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

DAVID ROSENBERG, MAE MOORE, HOLLY WINSTON, SHELBY COOPER, SHARI ETCHEBARREN, and INDIA PRICE, *individually and on behalf of all others similarly situated,* *Plaintiffs,* v. **TCL NORTH AMERICA INC,** *Defendant.*	Case No.: **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiffs David Rosenberg, Mae Moore, Holly Winston, Shelby Cooper, Shari Etchebarren, and India Price (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant TCL North America Inc ("TCL" 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. Every 500 milliseconds, in millions of American homes, a TCL Smart TV captures a fingerprint of every sound and image displayed on its screen and transmits that fingerprint, along with persistent identifiers tied to the household, the device, and the network, to a network of advertising-technology companies and—on information and belief—to TCL's Chinese state-linked corporate parents in the People's Republic of China. This case is about TCL's use of Automatic Content Recognition ("ACR") technology to engage in that conduct, the federal and California laws TCL violates by doing so, and more than five years of public regulatory and law-enforcement warnings TCL has knowingly disregarded in continuing to engage in it. Plaintiffs bring this consumer-privacy and consumer-protection class action under California and federal law, to redress Defendant's invasion of Plaintiffs' privacy and Defendant's interception, disclosure, and monetization of Plaintiffs' communications and personal information without informed consent.

2. Defendant TCL North America, Inc. is the United States operating arm of TCL Technology Group Corporation, a Chinese state-linked consumer-electronics conglomerate headquartered in Huizhou, Guangdong Province in the People's Republic of China.

3. TCL is one of the largest Smart TV manufacturers in the United States by installed base. TCL ranked No. 2 globally in television shipments in 2022 and shipped more than 29 million televisions worldwide in 2024 alone. The Texas Attorney General's December 15, 2025 enforcement Petition against TCL alleges that more than 1.09 million Texas households—

approximately 2.95 million Texans—own at least one TCL Smart TV in a single state, illustrating the scale of TCL's installed base nationwide.

4. TCL's ACR data-collection conduct is not the product of inadvertence, ignorance, or recent commercial expansion. To the contrary, TCL has knowingly continued, expanded, and deepened that conduct over more than eight years, despite a documented sequence of public regulatory, law-enforcement, and judicial warnings that put TCL squarely on notice that the conduct is unlawful.

5. In 2017, the Federal Trade Commission and the New Jersey Attorney General obtained a $2.2 million settlement from Vizio, Inc. for the same kind of undisclosed Smart TV ACR data-collection conduct alleged here. *See United States v. VIZIO, Inc.*, No. 2:17-cv-00758 (D.N.J.). In the same year, TCL began shipping TCL Roku TVs into the United States with Roku's ACR functionality enabled by default, initiating its own ACR data-collection program.

6. On December 21, 2020, in a speech at The Heritage Foundation titled "Homeland Security and the China Challenge," then-Acting Secretary of the U.S. Department of Homeland Security Chad F. Wolf publicly identified TCL by name as a Chinese-state-supported manufacturer whose Smart TVs were a national-security concern, stating that "this year it was discovered that TCL incorporated backdoors into all of its TV sets exposing users to cyber breaches and data exfiltration" and that "TCL also receives CCP state support to compete in the global electronics market, which has propelled it to the third largest television manufacturer in the world."[1] No other

[1] *See* U.S. Department of Commerce, National Institute of Standards and Technology, *CVE-2020-27403* (Nov. 10, 2020), https://nvd.nist.gov/vuln/detail/CVE-2020-27403 (NIST National Vulnerability Database technical finding that TCL Smart TVs allowed unauthorized access to device data and media files, with "any user or device connected to the adjacent network" able to "arbitrarily browse and download sensitive files"); *see also* Acting Secretary Chad F. Wolf, *Remarks as Prepared: Homeland Security and the China Challenge* (Heritage Found., Dec. 21, 2020), https://www.dhs.gov/archive/news/2020/12/21/acting-secretary-chad-f-wolf-remarks-prepared-homeland-security-and-china-challenge; Paul F. Roberts, *Update: DHS Looking Into Cyber Risk from TCL Smart TVs*, The Security Ledger (Dec. 2020), https://securityledger.com/2020/12/dhs-looking-into-cyber-risk-from-tcl-smart-tvs/; U.S. Department of Homeland Security, *Assessment of the Critical Supply Chains Supporting the U.S.*

Smart TV manufacturer received an equivalent contemporaneous public warning from a federal-cabinet-level official by name.

7. On January 5, 2023, despite the FTC/Vizio precedent and despite the December 2020 DHS warning, TCL publicly announced a research-and-development partnership with Samba TV, Inc. to develop AI-powered Smart TV features. Plaintiffs reserve the right to identify, in discovery, the specific TCL Smart TV models (if any) on which TCL has deployed the Samba TV ACR system pursuant to that partnership.

