with advertising partners.

164. Even after setup, consumers who wish to disable the surveillance feature must navigate through multiple menus and obscure settings to locate the opt-out controls.

165. This design—easy opt-in combined with difficult opt-out—is a well-known manipulative interface technique commonly referred to as a "dark pattern."

166. As a result, millions of consumers have unknowingly enabled Hisense's ACR surveillance.

XVI. HISENSE PROFITS FROM ITS SURVEILLANCE OF CONSUMERS.

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

167. The viewing data collected through Hisense's ACR system is highly valuable in the digital advertising marketplace.

168. By collecting, analyzing, and monetizing this data, Hisense generates significant revenue through advertising, audience segmentation, and analytics services.

169. The data collected through Hisense's ACR Tools is used to build household-level and cross-device identity profiles, which are then leveraged to enable targeted advertising across televisions, mobile devices, and computers.

170. These practices allow Hisense and its partners to deliver highly targeted advertisements, measure advertising effectiveness, and sell access to valuable audience segments.

171. As a direct result of its surreptitious collection, use, and disclosure of Plaintiffs' and Class Members' Sensitive Information, Hisense has generated, and continues to generate, substantial revenue attributable to its data-driven advertising and analytics operations.

172. Through these practices, Hisense has been unjustly enriched at the expense of Plaintiffs and Class Members, whose private viewing information was collected and monetized without their knowledge or informed consent.

B. Plaintiffs' and Class Members' Data Had Independent Financial Value.

173. Plaintiffs' and Class Members' Sensitive Information has independent economic value in the marketplace for consumer data.

174. Industry data confirms that consumer data has substantial and increasing per-user value, as reflected in growing revenues from targeted advertising and the existence of programs in which companies compensate consumers in exchange for access to their behavioral data, demonstrating that such information is a recognized and tradable asset.

175. 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."[5]

176. 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.

177. Companies routinely pay for access to user-level behavioral data, including browsing activity, viewing habits, and device-level identifiers, because such data enables precise targeting and profiling. For example, several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and

[5] 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).

SavvyConnect are all companies that pay for browsing history information.

178. By contrast, Hisense obtained Plaintiffs' and Class Members' Sensitive Information without compensation and without informed consent, while retaining the full economic benefit of that data.

179. The unauthorized interception and disclosure of Plaintiffs' and Class Members' Sensitive Information diminished the value of that information and deprived them of the ability to control, license, or otherwise monetize their own data.

180. As a result, Plaintiffs and Class Members have suffered economic harm.

XVII. HISENSE'S USE OF THE ACR TOOLS VIOLATES NUMEROUS STATE AND FEDERAL DATA PRIVACY LAWS

A. The Video Privacy Protection Act (VPPA)

181. The VPPA was enacted 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).

182. Congress was particularly concerned with the privacy of individuals' 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).

183. Although originally enacted in the context of videotape rentals, Congress has made clear that the VPPA applies to modern technologies, including "'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.[6]

[6] *See also The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

184. The VPPA prohibits a "video tape service provider" 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." 18 U.S.C. § 2710(b).

185. The statute defines a "video tape service provider" as any person "engaged in the business… of rental, sale, or delivery of… similar audio visual materials." 18 U.S.C. § 2710(a)(4).

186. It further defines "personally identifiable information" ("PII") as information that identifies a person as having requested or obtained specific video materials or services. 18 U.S.C. § 2710(a)(3).

187. Hisense is a "video tape service provider" within the meaning of the VPPA because it is engaged in the business of delivering video content to consumers, including through its Smart TV platform, which provides access to on-demand streaming services and Hisense's own video content offerings, including Hisense TV Plus.

188. As alleged herein, Hisense, through its ACR Tools, knowingly intercepts and discloses consumers' video-viewing activity—including the specific programs and content viewed—along with persistent identifiers such as IP addresses, device identifiers, and other data that enable those viewing selections to be associated with a particular individual or household.

189. These disclosures constitute the disclosure of "personally identifiable information" under the VPPA because they identify consumers as having requested or obtained specific video materials or services.

190. Hisense makes these disclosures to third parties, including advertising and

---

(Jan. 31, 2012), *available online at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-videoprivacy-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.").

analytics partners, for commercial purposes, including targeted advertising, audience segmentation, and measurement.

191. Hisense does so without obtaining consumers' informed, written consent in a form that is distinct and separate from other terms, and, in many cases, without providing any disclosure to the actual users of the television whose viewing activity is collected and disclosed.

192. Courts have recognized that the VPPA applies to modern streaming technologies and evolving forms of audiovisual content delivery. *See, e.g., 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").

B. The Federal Trade Commission Act ("FTC Act")

193. Hisense represents its Smart TVs and associated features, including "Enhanced Viewing Service" and similar functionality, as tools designed to enhance the user experience through personalization and content recommendations.

194. These representations are materially misleading because Hisense fails to disclose that these features operate by continuously capturing and analyzing the audio and video displayed on consumers' television screens, including content viewed through third-party applications and external devices.

195. Hisense further fails to disclose that this viewing data is transmitted to third parties, including advertising and analytics partners, and used to construct cross-device identity profiles for targeted advertising and other commercial purposes.

XVIII. CLASS ALLEGATIONS

196. This action is brought by the named Plaintiffs both individually, and on behalf of the following Classes and Subclasses under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4):

Nationwide ACR Class: All natural persons in the United States who, during the Class Period, used a Hisense Smart TV on which ACR technology was enabled and that captured, analyzed, or transmitted information regarding audiovisual content displayed on the device.

California ACR Subclass: All natural persons in California who, during the Class Period, used a Hisense Smart TV on which ACR technology was enabled and that captured, analyzed, or transmitted information regarding audiovisual content displayed on the device.

Nationwide VIDAA Identity Graph Class: All natural persons in the United States whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or VIDAA, USA, Inc., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, and identity-graph systems operated by VIDAA in connection with the VIDAA OS smart-television operating system embedded in Hisense Smart TVs, including but not limited to the identity- and audience-resolution products and segments licensed by VIDAA to Nexxen International Ltd. and other downstream ad-tech partners.

California VIDAA Identity Graph Subclass: All natural persons in California whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or VIDAA, USA, Inc., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, and identity-graph systems operated by VIDAA in connection with the VIDAA OS smart-television operating system embedded in Hisense Smart TVs, including but not limited to the identity- and audience-resolution products and segments licensed by VIDAA to Nexxen International Ltd. and other downstream ad-tech partners.

Nationwide Nexxen Identity Graph Class: All natural persons in the United States whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Nexxen International Ltd., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-resolution, and "TV retargeting

segment" systems operated by Nexxen using ACR data and associated identifiers obtained from Hisense Smart TVs (including, on information and belief, pursuant to Nexxen's exclusive global ACR-data-access and ad-monetization agreement with VIDAA).

California Nexxen Identity Graph Subclass: All natural persons in California whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Nexxen International Ltd., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-resolution, and "TV retargeting segment" systems operated by Nexxen using ACR data and associated identifiers obtained from Hisense Smart TVs (including, on information and belief, pursuant to Nexxen's exclusive global ACR-data-access and ad-monetization agreement with VIDAA).

Nationwide Roku Identity Graph Class: All natural persons in the United States whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Roku, Inc., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-graph, and OneView/dataxu identity-resolution systems operated by Roku using ACR data and associated identifiers obtained from Hisense Smart TVs configured with the Roku OS operating system (commonly marketed as "Hisense Roku TVs").

California Roku Identity Graph Subclass: All natural persons in California whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Roku, Inc., directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-graph, and OneView/dataxu identity-resolution systems operated by Roku using ACR data and associated identifiers obtained from Hisense Smart TVs configured with the Roku OS operating system (commonly marketed as "Hisense Roku TVs").

Nationwide Alphonso Identity Graph Class: All natural persons in the United States whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Alphonso,

Inc. (now operating as part of LG Ad Solutions following its 2020 acquisition by LG Electronics), directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, and identity-graph systems operated by Alphonso/LG Ad Solutions using ACR data and associated identifiers obtained from Hisense Smart TVs into which Alphonso ACR technology has been integrated (since at least February 1, 2019).

California Alphonso Identity Graph Subclass: All natural persons in California whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Alphonso, Inc. (now operating as part of LG Ad Solutions following its 2020 acquisition by LG Electronics), directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, and identity-graph systems operated by Alphonso/LG Ad Solutions using ACR data and associated identifiers obtained from Hisense Smart TVs into which Alphonso ACR technology has been integrated (since at least February 1, 2019).

Nationwide Amazon Identity Graph Class: All natural persons in the United States whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Amazon.com Services LLC, Amazon Advertising LLC, or their corporate affiliates (collectively, "Amazon"), directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-graph, and Amazon DSP / Twitch / Amazon Publisher Services / Amazon Marketing Cloud advertising-resolution systems operated by Amazon using ACR data and associated identifiers obtained from Hisense Smart TVs configured with the Amazon Fire TV operating system (commonly marketed as "Hisense Fire TVs").

California Amazon Identity Graph Subclass: All natural persons in California whose viewing activity on a Hisense Smart TV was used by Defendant Hisense and/or Amazon.com Services LLC, Amazon Advertising LLC, or their corporate affiliates (collectively, "Amazon"),

directly or through their respective partners, to associate that television with one or more other devices, identifiers, or datasets as part of the cross-device or household-level identification, matching, audience-segmentation, identity-graph, and Amazon DSP / Twitch / Amazon Publisher Services / Amazon Marketing Cloud advertising-resolution systems operated by Amazon using ACR data and associated identifiers obtained from Hisense Smart TVs configured with the Amazon Fire TV operating system (commonly marketed as "Hisense Fire TVs").

197. The Nationwide ACR Class and the five Nationwide Identity Graph Classes (the Nationwide VIDAA, Nexxen, Roku, Alphonso, and Amazon Identity Graph Classes) are collectively referred to as the "Nationwide Classes." The California ACR Subclass and the five California Identity Graph Subclasses (the California VIDAA, Nexxen, Roku, Alphonso, and Amazon Identity Graph Subclasses) are collectively referred to as the "California Subclasses." The Nationwide Classes and the California Subclasses are collectively referred to herein as the "Class." The five company-specific Identity Graph Classes and Subclasses are not mutually exclusive, as a given Class Member's ACR-derived viewing data may have been received, processed, and incorporated into more than one of the five identity-graph systems.

198. 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 any Defendant has a controlling interest, as well as their 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.

199. Plaintiffs reserve the right to amend the definitions of the Class or add or refine Subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified, including based on the identification of additional ACR providers, identity-graph operators, or other downstream recipients of Hisense ACR data in discovery.

200. **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.

201. **Commonality.** Common questions of law and fact arise from Defendant's uniform conduct and are capable of classwide resolution. These common questions predominate over any questions affecting only individual Class Members and include, without limitation:

a) Whether Defendant's ACR-enabled collection, interception, and disclosure of Sensitive Information occurred in a substantially similar manner for all Class Members;

b) Whether Defendant collected, transmitted, and disclosed Class Members' Sensitive Information—including video-viewing activity and associated identifiers—to third parties without adequate notice or consent;

c) Whether Defendant's disclosures, if any, regarding its data collection and sharing practices were misleading, incomplete, or insufficient to obtain informed consent;

d) Whether Defendant and its partners used persistent identifiers to link Class Members' viewing activity across devices and to create cross-device identity profiles;

e) Whether Defendant had a duty to refrain from collecting, intercepting, or disclosing Class Members' Sensitive Information without authorization;

f) Whether Defendant's conduct constitutes an unlawful interception, disclosure, or use of Sensitive Information under the statutes asserted herein, including but not limited to the Video Privacy Protection Act;

g) Whether the information disclosed by Defendant constitutes "personally identifiable information" or otherwise protected information under applicable law;

h) Whether Defendant's conduct was unfair, unlawful, or deceptive;

i) Whether Defendant was unjustly enriched by its collection and monetization of Class Members' Sensitive Information;

j) Whether Class Members suffered injury, including invasion of privacy and loss of control over their Sensitive Information, as a result of Defendant's conduct;

k) Whether Defendant's conduct entitles Plaintiffs and Class Members to

statutory, actual, nominal, and/or punitive damages; and

l) Whether injunctive or declaratory relief is warranted to prevent Defendant's ongoing collection, use, and disclosure of Class Members' Sensitive Information.

202. **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.

203. **Adequacy**. Plaintiffs will fairly and adequately represent and protect the 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.

204. **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.

205. **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.

206. 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.

207. 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 Members 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.

208. 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.

XIX. TOLLING AND ESTOPPEL

209. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of the incorporation and operation of ACR technology and related data-collection and transmission systems on Hisense Smart TVs.

210. The ACR systems on Hisense Smart TVs are, and at all relevant times have been, invisible to the average user and operate without any contemporaneous indication that audio or video content is being captured, analyzed, or transmitted, including because Defendant's conduct occurs at the device and server level and is not observable through ordinary use of the television. There is no on-screen indicator, recording light, transmission alert, or other visual cue that would alert a reasonable consumer that the Smart TV is, in real time, capturing fingerprints of every sound and image displayed on the screen and transmitting that data to remote servers operated by VIDAA, Nexxen, Roku, Alphonso, Hisense's Chinese parents and affiliates, or any other downstream recipient.

211. Defendant had exclusive knowledge that Hisense Smart TVs incorporated ACR technology and were configured to capture, process, and transmit content-derived data and associated identifiers to multiple separate third parties (including VIDAA, Nexxen, Roku, Alphonso, and Hisense's Chinese parents and affiliates), and to facilitate access to that data by Hisense's Chinese parents and affiliates in violation of the DOJ Bulk Sensitive Data Transfer Rule, yet failed to adequately disclose any of these practices to users, including Plaintiffs and Class Members.

212. Defendant further concealed the nature, scope, and consequences of these practices through misleading terminology, fragmented disclosures, and deceptive interface design, including (a) the use of the benign-sounding label "Enhanced Viewing Service" (which does not, by its terms, identify any third party, identify ACR functionality, or convey that the feature operates as continuous frame-by-frame surveillance); (b) the bundling of multiple agreements during setup such that meaningful review of the ACR-related disclosure was practically impossible; and (c) the

dispersion of opt-out controls across four or more separate menus requiring more than 200 clicks, which obscured the practices in operation at the time of each Plaintiff's purchase.

213. Under these circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of their collection, use, and disclosure of users' Sensitive Information. To date, Defendant has not fully disclosed or acknowledged the extent to which they captured, identified, and transmitted users' viewing activity and associated identifiers to third parties such as VIDAA, Nexxen, Roku, Alphonso, and Hisense's Chinese parents and affiliates.

214. Accordingly, Defendant is estopped from relying on any statute of limitations.

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

216. The earliest that Plaintiffs or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct (as alleged with specificity in this Complaint) was no earlier than December 15, 2025, when the Texas Attorney General publicly filed an Original Petition and Application for Temporary and Permanent Injunctions against Hisense USA Corporation in Comal County, Texas, alleging in detail the existence, scope, and operation of Hisense's ACR surveillance program. Prior to that filing, no public source identified, by name and with the specificity necessary to put a reasonable consumer on notice, Hisense's specific ACR practices, Hisense's specific third-party-disclosure pipelines, Hisense's specific deceptive labeling and dark-pattern consent architecture, or Hisense's specific data-transfer relationships with its Chinese parents and affiliates.

217. Although prior reports suggested that certain smart televisions collected viewing data, those generic reports did not reveal the nature, scope, or recipients of Hisense's specific ACR-based interceptions. Defendant did not disclose that Hisense Smart TVs captured content displayed across all inputs—including HDMI-connected devices—or that such information was transmitted in real time and near-real time to multiple separate third parties such as VIDAA, Nexxen, Roku, and Alphonso, or that the resulting bulk data was transferred or facilitated for access to Hisense's Chinese parents and affiliates in violation of the DOJ Bulk Sensitive Data

Transfer Rule. These transmissions occurred through hidden background processes not visible to users and were only recently uncovered through forensic network analysis by independent academic researchers, regulatory enforcement actions, and counsel's pre-suit investigation. As a result, Plaintiffs and Class Members could not reasonably have discovered Defendant's unlawful conduct earlier through the exercise of reasonable diligence.

218. Defendant may contend that Plaintiffs were on inquiry notice based on (i) Hisense's own privacy policy or EULA, (ii) the 2024 Anselmi academic study, (iii) a 2015 New York Times consumer-electronics article, (iv) a 2016 FTC workshop discussing ACR, or (v) the 2017 putative class action White v. LG Electronics. None of those sources put a reasonable Hisense Smart TV owner on inquiry notice of the specific conduct alleged here. Hisense's own disclosures used misleading terminology (including "Enhanced Viewing Service", which does not identify any third-party recipient or convey continuous ACR surveillance) and were buried behind dark-pattern consent flows. The 2024 Anselmi paper was published in a technical academic repository requiring network-analysis expertise to interpret and was not disseminated to consumers. The 2015 NYT article, the 2016 FTC workshop, and the 2017 White v. LG Electronics action each addressed Smart TV manufacturers other than Hisense, did not name Hisense, did not identify Hisense's specific ACR vendors (VIDAA, Nexxen, Roku, Amazon, or Alphonso), and did not disclose Hisense's transfer of bulk Hisense ACR data to its Chinese parents and affiliates in violation of the DOJ Bulk Sensitive Data Transfer Rule (which itself only took effect on April 8, 2025).

219. Beyond the discovery rule and equitable estoppel, Defendant's continuing course of conduct independently tolls the applicable limitations periods. Hisense's ACR system continues to capture, transmit, and re-distribute Plaintiffs' and Class Members' communications and personal identifiers in real time and near-real time, on every Hisense Smart TV in operation, to the present day. Each new interception, capture, transmission, and re-disclosure is an independent violation that triggers a fresh limitations period, including under the federal Wiretap Act (each interception), CIPA §§ 631, 632, and 638.50–638.51 (each unauthorized interception or

recording), the VPPA (each disclosure of personally identifiable viewing information), and the UCL (each unfair, unlawful, or fraudulent business act).

XX. CLAIMS FOR RELIEF

COUNT I

Invasion of Privacy – Intrusion Upon Seclusion

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

220. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

221. Plaintiffs bring this claim under California common law.

222. At all relevant times, Plaintiffs and members of the Class had a reasonable expectation of privacy in their homes and in the audiovisual content they viewed on their televisions.

223. The home is among the most private of spaces, and activities occurring within the home—including television viewing—are traditionally understood to be private.

224. Defendant Hisense, through its Smart TVs and embedded ACR technology, intentionally intruded upon Plaintiffs' and Class members' private affairs.

225. Specifically, Hisense's Smart TVs continuously monitored what appeared on the television screen by capturing audio and visual information from content displayed on the device.

226. Hisense's ACR system captured information reflecting Plaintiffs' viewing behavior, including the programs watched, the applications used, and the content displayed through external devices connected via HDMI.

227. By capturing and analyzing this information, Hisense intruded into Plaintiffs' private viewing activity within the home.

228. Hisense's conduct enabled it to construct detailed profiles of Plaintiffs' interests, habits, and personal characteristics based on viewing behavior.

229. These profiles included Sensitive Information reflecting Plaintiffs' preferences, beliefs, and lifestyle.

230. Hisense designed, implemented, and deployed ACR technology for the purpose of collecting and monetizing consumer viewing data.

231. Hisense's subsidiary, VIDAA, USA, Inc. ("VIDAA") independently and intentionally intruded upon Plaintiffs' and Class Members' private affairs by participating in the contemporaneous receipt, processing, and analysis of ACR-derived viewing data captured from Hisense Smart TVs. VIDAA's ACR software was integrated into Hisense Smart TV operating systems such that viewing data and associated identifiers were transmitted to VIDAA-operated servers in real time or near-real time as users watched content within the privacy of their homes.

232. VIDAA used this data to identify the specific audiovisual content being viewed—including programs, episodes, advertisements, and other on-screen material—regardless of whether that content originated from streaming applications, broadcast signals, or HDMI-connected external devices. This content recognition occurred within seconds of display and operated continuously or at frequent intervals during device use, enabling VIDAA to track Plaintiffs' and Class Members' viewing activity as it occurred.

233. In connection with this conduct, VIDAA received and processed persistent identifiers associated with Plaintiffs' and Class Members' devices and households, including IP addresses, MAC addresses, advertising identifiers, household identifiers, and other unique or quasi-unique signals. VIDAA used these identifiers, together with additional data obtained from third-party partners (including Nexxen, identity-resolution providers, and data brokers), to associate Plaintiffs' and Class Members' Smart TV activity with other devices and identities.

234. Through these practices, VIDAA constructed and maintained identity-resolution systems—commonly referred to as identity graphs—that linked Plaintiffs' and Class Members' televisions, mobile devices, computers, and other connected devices to a unified profile representing the household and its inferred members. VIDAA's identity graph and related systems enabled it to combine ACR-derived viewing data with other datasets, including advertising

identifiers and partner-provided information, to generate detailed, cross-device profiles reflecting Plaintiffs' viewing habits, preferences, and personal characteristics.

235. Through this aggregation and profiling, VIDAA was able to infer sensitive attributes about Plaintiffs and Class Members—including their political preferences, religious beliefs, health conditions, sexual orientation, family composition, financial status, and personal interests—and to associate those attributes with identifiable households and devices. VIDAA used these profiles to create audience segments, enable targeted advertising, and facilitate cross-device tracking, and disclosed or made the resulting information available to Nexxen and to other ad-tech partners, advertisers, data brokers, and identity-resolution providers for commercial purposes.

236. This conduct—intercepting and analyzing Plaintiffs' private viewing activity in real time or near-real time, linking that activity to persistent identifiers, constructing cross-device identity profiles, and disseminating those profiles within the connected-television advertising ecosystem—constitutes a separate and independently actionable intrusion into Plaintiffs' and Class Members' private affairs.

237. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

238. Hisense's intrusion into Plaintiffs' private affairs would be highly offensive to a reasonable person.

239. A reasonable consumer would not expect that a television would continuously monitor and record the content displayed on its screen for the purpose of data collection and advertising.

240. Hisense's conduct therefore constitutes an intentional intrusion upon the solitude and seclusion of Plaintiffs and members of the Class.

241. As a direct and proximate result of Hisense's conduct, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and related damages.

242. Plaintiffs and members of the Class are entitled to all available legal and equitable remedies, including compensatory damages, injunctive relief, and any other relief deemed appropriate by the Court.

COUNT II

Invasion of Privacy – Public Disclosure of Private Facts

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

243. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

244. Plaintiffs bring this claim under California common law.

245. At all relevant times, Plaintiffs and members of the Class had a reasonable expectation that their television viewing activity and related information would remain private.

246. Defendant Hisense, through its Smart TVs and embedded ACR technology, collected and disclosed private information concerning Plaintiffs' viewing behavior.

247. Specifically, Hisense collected detailed information about the audiovisual content displayed on Plaintiffs' television, including the programs watched, the timing and duration of viewing sessions, and the sources of such content.

248. This information also included content viewed through third-party applications, broadcast signals, and external devices connected via HDMI.