8. 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 "DOJ Rule" or "Bulk Sensitive Data Transfer Rule"), took effect. The DOJ Rule was promulgated under Executive Order 14117 to address what the U.S. government has formally determined to be an "unusual and extraordinary threat" to U.S. national security: the bulk transfer of Americans' sensitive personal data to hostile foreign regimes—including, expressly, the People's Republic of 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.

9. On December 15, 2025, the Texas Attorney General filed an Original Petition and Application for Temporary and Permanent Injunctions against TCL alleging that TCL Smart TVs "aren't just entertainment devices—they're mass surveillance systems" and that the Chinese Communist Party has access to all of the ACR data collected. That same day, the Texas Attorney General filed a parallel enforcement action against TCL's similarly situated Chinese-state-linked competitor Hisense USA Corporation, and within days obtained a "first-of-its-kind" temporary restraining order against Hisense prohibiting any further ACR-derived data collection, sale, sharing, disclosure, or transfer during the pendency of the Hisense action. In other enforcement

---

Information and Communications Technology Industry (Feb. 24, 2022), https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf.

actions, the Texas Attorney General recently obtained settlement agreements from both Samsung and LG requiring those manufacturers to implement clear and conspicuous ACR disclosures and consent screens.

10. Despite these clear signals to cease its invasion of Americans' privacy in their own homes, as of the filing of this Complaint, TCL continues to operate its ACR pipeline on millions of TCL Smart TVs in the United States, including those owned by Plaintiffs and Class Members.

11. The viewing data and persistent identifiers TCL captures from each TCL Smart TV are transmitted in real time and near-real time to a network of corporate recipients including Roku, Inc. (on TCL Smart TVs running the Roku OS); Google LLC (on TCL Smart TVs running Google TV); Amazon.com Services LLC and Amazon Advertising LLC (on TCL Smart TVs running Amazon Fire TV); and SpringServe, LLC (TCL's named ad-serving partner). Each of these recipients independently captures, processes, and uses Plaintiffs' and Class Members' intercepted communications and identifiers to construct cross-device household identity graphs, target individual consumers across devices for advertising, and resell the resulting audience products to advertisers, agencies, data brokers, and identity-resolution providers. On information and belief, the same data is, or can be, transferred to or accessed by TCL's parents and affiliates in the People's Republic of China, which under Chinese law (including Article 7 of the PRC National Intelligence Law, the PRC Cybersecurity Law, and the PRC Data Security Law) can be compelled to deliver that data to the Chinese government and the Chinese Communist Party on demand.

12. TCL's underlying business model is the same business model the FTC and the New Jersey Attorney General sanctioned in 2017: sell televisions at competitive prices and recoup margin (and generate a substantial second revenue stream) by surreptitiously monetizing the viewing behavior of the consumers who buy them. 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. TCL's ACR practices are materially identical to the practices for which Vizio was sanctioned, except that TCL operates that same business model at many times Vizio's installed-base scale and as the U.S. operating arm of a Chinese state-linked manufacturer whose ACR-

derived data may be transferred to or accessed by foreign-government recipients—a foreign-government dimension that did not exist when Vizio was sanctioned and that is now subject to the federal national-security regulatory regime described in paragraph 8 above.

13. TCL's own publicly published Privacy Notice expressly states that TCL "may transfer or allow limited access to [users'] Personal Data globally with the companies within [TCL's] corporate group" and that TCL's "corporate group entities located in China may have limited remote access to [TCL's] data centers" holding that data. TCL's Privacy Notice further identifies the data controller as TCL New Technology Co., Ltd., headquartered in Shenzhen, Guangdong Province, China (which TCL's Privacy Notice identifies as the TCL data controller for TCL websites, Smart TVs, and smart-service applications). As confirmed by the Texas Attorney General's December 15, 2025 enforcement Petition (which reproduces a screenshot of the TCL Smart TV setup screen on this point), TCL's consumer-facing Terms of Service for TCL Smart TVs sold in the United States are, on their face, governed by the laws of the People's Republic of China. Nowhere, however, does TCL disclose to consumers in California or elsewhere in the United States that, as a matter of Chinese law, TCL and its Chinese corporate-group entities can be compelled to share data collected from American consumers—including the granular ACR-derived viewing data and persistent identifiers at issue in this Complaint—with the Chinese government and the Chinese Communist Party on demand.

14. Plaintiffs are six California residents who, individually and on behalf of similarly situated consumers, bring this action to redress TCL's unlawful conduct. Each Plaintiff purchased and used a TCL Smart TV in his or her home in California, and each had his or her viewing communications and persistent identifiers ("Sensitive Information") intercepted, recorded, transmitted, and disclosed by TCL's ACR pipeline ("ACR Tools") without informed consent.

15. 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 the benefit of the bargain; (v) diminution in the

value of the Sensitive Information; (vi) statutory damages where applicable; and (vii) continued and ongoing risk to their Sensitive Information, including the foreseeable risk that the data will be transferred to or accessed by foreign-government recipients.