249. The viewing information collected by Hisense constituted private facts because it reflected Plaintiffs' personal interests, habits, and preferences.

250. More specifically, the private facts Defendant disclosed are not merely that Plaintiffs watched unspecified content; rather, they include (i) specific program titles, episodes, advertisements, and external-input content viewed by each Plaintiff; (ii) timestamped logs of each

viewing session, by household and device; and (iii) inferred sensitive attributes about each Plaintiff that Defendant's ad-tech partners, including VIDAA, Nexxen, Roku, and Alphonso, expressly compute from the disclosed viewing data, including political beliefs and affiliations (e.g., audience segments built from State of the Union viewing or "liberal affinity news" or "conservative affinity news" viewing), religious beliefs and observances, sexual orientation (e.g., audience segments built from Pride Month programming), racial and ethnic identification, family composition (including the presence and ages of children), health conditions and medical concerns, financial circumstances, and other intimate personal characteristics. These categories of inferred personal attributes are precisely the "embarrassing" or "intimate" private facts that California courts and the Ninth Circuit have recognized as actionable. *See Harris v. iHeartMedia, Inc.*, 2026 WL 247875, at *1–*2 (N.D. Cal. Jan. 29, 2026); *Riganian v. LiveRamp Holdings, Inc.*, 791 F. Supp. 3d 1075, 1088 (N.D. Cal. 2025); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 604 (9th Cir. 2020).

251. Defendant's disclosure of these private facts is "public" within the meaning of California law because it is not limited to a single recipient or a confidential audience. Defendant's disclosure pipeline routes the data to multiple separate corporate recipients (VIDAA, Nexxen, Roku, Alphonso, Hisense's Chinese parents and affiliates) and, through Nexxen's, Roku's, and Alphonso's downstream commercial pipelines, into the broader CTV advertising ecosystem—comprising hundreds of demand-side and supply-side platforms, identity-resolution providers, data brokers, advertisers, agencies, and measurement and attribution providers. Defendant's conduct therefore disseminates Plaintiffs' private facts well beyond a confidential or limited audience, satisfying the "public disclosure" element under California law as construed in cases such as *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 604, and Har*ris v. iHeartMedia, Inc.*, 2026 WL 247875, at *1–*2.

252. Such viewing activity is inherently private and is not ordinarily exposed to the public.

253. Hisense disclosed this private information to third parties, including advertisers, analytics providers, and other commercial entities.

254. VIDAA received Plaintiffs' and Class Members' viewing data and associated identifiers in real time or near-real time and used that information to identify the specific audiovisual content viewed by Plaintiffs and Class Members, including programs, advertisements, and other on-screen material. In connection with this conduct, VIDAA associated Plaintiffs' viewing activity with persistent identifiers, including IP addresses, MAC addresses, advertising identifiers, household identifiers, and other signals, and combined that information with data obtained from third-party partners and data providers.

255. Through these processes, VIDAA constructed and maintained cross-device and household-level identity profiles that linked Plaintiffs' Hisense Smart TV viewing activity to other devices, identities, and datasets. VIDAA used these profiles to generate audience segments and other commercially valuable datasets reflecting Plaintiffs' viewing habits, interests, and inferred characteristics.

256. VIDAA further disclosed, sold, licensed, or otherwise made available Plaintiffs' viewing information and derived profiles to additional third parties within the advertising and data ecosystem—including, pursuant to its multi-year exclusive partnership, to Nexxen International Ltd., which in turn re-distributed audience segments and targeting data to advertisers, agencies, and demand-side platforms. By transforming Plaintiffs' private viewing activity into identifiable, cross-device profiles and distributing that information to numerous third parties, Defendant caused Plaintiffs' private facts to be publicly disclosed within the meaning of California law.

257. Upon information and belief, Hisense shared or made available Plaintiffs' viewing data to these third parties in a manner that enabled them to use the data for targeted advertising, analytics, and profiling purposes.

258. Hisense's disclosures were not limited to a small or confidential group but instead were made to multiple third-party entities within the advertising and data ecosystem.

259. Through these disclosures, Plaintiffs' private viewing information was disseminated beyond Hisense and into a broader commercial network.

260. Hisense's disclosures were made without Plaintiffs' consent.

261. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

262. Hisense also failed to adequately disclose the scope and nature of the information being disclosed.

263. Even where settings existed to limit data sharing, those settings were difficult to locate, buried within multiple layers of menus, and not clearly described.

264. Hisense's consent framework therefore constitutes a "dark pattern" designed to obtain user acquiescence rather than informed consent.

265. The private facts disclosed by Hisense would be highly offensive and objectionable to a reasonable person.

266. A reasonable consumer would not expect that a television manufacturer would collect and disclose detailed information about their viewing habits to third parties.

267. The disclosure of such information exposes intimate details about an individual's interests, beliefs, and lifestyle.

268. Hisense's conduct therefore constitutes a public disclosure of private facts.

269. As a direct and proximate result of Hisense's conduct, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and related damages.

270. Plaintiffs and members of the Class are entitled to all available legal and equitable remedies, including compensatory damages, injunctive relief, and any other relief deemed appropriate by the Court.

COUNT III

Invasion of Privacy – Violation of the California Constitution (Art. I, § 1)

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses; and, as to the public injunction, on behalf of the general public)

271. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

272. Plaintiffs bring this claim under Article I, Section 1 of the California Constitution, which guarantees a right to privacy.

273. The California Constitution protects individuals against the invasion of their privacy by private entities, including the unauthorized collection, use, and disclosure of personal information.

274. To establish a violation of the constitutional right to privacy, a plaintiff must show: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) a serious invasion of privacy.

275. Plaintiffs and members of the Class possessed legally protected privacy interests in their personal information, including their television viewing activity and related audiovisual data.

276. Plaintiffs' viewing behavior, including the content watched, the timing and duration of viewing sessions, and the sources of such content, constituted personal Sensitive Information.

277. This information revealed details about Plaintiffs' interests, habits, preferences, and personal characteristics.

278. Plaintiffs and members of the Class had a reasonable expectation that their television viewing activity within their homes would remain private.

279. The home is among the most private of spaces, and activities occurring within the home—including television viewing—are traditionally understood to be private.

280. Defendant Hisense violated Plaintiffs' reasonable expectation of privacy by collecting, analyzing, and disclosing Plaintiffs' viewing data through its Smart TVs and embedded ACR technology.

281. This capture occurred continuously during use of the television and operated independently of the source of the content.

282. Hisense's surveillance extended to content viewed through streaming applications, broadcast television, and external devices connected via HDMI.

283. Hisense thereby monitored Plaintiffs' viewing activity across all inputs and sources.

284. Hisense used the information obtained through this surveillance to build detailed profiles of Plaintiffs' viewing habits and preferences.

285. Hisense further disclosed or made this information available to third parties, including advertisers and analytics providers, for commercial purposes.

286. Hisense's conduct constituted a serious invasion of Plaintiffs' privacy.

287. The scope, duration, and nature of Hisense's surveillance—continuous monitoring of audiovisual content within the home—were highly intrusive.

288. Hisense's conduct enabled the collection of detailed and Sensitive Information about Plaintiff's private life.

289. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

290. Hisense also failed to disclose the full scope and purpose of its data collection and sharing practices.

291. Even where settings existed to limit data collection or sharing, those settings were difficult to locate, buried within multiple layers of menus, and not clearly described.

292. Hisense's consent framework therefore constitutes a "dark pattern" designed to obtain user acquiescence rather than informed consent.

293. Moreover, Hisense's surveillance affected individuals who never interacted with Hisense's disclosures or consent mechanisms, including other household members and guests.

294. Hisense's conduct therefore violated Plaintiffs' right to privacy under the California Constitution.

295. As a direct and proximate result of Hisense's conduct, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and related damages.

296. Plaintiffs and members of the Class are entitled to all available legal and equitable remedies, including injunctive relief and any other relief deemed appropriate by the Court.

297. Plaintiffs, on behalf of the general public, seek public injunctive relief under the California Constitution enjoining Defendant from deploying, operating, or enabling Automatic Content Recognition technology that intercepts, records, or discloses the viewing activity or other personal information of California consumers without first obtaining clear, conspicuous, and separately disclosed consent. The primary purpose and effect of this relief is to prohibit unlawful acts that threaten future injury to the general public—every California consumer who now owns, later purchases, or otherwise uses a Hisense Smart TV—rather than to redress past injury to Plaintiffs or any discrete group of prior purchasers. Because Defendant continues to manufacture, sell, and operate Smart TVs that perform this surveillance, its unlawful conduct is ongoing and, absent an injunction, will continue to harm the public at large. This relief is prospective, runs to the general public, and does not require the Court to consider the individual claims of any non-party. Plaintiffs and the general public have no adequate remedy at law to secure Defendant's future compliance with California law.

COUNT IV

Violation of the California Invasion of Privacy Act (CIPA), Cal. Penal Code § 631

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses)

298. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

299. CIPA § 631 prohibits any person who by means of any "machine, instrument, contrivance" or in "any other manner:" (1) intentionally taps or makes an unauthorized connection with "any telegraph or telephone wire, line, cable, or instrument;" (2) willfully and without consent of "all parties to the communication" or in "any unauthorized manner" reads or "attempts to read" or "learn[s] 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" California; (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way" information so obtained; or (4) from aiding, agreeing, employing, or conspiring 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."

300. Defendant is a person under CIPA § 631.

301. At all relevant times, Plaintiffs and members of the Class used Hisense Smart TVs to access and display audiovisual content transmitted over the internet and other communication networks while in California.

302. Defendant Hisense—directed from and within California—through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including, but not limited to, VIDAA—to intercept Plaintiffs' communications while they were in transit.

303. Specifically, Hisense integrated and deployed third-party ACR and analytics technologies within its Smart TVs that captured audio and/or visual information from content displayed on the television screen in near real time.

304. These third-party technologies intercepted communications transmitted to and from Plaintiffs' device, including content delivered through streaming services, broadcast signals, and external devices connected via HDMI.

305. This interception occurred contemporaneously with the transmission and display of audiovisual content, while such communications were in transit, and before they reached a completed and static form.

306. More specifically, Hisense's ACR architecture is designed to read and learn the contents of consumers' audiovisual communications while those communications are still in transit, before they are received in a completed and static form. Hisense's ACR software (developed and operated through Defendant's wholly-owned subsidiary VIDAA and, where applicable, through Roku, Inc. and Alphonso, Inc.) generates content-identifying digital "fingerprints" on the Hisense Smart TV itself by sampling each frame of audio and video as the frame is rendered to the consumer's screen—as documented by independent academic forensics, in increments measured in milliseconds (e.g., every 10 milliseconds, batched and transmitted to ACR-vendor servers every approximately 15 seconds). The fingerprint generation is itself a real-time learning of the substance, purport, and meaning of the audiovisual communication: the device-side ACR module identifies the on-screen content (program, episode, advertisement, application, or HDMI source) at the moment of display and prior to any persistent storage of the fingerprint by the ACR vendor.

307. Once transmitted, the fingerprints are matched in real time or near-real time against VIDAA-, Nexxen-, Roku-, or Alphonso-controlled databases of known content. That matching process is itself a contemporaneous learning of the contents of Plaintiffs' communications: the ACR vendor identifies the specific program, episode, advertisement, or external-input content displayed on the Hisense Smart TV before the data is stored, before the consumer's viewing session is complete, and before the audiovisual communication has reached a completed and static form on the consumer's screen. Plaintiffs further allege, on information and belief, that the third-party recipients (VIDAA, Nexxen, Roku, and Alphonso) incorporate the identified content into household-level audience segments, identity-graph nodes, and real-time bidding inventories before the consumer finishes watching the content—mirroring the architectures held to satisfy CIPA §

631's "in transit" requirement in Riganian v. LiveRamp Holdings, Inc., 791 F. Supp. 3d 1075, 1092 (N.D. Cal. 2025), and Doe v. FullStory, Inc., 712 F. Supp. 3d 1244 (N.D. Cal. 2024).

308. Accordingly, Hisense's and the third-party ACR vendors' interception of Plaintiffs' communications is not a mere post-hoc processing of stored data. It is a real-time, frame-by-frame reading and learning of the contents of consumers' audiovisual communications while those communications are in transit and before they reach a completed and static form, in violation of Cal. Penal Code § 631(a).

309. By capturing fragments of audiovisual output and processing them to identify the underlying content, these third parties acquired the contents and meaning of Plaintiffs' communications.

310. Hisense knowingly aided, agreed with, employed, and conspired with each of multiple separate third parties—including, but not limited to, VIDAA, USA, Inc.; Nexxen International Ltd.; Roku, Inc. (with respect to Hisense Smart TVs configured with the Roku OS operating system); Alphonso, Inc. (now part of LG Ad Solutions); and additional downstream demand-side platforms, supply-side platforms, identity-resolution providers, and measurement and attribution providers—to intercept, read, and learn the contents and meaning of Plaintiffs' and Class Members' electronic communications in real time or near-real time, while those communications were in transit and before they reached a completed and static form, in violation of Cal. Penal Code § 631(a). Each such third party is a separate "person" within the meaning of Cal. Penal Code § 631(a) and the cases construing it. Hisense's status as a party to certain of those communications therefore does not shield it from liability, because Hisense's conduct falls within the "aids, agrees with, employs, or conspires with any person or persons" clause of § 631(a). Hisense's aiding was undertaken knowingly and intentionally, with full awareness that VIDAA, Nexxen, Roku, Alphonso, and the other downstream third-party recipients would, in real time or near-real time, capture, decode, fingerprint, and learn the contents and meaning of consumers' private viewing communications. Hisense engineered and configured its Smart TVs, software, and over-the-air updates with the specific purpose of enabling these third-party interceptions; entered

into commercial agreements (including, in the case of Nexxen, a multi-year exclusive ACR-data and ad-monetization agreement extending through at least 2029, and including a substantial equity investment by Nexxen in VIDAA) the express purpose of which is to enable third-party access to consumers' intercepted ACR communications; and continues to update and operationally support the systems through which the third-party interceptions occur.

311. Hisense provided the hardware, software environment, and system-level access necessary for these third parties to perform the interception.

312. Hisense also configured its Smart TVs to permit and facilitate the operation of these third-party interception technologies across all inputs, including:

- content streamed through third-party applications;
- cable and broadcast television signals; and
- content from external devices such as streaming boxes, gaming consoles, and computers connected via HDMI.

313. As a result, third parties intercepted communications that occurred entirely outside of Hisense's own services or platforms.

314. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

315. Because CIPA requires the consent of all parties to a communication, the real-time and near-real-time interception of communications by Hisense's third-party partners—including, but not limited to, VIDAA, USA, Inc., Nexxen International Ltd., Roku, Inc., Alphonso, Inc. (now part of LG Ad Solutions), and additional downstream demand-side platforms, supply-side platforms, identity-resolution providers, and measurement and attribution providers—was unlawful.

316. Plaintiffs and members of the Class had a reasonable expectation that their viewing activity—including the audiovisual content displayed on their televisions—would not be intercepted or monitored by Hisense.

317. Hisense's conduct constitutes an egregious invasion of privacy and a violation of California law.

318. As a direct and proximate result of Hisense's violations of CIPA, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and statutory damages.

319. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and members of the Class seek statutory damages, injunctive relief, and all other relief available under the law.

COUNT V

Violation of the California Invasion of Privacy Act (CIPA), Cal. Penal Code § 632

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses)

320. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

321. Cal. Penal Code § 632 prohibits any person, without the consent of all parties to a confidential communication, from intentionally eavesdropping upon or recording the confidential communication by means of any electronic amplifying or recording device.

322. At all relevant times, Plaintiffs and members of the Class engaged in communications through their use of Hisense Smart TVs, including audiovisual transmissions delivered through streaming applications, broadcast signals, and external devices connected via HDMI.

323. Defendant Hisense, through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including, but not limited to, VIDAA—to eavesdrop upon and record Plaintiffs' confidential communications.

324. Specifically, Hisense integrated and deployed third-party ACR and analytics technologies within its Smart TVs that captured audio and/or audiovisual information from content displayed on the television screen in near real time.

325. Hisense knowingly aided, agreed with, employed, and conspired with these third parties to eavesdrop upon and record Plaintiffs' confidential communications in violation of Cal. Penal Code § 632.

326. Hisense provided third parties with persistent identifiers, device-level access, and content recognition outputs sufficient to associate recorded communications with specific users and households.

327. Plaintiffs and members of the Class reasonably expected that their viewing activity and the audio and audiovisual content displayed within their homes would not be recorded or monitored by Hisense.

328. The communications occurred within private residences and concerned personal viewing choices, habits, and interests, which are inherently private in nature.

329. Hisense configured its Smart TVs to permit and facilitate the operation of these third-party recording technologies across all inputs, including:

- content streamed through third-party applications;
- cable and broadcast television signals; and
- content from external devices such as streaming boxes, gaming consoles, and computers connected via HDMI, as well as other personal devices connected over Wi-Fi internet, such as computers, smartphones and tablets.

330. Plaintiffs and members of the Class did not consent to the recording of their confidential communications by Hisense's third-party partners.

331. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the

section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

332. Because CIPA requires the consent of all parties to a communication, the recording of communications by Hisense's third-party partners—including, but not limited to, VIDAA—was unlawful.

333. Plaintiffs and members of the Class had a reasonable expectation that their confidential communications—including audiovisual content viewed within their homes—would not be recorded by Hisense.

334. Hisense's conduct constitutes an egregious invasion of privacy and a violation of California law.

335. As a direct and proximate result of Hisense's violations of Cal. Penal Code § 632, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and statutory damages.

336. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and members of the Class statutory damages, injunctive relief, and all other relief available under the law.

COUNT VI

Violation of the California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 638.50–638.51

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses)

337. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

338. Cal. Penal Code § 638.50 prohibits any person or entity from knowingly installing or using a pen register or trap and trace device without first obtaining a court order or authorization as required by law.

339. Cal. Penal Code § 638.51 prohibits any person or entity from installing or using a pen register or trap and trace device without the consent of the user of the service.

340. A "pen register" is defined under California law as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

341. A "trap and trace device" is defined as a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication.

342. At all relevant times, Plaintiffs and members of the Class used Hisense Smart TVs to send and receive electronic communications over the internet and other communication networks while in California.

343. These communications included, among other things:

- requests for streaming video content;
- application usage data;
- device-level communications between Smart TVs and remote servers; and
- audiovisual transmissions delivered to the television through streaming services and external devices.

344. Defendant Hisense, through its Smart TVs and embedded ACR technology, knowingly installed and operated processes that functioned as pen registers and trap and trace devices.

345. Specifically, Hisense's ACR system and related telemetry processes captured and recorded routing, addressing, and signaling information associated with communications transmitted to and from Plaintiffs' Smart TV.

346. This information included, among other things:

- identifiers associated with content being requested or displayed;
- application identifiers and usage signals;
- device identifiers and network information; and

- other metadata reflecting how, when, and from where communications were transmitted.

347. Hisense's systems captured this information contemporaneously with the transmission of communications and without regard to the source of the content.

348. By capturing and processing this information, Hisense recorded dialing, routing, addressing, and signaling information associated with Plaintiffs' electronic communications.

349. Hisense also captured incoming and outgoing communication signals sufficient to identify the source and destination of communications involving Plaintiffs' Smart TV.

350. Hisense's conduct therefore constituted the use of pen registers and trap and trace devices within the meaning of Cal. Penal Code §§ 638.50–638.51.

351. Hisense installed and used these devices and processes without obtaining a court order or lawful authorization.

352. Hisense also installed and used these devices and processes without the consent of Plaintiffs and members of the Class.

353. Plaintiffs and members of the Class were not informed that Hisense would capture routing, addressing, and signaling information associated with their communications.

354. Any purported consent obtained by Hisense was invalid because it was not informed, explicit, or meaningful.

355. Hisense obscured the nature of its data collection through misleading terminology, including labeling its surveillance features as "Enhanced Viewing Service" or "Enhanced Viewing Service."

356. Defendant Hisense, through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including, but not limited to, VIDAA—to eavesdrop upon and record Plaintiffs' confidential communications.

357. Specifically, Hisense integrated and deployed third-party ACR and analytics technologies within its Smart TVs that captured audio and/or audiovisual information from content displayed on the television screen in near real time.

358. Hisense knowingly aided, agreed with, employed, and conspired with these third parties to eavesdrop upon and record Plaintiffs' confidential communications in violation of Cal. Penal Code § 632.

359. Moreover, Hisense's data collection captured communications and associated signaling information of individuals who never interacted with Hisense's disclosures or consent mechanisms, including other household members and guests.

360. Plaintiffs and members of the Class had a reasonable expectation that the routing, addressing, and signaling information associated with their communications would not be captured or monitored by Hisense.

361. Hisense's conduct constitutes an egregious invasion of privacy and a violation of California law.

362. As a direct and proximate result of Hisense's violations of Cal. Penal Code §§ 638.50–638.51, Plaintiffs and members of the Class have suffered harm, including invasion of privacy, loss of control over personal information, and statutory damages.

363. Pursuant to Cal. Penal Code § 637.2 and other applicable provisions, Plaintiffs and members of the Class seek statutory damages, injunctive relief, and all other relief available under the law.

COUNT VII

Violation of the Comprehensive Computer Data Access and Fraud Act (CDAFA), Cal. Penal Code § 502

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses)

364. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

365. Plaintiffs bring this claim under the CDAFA, Cal. Penal Code § 502.

366. At all relevant times, Plaintiffs' Hisense Smart TV constituted a "computer," "computer system," and/or "computer network" within the meaning of Cal. Penal Code § 502(b).

367. Plaintiffs and members of the Class were the owners and/or authorized users of their Hisense Smart TVs.

368. Defendant Hisense knowingly and without permission accessed, used, and caused to be used Plaintiffs' Smart TV and related computer systems.

369. Specifically, Hisense, through its embedded ACR technology and related software processes, accessed Plaintiffs' Smart TV to collect, extract, and transmit data regarding Plaintiffs' viewing activity.

370. Hisense's conduct included taking, copying, and making use of data from Plaintiffs' Smart TV, including audiovisual content information, device-level data, and associated identifiers.

371. Hisense used this data for its own commercial purposes, including advertising, analytics, and consumer profiling.

372. Hisense's conduct violated Cal. Penal Code § 502(c), including but not limited to:

- § 502(c)(1), by knowingly accessing and without permission altering, damaging, deleting, destroying, or otherwise using data and computer systems;
- § 502(c)(2), by knowingly accessing and without permission taking, copying, or making use of data from a computer, computer system, or computer network;
- § 502(c)(3), by knowingly and without permission using or causing to be used computer services; and
- § 502(c)(7), by knowingly accessing or causing to be accessed any computer, computer system, or computer network without permission.

373. Hisense's access to Plaintiffs' Smart TV and associated data was without permission because Plaintiffs did not authorize Hisense to collect, extract, or monetize detailed information about the audiovisual content displayed on the device.

374. Any purported authorization obtained by Hisense was invalid because it was not informed, explicit, or meaningful.

375. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs

incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

376. As a direct and proximate result of Hisense's conduct, Plaintiffs and members of the Class suffered damage and loss within the meaning of Cal. Penal Code § 502(e), including but not limited to:

- unauthorized use of their devices and data;
- misappropriation of valuable personal information; and
- loss of control over their data.

377. Hisense's conduct was knowing, intentional, and wrongful.

378. Plaintiffs and Class Members have suffered "damage or loss" within the meaning of Cal. Penal Code § 502(e). Plaintiffs intended to retain the option to monetize, license, or otherwise control the disposition of their viewing data and household-level identifiers, including by participating in the established market in which companies (such as Nielsen, UpVoice, HoneyGain, SavvyConnect, and others) compensate consumers in exchange for license to track specified categories of personal data. Defendant's unauthorized capture, extraction, transmission, and re-distribution of Plaintiffs' viewing data and identifiers materially diminished the value of that data to Plaintiffs by (i) extracting and segmenting the data before Plaintiffs could license it themselves, (ii) injecting the data into proprietary identity graphs and audience segments operated by VIDAA, Nexxen, Roku, and Alphonso (which exclude Plaintiffs from any subsequent monetization), and (iii) reducing the marginal commercial value of the data on the consumer-data market by virtue of its prior unauthorized commercial exploitation. Plaintiffs have therefore suffered both deprivation of the right to control their data and a diminution in its market value—each of which constitutes "damage or loss" under § 502(e).

379. In addition, Plaintiffs and Class Members have incurred (and on information and belief will continue to incur) reasonable expenditures—within the meaning of Cal. Penal Code § 502(e)(1)—to investigate, identify, and verify the unauthorized access to and extraction of data

from their Hisense Smart TVs, including time and resources expended to ascertain whether their Smart TV systems and stored configuration data have been altered, accessed, or used by Defendant and the third-party ACR vendors (VIDAA, Nexxen, Roku, and Alphonso) without authorization.

380. Pursuant to Cal. Penal Code § 502(e) and (e)(1), Plaintiffs and members of the Class seek compensatory damages, injunctive relief, and all other relief available under the law.

COUNT VIII

Violation of the Federal Wiretap Act (as amended by the Electronic Communications Privacy Act or "ECPA"), 18 U.S.C. § 2510, et seq.

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes)

381. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

382. Plaintiffs bring this claim under the Federal Wiretap Act, 18 U.S.C. § 2510, et seq.

383. The Federal Wiretap Act prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept any wire, oral, or electronic communication, as well as from using or disclosing the contents of such communications without consent.

384. At all relevant times, Plaintiffs and members of the Nationwide Class transmitted and received electronic communications through their use of Hisense Smart TVs.

385. These communications included, among other things, streaming video content, audiovisual transmissions, application data, and communications between Plaintiffs' Smart TV and remote servers.

386. These transmissions constitute "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

387. Defendant Hisense, through its Smart TVs and embedded ACR technology, intentionally intercepted, endeavored to intercept, and procured the interception of these communications.

388. Specifically, Hisense's ACR system captured audio and/or visual information from content displayed on Plaintiffs' television screen in near real time.

389. This capture occurred contemporaneously with the transmission and display of the communications.

390. By capturing fragments of audiovisual output and processing them to identify underlying content, Hisense acquired the contents of Plaintiffs' electronic communications.

391. Hisense's interception occurred while the communications were in transit, and before they reached their intended destination in a completed and static form.

392. Hisense's ACR system captured communications across all inputs, including:

- content streamed through third-party applications;
- cable and broadcast television signals; and
- content from external devices such as streaming boxes, gaming consoles, and computers connected via HDMI.

393. As a result, Hisense intercepted communications that occurred entirely outside of Hisense's own services or platforms.

394. Hisense also used and disclosed the contents of these communications for its own commercial purposes, including advertising, analytics, and profiling.

395. Hisense's conduct was intentional.

396. Plaintiffs and members of the Nationwide Class did not consent to Hisense's interception, use, or disclosure of their communications.

397. Any purported consent obtained by Hisense was invalid because it was not informed, explicit, or meaningful.

398. Even if Hisense were deemed a party to any of the intercepted communications, the statutory exception set forth in 18 U.S.C. § 2511(2)(d) does not apply because Hisense intercepted such communications for the purpose of committing tortious and unlawful acts.

399. Specifically, Hisense intercepted Plaintiffs' communications in order to collect, analyze, monetize, and disclose detailed information regarding Plaintiffs' viewing activity without authorization.

400. Hisense's interception was undertaken for the purpose of committing, and in furtherance of committing, multiple independent torts and statutory violations, including:

- invasion of privacy – intrusion upon seclusion;
- invasion of privacy – public disclosure of private facts;
- invasion of privacy in violation of the California Constitution;
- violations of the California Invasion of Privacy Act (Cal. Penal Code §§ 631, 632, and 638.50–638.51);
- violations of the Video Privacy Protection Act (18 U.S.C. § 2710);
- violations of the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200); and
- unjust enrichment and other unlawful business practices; and
- willful violations of the U.S. Department of Justice's Bulk Sensitive Data Transfer Rule, 28 C.F.R. Part 202, promulgated under Executive Order 14117 and enforceable as a criminal offense under the International Emergency Economic Powers Act, 50 U.S.C. § 1705(c).

401. Hisense's interception of communications was therefore carried out for a tortious and unlawful purpose within the meaning of 18 U.S.C. § 2511(2)(d).

402. The crime-tort exception to § 2511(2)(d) is independently satisfied by Hisense's knowing and willful violations of the U.S. Department of Justice's Bulk Sensitive Data Transfer Rule, 28 C.F.R. Part 202, promulgated under Executive Order 14117. As alleged above, Hisense USA Corporation is a "U.S. person" under the DOJ Rule, 28 C.F.R. § 202.256, and Hisense's Chinese parents and affiliates—including Hisense Group Holdings Co., Ltd. and Hisense Co., Ltd.—are "covered persons" under the DOJ Rule, 28 C.F.R. § 202.211. The Hisense ACR data at issue—including IP addresses, MAC addresses and other device-based identifiers, advertising

identifiers, cookie data, and the granular viewing-behavior data with which they are linked—constitutes "covered personal identifiers" that, given the millions of U.S. households whose Hisense Smart TVs feed Defendant's ACR pipeline, plainly meets the "bulk" threshold under 28 C.F.R. § 202.205. Hisense's knowing transfer of, or knowing facilitation of access to, that bulk data by its Chinese parents and affiliates—without compliance with the CISA Security Requirements for Restricted Transactions issued under Executive Order 14117 and incorporated by reference at 28 C.F.R. § 202.248—constitutes either a Prohibited Data Transaction under 28 C.F.R. § 202.301 or a Restricted Data Transaction under 28 C.F.R. § 202.401, on or after the April 8, 2025 effective date of the Rule.

403. Hisense's violation of the DOJ Rule is willful. Hisense knows—through public statements by the Department of Justice, congressional and Treasury attention to the "data export to countries of concern" problem, the Texas Attorney General's December 15, 2025 enforcement action, its participation in industry groups that submitted comments during the DOJ Rule's rulemaking, and its own corporate-risk disclosures concerning cross-border data-transfer compliance—that the bulk transfer of, or facilitation of access to, the categories of identifiers at issue here by Chinese-controlled covered persons is prohibited absent strict CISA-compliant security controls. Hisense nevertheless has continued, on and after April 8, 2025, to design, configure, and operate its Smart TVs and ACR pipeline in a manner that systematically transfers, or facilitates the foreign-parent and CCP access to, that bulk U.S. sensitive personal data without the requisite controls.

404. Willful violations of the DOJ Rule constitute a federal criminal offense. The DOJ Rule is promulgated under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701 et seq. Section 1705(c) provides that any person who "willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act" under IEEPA "shall, upon conviction, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both." 50 U.S.C. § 1705(c). Hisense's willful violations of the DOJ Rule therefore independently constitute a "criminal" act "in violation

of the … laws of the United States" sufficient to defeat the "party" or "one-party consent" exception under 18 U.S.C. § 2511(2)(d).

405. Hisense's real-time and near-real-time disclosure of intercepted communications and associated identifiers to multiple separate third-party recipients—including, but not limited to, VIDAA, USA, Inc., Nexxen International Ltd., Roku, Inc. (with respect to Hisense Smart TVs configured with the Roku OS operating system), Alphonso, Inc. (now part of LG Ad Solutions), and additional downstream demand-side platforms, supply-side platforms, identity-resolution providers, and measurement and attribution providers—further confirms that, even if Hisense were deemed a "party" to certain of those communications, Hisense intentionally "procur[ed] [ ] other person[s] to intercept" them within the meaning of 18 U.S.C. § 2511(1)(a) and intentionally "disclose[d]" their contents within the meaning of 18 U.S.C. § 2511(1)(c), in each case for a criminal and tortious purpose.

406. Accordingly, any purported consent—whether actual, implied, or constructive—does not shield Hisense from liability under the Federal Wiretap Act.

407. Hisense's disclosures further obscured the nature of its surveillance through misleading terminology, including labeling its ACR features as "Enhanced Viewing Service" or "Enhanced Viewing Service."

408. Hisense presented disclosures during a forced, multi-step setup process that pressured consumers to agree to all terms in order to use the television, and failed to clearly inform users that Hisense would intercept, record, analyze, and monetize the content of their communications.

409. Hisense's conduct therefore was not authorized by law and does not fall within any statutory exception.

410. As a direct and proximate result of Hisense's violations of the Federal Wiretap Act, Plaintiffs and members of the Nationwide Class have suffered harm, including invasion of privacy, loss of control over personal information, and statutory damages.

411. Pursuant to 18 U.S.C. § 2520, Plaintiffs and members of the Nationwide Class seek statutory damages, punitive damages, injunctive relief, and all other relief available under the law.

COUNT IX

Violation of the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes)

412. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

413. Plaintiffs bring this claim under the VPPA, 18 U.S.C. § 2710.

414. The VPPA prohibits a "video tape service provider" from knowingly disclosing to any person personally identifiable information concerning a consumer's request for or obtaining of specific video materials or services, without the informed, written consent of the consumer.

415. Defendant Hisense was, and is, a "video tape service provider" within the meaning of 18 U.S.C. § 2710(a)(4), because it engaged in the business of delivering, providing, and facilitating access to audiovisual content and video programming through its Smart TVs and integrated software platforms.

416. More specifically, Hisense's (directly and through its wholly-owned operating-system and ACR subsidiary VIDAA, USA, Inc.) is "engaged in the business of … rental, sale, or delivery of … similar audio visual materials" under 18 U.S.C. § 2710(a)(4) because, inter alia: (i) Hisense markets, distributes, and operates the "Hisense TV+" (a/k/a "VIDAA Free" or "VIDAA Free Channels") streaming-video service that is pre-installed and prominently featured on Hisense Smart TVs, including a curated catalog of advertising-supported video content delivered to consumers directly by Hisense / VIDAA; (ii) Hisense's VIDAA OS home screen and content-discovery rails curate and surface specific audiovisual content from Hisense / VIDAA-controlled video sources to the consumer; and (iii) Hisense and VIDAA make available to consumers an integrated platform through which audiovisual content is delivered. The Hisense / VIDAA video-content-delivery business constitutes a substantial focus of Defendant's work for purposes of

Tawam v. Feld Ent. Inc., 684 F. Supp. 3d 1056, 1060 (S.D. Cal. 2023), and Osheske v. Silver Cinemas Acquisition Co., 132 F.4th 1110 (9th Cir. 2025).

417. Plaintiffs are "consumers" under 18 U.S.C. § 2710(a)(1) because each Plaintiff is, at minimum, a "subscriber" of Hisense's video goods or services. Each Plaintiff accessed Hisense's video-content-delivery functionality (including the "Hisense TV+" / VIDAA Free streaming service); each Plaintiff provided personal information to Hisense / VIDAA in connection with receiving that video content; and each Plaintiff has accessed audiovisual content delivered through Hisense's / VIDAA's integrated streaming services. These commitments and exchanges of value satisfy the "subscriber" definition under Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1256 (11th Cir. 2015), Perry v. Cable News Network, Inc., 854 F.3d 1336, 1342 (11th Cir. 2017), and Golden v. NBCUniversal Media, LLC, 688 F. Supp. 3d 150, 164 (S.D.N.Y. 2023).

418. The information Hisense's has knowingly disclosed constitutes "personally identifiable information" under 18 U.S.C. § 2710(a)(3) and the "ordinary person" test of Eichenberger v. ESPN, Inc., 876 F.3d 979, 985 (9th Cir. 2017). Specifically, Hisense's has disclosed to VIDAA, Nexxen, Roku, Alphonso, and other downstream recipients—in real time and near-real time, in transmissions transmitted from each Plaintiff's Hisense Smart TV—the specific audiovisual content viewed by Plaintiffs (including specific program titles, episodes, advertisements, and external-input identifications) tied directly and inextricably to persistent identifiers (including IP address, MAC address, advertising identifier, household identifier, Hisense / VIDAA account identifier, and a unique VIDAA-issued device identifier). The combination of specific viewing-content identification + persistent personal identifiers "readily permits an ordinary person to identify a particular individual as having watched certain videos"—indeed, that combination is precisely the basis on which VIDAA / Nexxen / Roku / Alphonso construct identity-graph profiles, target consumers across devices, and measure advertising attribution at the household and individual level.

419. Plaintiffs were "consumers" within the meaning of 18 U.S.C. § 2710(a)(1), as Plaintiffs used Hisense's Smart TV services to obtain video content.

420. Defendant Hisense knowingly disclosed to third parties personally identifiable information ("PII") concerning Plaintiffs' requests for and viewing of specific video materials and services.

421. Specifically, Hisense collected and disclosed detailed information about the audiovisual content displayed on Plaintiffs' television, including the programs watched, the timing and duration of viewing sessions, and the sources of such content.

422. This information included content viewed through streaming applications, broadcast signals, and external devices connected via HDMI.

423. Hisense disclosed this viewing information to third parties, including advertisers, analytics providers, and other commercial entities.

424. Upon information and belief, Hisense disclosed Plaintiffs' viewing data in conjunction with persistent identifiers and other information that allowed third parties to identify Plaintiffs and/or Plaintiffs' household.

425. These identifiers included, among other things, device identifiers, network identifiers, and other unique identifiers associated with Plaintiffs' Smart TV.

426. By linking viewing information with such identifiers, Hisense disclosed information that identified Plaintiffs as having requested or obtained specific video materials or services.

427. The information disclosed by Hisense therefore constituted "personally identifiable information" within the meaning of the VPPA.

428. Hisense made these disclosures knowingly.

429. Plaintiffs did not provide informed, written consent to Hisense's disclosure of Plaintiffs' personally identifiable viewing information.

430. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the

section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

431. Hisense also failed to disclose the scope, nature, and purpose of such disclosures.

432. Even where settings existed to limit data sharing, those settings were difficult to locate, buried within multiple layers of menus, and not clearly described.

433. Hisense's consent framework therefore constitutes a "dark pattern" designed to obtain user acquiescence rather than informed consent.

434. Hisense's conduct constituted a violation of 18 U.S.C. § 2710(b)(1).

435. As a direct and proximate result of Hisense's violations of the VPPA, Plaintiffs and members of the Nationwide Class have suffered harm, including invasion of privacy and loss of control over personal information.

436. Pursuant to 18 U.S.C. § 2710(c), Plaintiffs and members of the Nationwide Class seek statutory damages, punitive damages, attorneys' fees and costs, injunctive relief, and all other relief available under the law.

COUNT X

Negligence

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

437. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

438. Plaintiffs bring this claim under California common law.

439. At all relevant times, Defendant Hisense owed Plaintiffs and members of the Class a duty to exercise reasonable care in the design, development, manufacture, configuration, and operation of its Smart TVs and embedded software systems.

440. Beyond the data-security duty traditionally implicated in data-breach cases, Defendant's duty of reasonable care extends to the design, configuration, marketing, sale, software-updating, and ongoing operational support of Hisense Smart TVs in a manner consistent

with reasonable consumer privacy expectations and applicable federal and California law. That duty includes (a) the duty to make accurate, complete, and meaningful disclosures about ACR functionality, third-party data flows, and PRC data-transfer risks at the point of sale and during device setup; (b) the duty to refrain from designing, configuring, or operating Smart TVs in a manner that captures, intercepts, transmits, or re-distributes consumers' in-home audiovisual communications and personal identifiers without informed consent; (c) the duty to comply with federal national-security law, including the DOJ Bulk Sensitive Data Transfer Rule, 28 C.F.R. Part 202; and (d) the duty to ensure that Smart TVs designed for use in U.S. consumers' homes are not configured to facilitate the export of bulk U.S. sensitive personal data to covered persons in countries of concern absent CISA-compliant security controls.

441. This is not merely a data-security or data-breach case. Defendant's breaches of duty include the active design and operation of an architectural surveillance and disclosure pipeline that intentionally collects, transmits, and re-distributes Plaintiffs' sensitive viewing data and identifiers, in violation of Plaintiffs' reasonable expectations and applicable law. Negligent design and negligent configuration of consumer-electronic devices—as distinct from negligent failure to safeguard data already lawfully collected—are independently actionable.

442. Hisense also owed a duty to refrain from collecting, accessing, using, and disclosing Plaintiffs' personal information without authorization or adequate disclosure.

443. Hisense further owed a duty to implement reasonable practices to protect consumers' privacy and to avoid engaging in conduct that foreseeably invaded users' privacy interests.

444. Hisense knew or should have known that its Smart TVs would be used within consumers' homes and would display sensitive audiovisual content reflecting users' personal interests, habits, and preferences.

445. Hisense knew or should have known that the continuous monitoring and capture of such content through ACR technology would intrude upon users' privacy and expose personal Sensitive Information.

446. Hisense breached its duties by, among other things:

- designing and deploying ACR technology that continuously monitored and captured audiovisual content displayed on users' televisions;
- collecting detailed information about Plaintiffs' viewing activity without adequate disclosure or authorization;
- accessing and extracting data from Plaintiffs' Smart TV for purposes unrelated to core device functionality;
- failing to implement reasonable and transparent consent mechanisms;
- obscuring its data collection practices through misleading terminology and design; and
- disclosing or making available Plaintiffs' viewing information to third parties for commercial purposes.

447. Hisense's conduct fell below the standard of care expected of a reasonable company operating connected consumer devices in the home.

448. Hisense's actions were negligent and created a foreseeable risk of harm to Plaintiffs and members of the Class.

449. Plaintiffs and members of the Class did not consent to Hisense's conduct.

450. Any purported consent obtained by Hisense was invalid because it was not informed, explicit, or meaningful.

451. Hisense's conduct was a substantial factor in causing harm to Plaintiffs and members of the Class.

452. As a direct and proximate result of Hisense's negligence, Plaintiffs and members of the Class have suffered damages, including invasion of privacy, loss of control over personal information, and the unauthorized use and exploitation of their data.

453. Plaintiffs and members of the Class are entitled to recover damages, injunctive relief, and all other relief available under California law.

COUNT XI

Violation of California Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 et seq.

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclasses; and, as to the public injunction, on behalf of the general public)

454. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

455. Plaintiffs bring this claim under California's UCL, Cal. Bus. & Prof. Code § 17200 et seq.

456. The UCL prohibits any unlawful, unfair, or fraudulent business act or practice.

457. Defendant Hisense engaged in unlawful, unfair, and fraudulent business acts and practices in connection with its Smart TVs and embedded ACR technology.

1. Unlawful Prong

458. Hisense's conduct violated multiple laws, including but not limited to:

- the California Invasion of Privacy Act (Cal. Penal Code §§ 631, 632, 638.50–638.51);
- the Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502); and
- the Federal Wiretap Act (18 U.S.C. § 2510 et seq.).

459. These violations constitute "unlawful" business acts and practices under the UCL.

2. Unfair Prong

460. Hisense's conduct was unfair because it offended established public policy and was immoral, unethical, oppressive, and substantially injurious to consumers.

461. Hisense's conduct caused substantial injury to Plaintiffs and members of the Class by invading their privacy and misappropriating their personal information.

462. The harm to Plaintiffs and members of the Class outweighed any purported benefits associated with Hisense's conduct.

463. Plaintiffs and members of the Class could not reasonably have avoided the injury.

464. Hisense's surveillance practices were not necessary to provide the core functionality of its Smart TVs and instead served Hisense's commercial interests in data collection and advertising.

465. Hisense continuously monitored the content displayed on consumers' televisions, including content from streaming applications, broadcast signals, and HDMI-connected devices.

466. Hisense collected, analyzed, and monetized detailed information about Plaintiffs' viewing activity.

467. Hisense also shared or made this information available to third parties, including advertisers and analytics providers.

468. Hisense's conduct therefore constituted an unfair business practice.

3. Fraudulent Prong

469. Hisense's conduct was fraudulent because it was likely to deceive reasonable consumers.

470. Hisense misrepresented and omitted material facts regarding its data collection and surveillance practices.

471. Hisense used misleading terminology, including labeling its ACR features as "Enhanced Viewing Service," which did not disclose that the feature enabled continuous monitoring of on-screen content.

472. Hisense failed to clearly disclose that it would capture, analyze, and monetize the audiovisual content displayed on consumers' televisions.

473. Hisense also failed to disclose that such information would be shared with or made available to third parties.

474. Hisense presented disclosures during a forced, multi-step setup process that pressured consumers to agree to all terms in order to use the television.

475. Even where settings existed to limit data collection, those settings were difficult to locate, buried within multiple layers of menus, and not clearly described.

476. Hisense's consent framework therefore constitutes a "dark pattern" designed to obtain user acquiescence rather than informed consent.

477. These misrepresentations and omissions were material because a reasonable consumer would consider them important in deciding whether to purchase or use a Hisense Smart TV.

478. Plaintiffs and members of the Class were likely to be deceived by Hisense's conduct.

479. As a result of Hisense's unlawful, unfair, and fraudulent conduct, Plaintiffs and members of the Class suffered injury in fact and lost money or property.

480. Plaintiffs and members of the Class lost the value of their personal information and the benefit of their bargain.

481. Plaintiffs and members of the Class would not have purchased, or would have paid less for, Hisense Smart TVs had they known of Hisense's conduct.

482. Plaintiffs and members of the Class have suffered injury in fact and lost money or property as a direct result of Hisense's unfair, unlawful, and fraudulent business practices. Specifically, Plaintiffs paid for their Hisense Smart TVs (with the consumer purchase price flowing in substantial part to Hisense as wholesale revenue, even where the immediate point-of-sale transaction was through a retailer such as Amazon, Best Buy, Costco, Sam's Club, Target, or Walmart). Plaintiffs would not have purchased their Hisense Smart TVs at the prices paid—and on information and belief would have purchased a competing television, paid less, or not purchased a Smart TV at all—had Defendant disclosed (i) Hisense's continuous, frame-by-frame ACR surveillance, (ii) Hisense's real-time and near-real-time disclosure of consumers' viewing communications and identifiers to multiple separate third parties (VIDAA, Nexxen, Roku, Alphonso), and (iii) Hisense's transfer of, and facilitation of access to, that data by Hisense's Chinese parents and affiliates in violation of the DOJ Bulk Sensitive Data Transfer Rule. *See*

Kwikset Corp. v. Superior Ct., 51 Cal. 4th 310, 317, 322 (2011). That Plaintiffs purchased their Hisense Smart TVs through authorized retailers rather than directly from Hisense does not defeat standing. UCL benefit-of-the-bargain standing turns on whether the plaintiff surrendered more in a transaction than she otherwise would have as a result of the defendant's deception—not on privity between the plaintiff and the defendant. In *Kwikset*, the California Supreme Court found standing where a manufacturer's deceptive "Made in U.S.A." labeling caused consumers to overpay for products acquired through the ordinary retail distribution chain. So too here: Hisense markets, brands, and makes representations directly to consumers through its packaging, advertising, and on-device user interface, and Hisense realizes the economic value of each consumer purchase as wholesale revenue. This case is therefore unlike *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024 (S.D. Cal. 2023), in which the defendant data broker had no consumer-facing relationship with, and made no representations to, the plaintiff. *See Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 317, 322 (2011).

483. Hisense's misrepresentations and material omissions are precisely the kind that satisfy the UCL "fraudulent" prong: Hisense's marketing materials, packaging, and on-device disclosures portray the Hisense Smart TV as a premium personal entertainment device that delivers personalized content recommendations and a tailored viewing experience, while affirmatively concealing (a) the existence and operation of continuous frame-by-frame ACR surveillance behind the misleading "Enhanced Viewing Service" label, (b) the real-time disclosure of viewing data to VIDAA, Nexxen, Roku, and Alphonso, and (c) the transfer of, and facilitation of access to, bulk consumer data by Hisense's Chinese parents and affiliates. These misrepresentations and omissions were material to Plaintiffs' purchasing decisions, and Plaintiffs reasonably relied on Hisense's representations and the absence of disclosure of these practices.

484. Plaintiffs' personal information and ACR-derived viewing data also have independent economic value in identifiable markets. Industry data confirms that consumer behavioral and viewing data has substantial and increasing per-user value—reflected in the existence of an established market in which companies (including Nielsen, UpVoice, HoneyGain,

SavvyConnect, Google, and others) compensate consumers in exchange for license to track and use specified categories of behavioral data. Plaintiffs intended to retain, and to be able to exercise, the option to monetize, license, or otherwise control the disposition of their viewing data and associated identifiers, including by participating in that established consumer-data market. Defendant's interception, exclusive licensing of VIDAA ACR data to Nexxen, and re-distribution of that data through the broader CTV advertising ecosystem deprived Plaintiffs of that option and diminished the value of the data to Plaintiffs themselves by extracting, segmenting, and monetizing it before Plaintiffs could do so, and by injecting it into proprietary identity graphs and audience segments from which Plaintiffs are excluded. Plaintiffs' personal information is further property in which they hold a present and future interest, and Defendant's unauthorized collection and disclosure of that information violated Plaintiffs' right to exclude others from it—an independent diminishment of a present or future property interest under *Kwikset*. *See Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011); *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987 (N.D. Cal. 2024); *A.B. v. Google LLC*, 737 F. Supp. 3d 869 (N.D. Cal. 2024); *Brown v. Google LLC*, 685 F. Supp. 3d 909 (N.D. Cal. 2023).

485. Plaintiffs lack an adequate remedy at law for the equitable relief they seek under the UCL. The injunctive and restitutionary relief Plaintiffs seek—including orders compelling Defendant to cease ongoing ACR collection, to disgorge profits from the past and ongoing misappropriation of bulk consumer ACR data, to delete or de-identify previously collected data, to implement clear and conspicuous disclosures and meaningful opt-out controls, and to comply with the CISA Security Requirements applicable to restricted DOJ-Rule transactions—is not available through any of Plaintiffs' legal claims, which are limited to backward-looking compensatory and statutory damages. Plaintiffs therefore satisfy *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020).

486. Each named Plaintiff continues to own and use his or her Hisense Smart TV, which remains operational and connected, such that each Plaintiff's viewing activity and associated identifiers remain subject to Defendant's ongoing, continuous ACR interception, collection,

transmission, and disclosure. Absent injunctive relief, Defendant's unlawful conduct will continue to capture and disclose Plaintiffs' Sensitive Information. Plaintiffs therefore face a real and immediate threat of continuing and future injury, and monetary damages—which can redress only past collection—cannot remedy this ongoing and prospective harm.

487. Even if any of the foregoing economic-injury allegations were deemed insufficient, Plaintiffs alternatively seek disgorgement of Defendant's ill-gotten gains under the UCL on the basis that Defendant is not entitled to retain profits that they realized from the misappropriation of Plaintiffs' personal information and audiovisual communications, irrespective of any corresponding economic loss to Plaintiffs.

488. Plaintiffs seek restitution, injunctive relief, and all other relief available under Cal. Bus. & Prof. Code § 17203.

489. Plaintiffs, on behalf of the general public, seek public injunctive relief under the UCL, Cal. Bus. & Prof. Code § 17203, enjoining Defendant from deploying, operating, or enabling Automatic Content Recognition technology that intercepts, records, or discloses the viewing activity or other personal information of California consumers without first obtaining clear, conspicuous, and separately disclosed consent. The primary purpose and effect of this relief is to prohibit unlawful acts that threaten future injury to the general public—every California consumer who now owns, later purchases, or otherwise uses a Hisense Smart TV—rather than to redress past injury to Plaintiffs or any discrete group of prior purchasers. Because Defendant continues to manufacture, sell, and operate Smart TVs that perform this surveillance, its unlawful conduct is ongoing and, absent an injunction, will continue to harm the public at large. This relief is prospective, runs to the general public, and does not require the Court to consider the individual claims of any non-party. Plaintiffs and the general public have no adequate remedy at law to secure Defendant's future compliance with California law.

COUNT XII

Violation of the Consumers Legal Remedies Act (CLRA), Cal. Civ. Code §§ 1750–1784 — Injunctive and Declaratory Relief Only

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the California Subclass; and, as to the public injunction, on behalf of the general public)

490. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

491. This Count seeks injunctive and declaratory relief only. Plaintiffs do not seek damages under the CLRA in this Count. Accordingly, the pre-suit notice and demand requirements of Cal. Civ. Code § 1782(a)–(b) do not apply, because those requirements govern only actions for damages. Cal. Civ. Code § 1782(d); Plaintiffs reserve the right to amend to add a claim for CLRA damages after serving the notice required by § 1782(a).

492. Plaintiffs and the members of the California Subclass are "consumers" within the meaning of Cal. Civ. Code § 1761(d). The Hisense Smart TVs are "goods" within the meaning of § 1761(a). Plaintiffs' purchases of Hisense Smart TVs are "transactions" within the meaning of § 1761(e). The CLRA applies to Hisense's representations and omissions made to consumers through its packaging, marketing, and on-device user interface, even where the point-of-sale transaction occurred through an authorized retailer; privity is not required. Cal. Civ. Code § 1770(a).

493. Hisense engaged in unfair and deceptive acts and practices declared unlawful by Cal. Civ. Code § 1770(a), including: (5) representing that the Hisense Smart TVs have characteristics, uses, or benefits they do not have; (7) representing that the goods are of a particular standard, quality, or grade when they are of another; (9) advertising the goods with intent not to sell them as advertised; (14) representing that the transaction confers or involves rights, remedies, or obligations it does not; and (16) representing that the goods have been supplied in accordance with a previous representation when they have not.

494. Hisense represented, through its marketing, packaging, and on-device interface, that the Hisense Smart TVs are premium personal-entertainment devices delivering personalized content and a tailored viewing experience, while concealing that the devices conduct continuous, frame-by-frame ACR surveillance of everything displayed on screen, transmit that data in real time to multiple separate third parties (VIDAA, Nexxen, Roku, Alphonso), and facilitate the transfer of bulk consumer data to Hisense's Chinese parents and affiliates in violation of the DOJ Bulk Sensitive Data Transfer Rule.

495. Hisense had a duty to disclose the foregoing facts because (a) Hisense had exclusive knowledge of the ACR architecture, data pipelines, and downstream recipients, which were not reasonably accessible to consumers; (b) Hisense actively concealed these practices through the benign-sounding "Enhanced Viewing Service" label (which does not identify ACR functionality, any third-party recipient, or continuous surveillance), through bundled multi-step setup flows, and through opt-out controls dispersed across four or more menus requiring more than 200 clicks; and (c) Hisense made partial representations about the devices' characteristics and the "Enhanced Viewing Service" that were misleading absent disclosure of the surveillance.

496. The concealed and omitted facts were material: a reasonable consumer would consider them important in deciding whether to purchase or use a Hisense Smart TV. Had Hisense disclosed these facts at the point of sale or on its packaging or device interface, Plaintiffs and California Subclass members would have been aware of them and would not have purchased their Hisense Smart TVs, or would have paid materially less. Because the omissions were material, reliance is presumed and inferred.

497. Plaintiffs have suffered "any damage" within the meaning of Cal. Civ. Code § 1780(a). Plaintiffs paid for, and overpaid for, their Hisense Smart TVs as a result of Hisense's deceptive practices, and were deprived of the benefit of their bargain and of the value of their personal information, as alleged above.

498. Hisense's unlawful practices are ongoing. Each named Plaintiff continues to own and use his or her Hisense Smart TV, which remains operational and connected, and Hisense's

ACR system continues to intercept, collect, transmit, and disclose Plaintiffs' viewing activity and associated identifiers in real time and near-real time to the present day. Plaintiffs therefore face a real and immediate threat of continuing and future injury. An injunction would redress that injury by halting Hisense's ongoing and future collection and disclosure; monetary damages, which redress only past collection, cannot.

499. Plaintiffs lack an adequate remedy at law for the prospective relief sought in this Count. Monetary damages are retrospective and compensate only for past harm; the injunction sought here is prospective and is the only remedy that can prevent Hisense's continued and future interception and disclosure of Plaintiffs' and the public's viewing data. These remedies are not interchangeable, and damages are inadequate to address the ongoing and future harm.

500. Pursuant to Cal. Civ. Code § 1780(a)(2), Plaintiffs, individually and on behalf of the California Subclass, seek an order enjoining Hisense's unlawful methods, acts, and practices, and a declaration that those practices violate the CLRA.

501. In addition, on behalf of the general public, Plaintiffs seek a public injunction under the CLRA whose primary purpose and effect is to prohibit unlawful acts that threaten future injury to the general public—every California consumer who now owns, later purchases, or otherwise uses a Hisense Smart TV—rather than to redress past injury to Plaintiffs or any discrete group of prior purchasers. This relief is prospective, runs to the general public as a whole rather than a discrete subset of similarly situated persons, and does not require the Court to consider the individual claims of any non-party.

502. Plaintiffs accordingly seek injunctive and declaratory relief requiring Hisense to:

- cease intercepting, recording, collecting, using, and disclosing consumers' viewing data through ACR technology without first obtaining valid, informed, affirmative, and standalone consent;
- obtain affirmative, informed, and standalone consent before enabling or engaging in any ACR-based data collection on its Smart TVs;

- refrain from using deceptive terminology, pre-checked defaults, or dark patterns to obtain or imply consent to ACR-based data practices;
- implement clear, conspicuous, and truthful disclosures regarding its data collection and sharing practices; and
- provide current and future users with a simple, effective, and easily accessible means to disable ACR functionality.

503. Concurrently with this Complaint, Plaintiffs file the affidavit required by Cal. Civ. Code § 1780(d) showing that this action is commenced in a proper forum.

COUNT XIII

Unjust Enrichment

(Against Defendant Hisense USA Corporation on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

504. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

505. Plaintiffs bring this claim for unjust enrichment under California law.

506. Defendant Hisense received and retained benefits at the expense of Plaintiffs and members of the Class.

507. Specifically, Hisense's received two distinct categories of benefit at Plaintiffs' expense. First, Hisense's received the consumer purchase price for the Hisense Smart TVs Plaintiffs purchased—even where the immediate point-of-sale transaction was through a retailer such as Amazon, Best Buy, Costco, Sam's Club, Target, or Walmart, the substantial economic value of the consumer purchase price flowed back to Hisense as wholesale revenue, and Hisense would not have realized that wholesale revenue but for Plaintiffs' consumer-side purchases. Second, Hisense's received—directly and through its wholly-owned ACR subsidiary VIDAA, and through its commercial relationships with Nexxen, Roku, and Alphonso—the substantial commercial benefit of the bulk ACR-derived data captured from Plaintiffs' in-home use of the Hisense Smart TV, which Defendant and its downstream partners monetized through targeted

advertising, audience segmentation, identity-graph construction, and measurement and attribution products. By 2021, the smart-TV manufacturer Vizio publicly reported that its profits from monetization of ACR-derived consumer data exceeded its profits from the sale of the televisions themselves.

508. Hisense's retention of these benefits is unjust because Defendant secured them through misrepresentation, omission, and dark-pattern consent architecture: Hisense's marketing, packaging, EULA, and on-device disclosures concealed the true nature, scope, and downstream uses of Hisense's ACR-data collection (including the deceptive "Enhanced Viewing Service" label and the omission of the Chinese-parent / DOJ-Rule data-transfer risk), and Hisense's consent architecture consisted of bundled multi-step setup flows, more than 200-click opt-out menus, and other manipulative interface design. These misrepresentations and omissions constitute the "fraud" element required for unjust enrichment under California law.

509. In the alternative, Plaintiffs seek disgorgement of Defendant's ill-gotten gains as an independent remedy. Even if any individual Plaintiff is unable to establish a corresponding economic loss, Defendant is not entitled to retain profits realized from the misappropriation of Plaintiffs' personal information and audiovisual viewing communications.

510. Plaintiffs conferred benefits on Hisense, including payment for the Smart TV and valuable data generated through Plaintiffs' use of the device.

511. Plaintiffs' viewing activity and associated data constituted valuable information that Hisense collected, analyzed, and monetized.

512. Hisense knowingly accepted and retained these benefits.

513. Hisense appreciated and understood that it was receiving valuable benefits from Plaintiffs, including access to and use of Plaintiffs' personal information.

514. Hisense obtained these benefits through its collection, use, and disclosure of Plaintiffs' viewing data via its Smart TVs and embedded ACR technology.

515. Hisense used Plaintiffs' data for commercial purposes, including advertising, analytics, profiling, and data monetization.

516. Hisense also shared or made this data available to third parties, thereby further profiting from Plaintiffs' information.

517. Hisense's retention of these benefits was unjust because it was obtained through deceptive, unlawful, and unfair conduct.

518. Hisense collected and used Plaintiffs' data without valid consent.

519. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by Hisense for that conduct was invalid. Plaintiffs incorporate by reference, as if fully set forth herein, the consent-defect allegations set forth in the section titled "HISENSE PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

520. It would be inequitable and unjust for Hisense to retain the benefits it obtained from Plaintiffs and members of the Class.

521. As a direct and proximate result of Hisense's conduct, Plaintiffs and members of the Class have suffered harm.

522. Plaintiffs seek restitution, disgorgement of all ill-gotten gains, and all other relief available under California law.

COUNT XIV

Public Injunctive Relief on Behalf of the General Public

(Against Defendant Hisense USA Corporation; and, in the alternative, Classwide Injunctive Relief on Behalf of the Nationwide Classes or the California Subclasses)

523. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein, including the public-injunction allegations set forth in their California Unfair Competition Law, Consumers Legal Remedies Act, and California constitutional privacy counts.

524. Plaintiffs bring this claim for public injunctive and declaratory relief as a remedy independently authorized by, and integral to, the substantive claims pleaded herein. Plaintiffs seek public injunctive relief under two independent and mutually reinforcing bases: (i) the Unfair Competition Law, Cal. Bus. & Prof. Code § 17203, which authorizes injunctions to restrain

unlawful, unfair, and fraudulent business practices for the protection of the general public; (ii) the California Consumers Legal Remedies Act, Cal. Civ. Code § 1780(a)(2), which authorizes an order enjoining the unlawful methods, acts, and practices declared unlawful by § 1770; and (iii) the self-executing California constitutional right to privacy, Cal. Const. art. I, § 1, for which injunctive relief is the recognized and primary remedy. To the extent the Court determines that injunctive relief is not properly pleaded as a stand-alone count, Plaintiffs incorporate the allegations of this Count into each of the foregoing substantive counts as a remedial component.

525. The UCL and the CLRA are statutes "established for a public reason" within the meaning of Cal. Civ. Code § 3513, and case law squarely holds that the statutory right to seek public injunctive relief under those consumer-protection statutes cannot be waived by private agreement and is unenforceable insofar as a predispute agreement purports to waive it in any forum.

526. The California constitutional right to privacy was adopted by voter initiative in 1974 and, as the California Supreme Court has held, is self-executing and "creates a legal and enforceable right of privacy for every Californian." *White v. Davis*, 13 Cal. 3d 757 (1975). It protects natural persons against intrusions by private entities, not merely the government. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1 (1994). Because that right was established for a public reason—to protect the privacy of all Californians, and not merely to redress the grievances of individual litigants—the right to seek prospective injunctive relief restraining its ongoing violation is a right that "cannot be contravened by a private agreement." Cal. Civ. Code § 3513.

527. Plaintiffs, on behalf of the general public, seek a public injunction under the UCL, the CLRA, and the California Constitution whose primary purpose and effect is to prohibit unlawful acts that threaten future injury to the general public—every California consumer who now owns, later purchases, or otherwise uses a Hisense Smart TV—rather than to redress past injury to Plaintiffs or any discrete group of prior purchasers. This relief is prospective, runs to the general public as a whole rather than a discrete subset of similarly situated persons, and does not require the Court to consider the individual claims of any non-party.

528. Defendant Hisense engaged in, and continues to engage in, unlawful, unfair, and deceptive acts and practices as alleged herein, including the ongoing collection, interception, recording, use, and disclosure of consumers' viewing data through its Smart TVs and embedded ACR technology.

529. This conduct threatens the general public because Hisense continues to manufacture, sell, and operate Smart TVs that perform ACR surveillance, such that members of the public who have not yet acquired a Hisense Smart TV will be subjected to the same unlawful practices upon doing so. Absent a public injunction, Hisense will continue these practices against the consuming public indefinitely.

530. Plaintiffs are themselves aggrieved Californians whose constitutional and statutory privacy rights Hisense has violated, and they face a real and immediate threat of continued and future injury, because they continue to own and use Hisense Smart TVs on which ACR functionality remains enabled or available and remain exposed to Hisense's ongoing interception and disclosure of their viewing data. As aggrieved individuals with standing, Plaintiffs may seek public injunctive relief that primarily benefits the general public without acting as private attorneys general or prosecuting the action on behalf of others.

531. Plaintiffs and the general public lack an adequate remedy at law. Monetary damages cannot redress the ongoing invasion of privacy, the continuing loss of control over personal information, or Hisense's prospective noncompliance with California law; the CLRA (§ 1780(a)(2)) authorizes injunctive relief; and under the California constitutional right to privacy, injunctive relief—not damages—is the recognized remedy, underscoring the inadequacy of any legal remedy.

532. Plaintiffs accordingly seek a public injunction requiring Hisense to:

- cease intercepting, recording, collecting, using, and disclosing consumers' viewing data through ACR technology without first obtaining valid, informed, affirmative, and standalone consent;

- obtain affirmative, informed, and standalone consent before enabling or engaging in any ACR-based data collection on its Smart TVs;
- refrain from using deceptive terminology, pre-checked defaults, or dark patterns to obtain or imply consent to ACR-based data practices;
- implement clear, conspicuous, and truthful disclosures regarding its data collection and sharing practices; and
- provide current and future users with a simple, effective, and easily accessible means to disable ACR functionality.

533. The balance of equities favors a public injunction because Hisense's practices harm the privacy of the consuming public and provide no countervailing benefit that outweighs that harm; and the public interest is served by enjoining ongoing unlawful, unfair, and deceptive conduct directed at California consumers at large.

534. In the alternative, and only to the extent the Court declines to grant public injunctive relief, Plaintiffs seek classwide injunctive relief on the substantive counts on behalf of the Nationwide Classes or, in the alternative, the California Subclasses. This alternative request is pleaded separately so as not to limit or privatize the public injunctive relief sought on behalf of the general public in the preceding paragraphs of this count.

535. Plaintiffs and the general public are therefore entitled to injunctive and declaratory relief as requested herein.

RELIEF REQUESTED

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, respectfully request the Court enter judgment in their favor and against Hisense as follows:

a. An order certifying this action as a class action, appointing Plaintiffs as class representatives and their counsel as Class Counsel under Fed. R. Civ. P. 23;

b. A public injunction, on behalf of the general public, pursuant to Cal. Bus. & Prof. Code § 17203, Article I, § 1 of the California Constitution, and Cal. Civ. Code § 1780(a)(2), enjoining Hisense from deploying, operating, or enabling ACR

technology that intercepts, records, or discloses the viewing activity or other personal information of California consumers without first obtaining clear, conspicuous, affirmative, and separately disclosed consent—the primary purpose and effect of which is to prohibit unlawful acts that threaten future injury to the general public, and which does not require adjudication of any non-party's individual claim—and specifically requiring Hisense to:

- cease intercepting, recording, collecting, using, and disclosing consumers' viewing data through ACR technology without first obtaining valid, informed, affirmative, and standalone consent;
- obtain affirmative, informed, and standalone consent before enabling or engaging in any ACR-based data collection on its Smart TVs;
- refrain from using deceptive terminology, pre-checked defaults, or dark patterns to obtain or imply consent to ACR-based data practices;
- implement clear, conspicuous, and truthful disclosures regarding its data collection and sharing practices; and
- provide current and future users with a simple, effective, and easily accessible means to disable ACR functionality;

c. Injunctive relief pursuant to Cal. Civ. Code § 1780(a)(2) and a declaration that Hisense's practices violate the CLRA;

d. In the alternative to the public injunction, and on the substantive Counts, classwide injunctive and declaratory relief on behalf of the Class enjoining the unlawful, unfair, and deceptive practices alleged herein;

e. Restitution and disgorgement of all money or property Hisense acquired through its unlawful, unfair, and fraudulent business practices, including under Cal. Bus. & Prof. Code § 17203 and Plaintiffs' unjust-enrichment claim;

f. On all Counts other than the CLRA Count, an award of damages, including actual, compensatory, general, special, incidental, consequential, nominal, and punitive damages, and statutory damages as provided by law, in amounts to be determined

at trial;

g. A declaratory judgment that Hisense's practices violate the laws alleged herein;

h. Pre- and post-judgment interest to the extent provided by law;

i. An award of reasonable attorneys' fees, litigation expenses, and costs of suit to the extent provided by law; and

j. Such other relief the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial for all claims so triable.

Dated: June 23, 2026

Respectfully submitted,

By: */s/ Andrew R. Tate*

PEIFFER WOLF CARR KANE CONWAY & WISE LLP

Andrew R. Tate*
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Tel: (314) 669-3600
atate@peifferwolf.com

Melisa A. Rosadini-Knott
(California Bar No. 316369)
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010-1923
Tel: (323) 982-4109
mrosadini@peifferwolf.com

Brandon M. Wise*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Tel: (314) 833-4825
bwise@peifferwolf.com

* *pro hac vice* granted

Counsel for Plaintiffs and the Proposed Class