16. Therefore, Plaintiffs seek, on behalf of themselves and a Class of similarly situated persons, to remedy these harms and to assert claims against Defendant for invasion of privacy (intrusion upon seclusion and 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 Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710, common-law negligence, common-law breach of implied contract, violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*., common-law unjust enrichment, and prospective injunctive and declaratory relief.

II. THE PARTIES

Plaintiff David Rosenberg

17. Plaintiff David Rosenberg is a resident and citizen of Danville, California (Contra Costa County), in the San Francisco/Oakland Division of the Northern District of California.

18. Plaintiff Rosenberg purchased a TCL Smart TV (model 55Q77K) in approximately 2025, and has used it regularly since then while in his home in Danville, California. Plaintiff Rosenberg's home internet service connected to his TCL Smart TV has been provided by Xfinity and most recently, T-Mobile. The TCL Smart TV runs the Google TV operating system, in which TCL's ACR functionality is enabled by default.

19. Plaintiff Rosenberg, along with the three other adult members of his household (totaling four adults in his household), regularly uses the TCL Smart TV to access video-viewing content, including through streaming services such as Netflix, YouTube, Apple TV+, Amazon Prime Video, and Hulu, as well as through TCL's native "TCLtv+" and "TCL Channel" streaming

services. The video-viewing content Plaintiff Rosenberg selected and watched within the privacy of his home constitutes private, Sensitive Information.

20. Because Plaintiff Rosenberg's TCL Smart TV is a TCL Google TV running the Google TV operating system, the device's Google Advertising Identifier, signed-in Google account activity, application telemetry, and household and device identifiers are transmitted to Google LLC in real time and incorporated into Google's ad-tech and identity-graph systems (including Google Ads, Google Marketing Platform, and Display & Video 360) as alleged herein. The ACR-derived viewing communications captured by Plaintiff Rosenberg's TCL Smart TV at the firmware and chipset level are operated by Defendant TCL itself (and any third-party ACR provider with which TCL contracts) and are transmitted in real time to Defendant TCL, to SpringServe, to TCL's Chinese parents and affiliates, and to additional downstream ad-tech partners as alleged herein.

21. Plaintiff Rosenberg did not personally perform the installation or setup of the TCL Smart TV. Those steps were performed by Best Buy's Geek Squad service, which physically installed and initially set up the TCL Smart TV shortly after he purchased the TV. At no time was Plaintiff Rosenberg presented with, or did he knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing TCL's, Google's, or any third party's collection, interception, or use of his viewing activity or associated data.

22. Unbeknownst to Plaintiff Rosenberg, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed his Sensitive Information during his use of the TCL Smart TV (including the specific programs and content he viewed, applications he accessed, device-level identifiers, and his IP address). Plaintiff Rosenberg never authorized Defendant TCL, Google, or any other third party 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.

23. Plaintiff Rosenberg intends to continue using his TCL Smart TV in his home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Rosenberg to the same real-time interception and disclosure of his private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of his privacy rights with each viewing session.

Plaintiff Mae Moore

24. Plaintiff Mae Moore is a resident and citizen of Long Beach, California (Los Angeles County), in the Western Division of the Central District of California.

25. Plaintiff Moore purchased a TCL Smart TV (model 40S325, an S-series TCL Roku TV) in approximately 2020, and has used it regularly since then while in her home in Long Beach, California. The TCL Smart TV runs the Roku OS operating system, in which TCL's ACR functionality is enabled by default.

26. Plaintiff Moore, along with one other member of her household (totaling two people in her household), regularly uses the TCL Smart TV to access video-viewing content, including through streaming services such as Amazon Prime Video, Hulu, Apple TV, Tubi, Pluto TV, Fawesome TV, Sirius XM, ESPN, Boomerang/Cartoon Network, Paramount+, Amazon Music, and Amazon Alexa, as well as through TCL's native "TCLtv+" and "TCL Channel" streaming services. The video-viewing content Plaintiff Moore selected and watched within the privacy of her home constitutes private, Sensitive Information.

27. Because Plaintiff Moore's TCL Smart TV is a TCL 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 and Roku's broader ad-tech and identity-resolution platform as alleged herein. On information and belief, the same ACR-derived data is also transmitted to or shared with Roku's downstream ad-tech, identity-resolution, and data-broker partners (including, on information and belief, SpringServe, LLC) and, in light of TCL's Privacy Notice

acknowledgment of cross-border data transfer to its China-based corporate-group entities, to or accessible by TCL's Chinese parents and affiliates.

28. Plaintiff Moore did not personally perform the assembly, installation, or initial configuration of the TCL Smart TV. Those steps were performed by another member of her household, not by Plaintiff Moore herself. At no time was Plaintiff Moore presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing TCL's, Roku's, or any third party's collection, interception, or use of her viewing activity or associated data.

29. Unbeknownst to Plaintiff Moore, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the TCL Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Moore never authorized Defendant TCL, Roku, or any other third party 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.

30. Plaintiff Moore intends to continue using her TCL Smart TV in her home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Moore to the same real-time interception and disclosure of her private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of her privacy rights with each viewing session.

Plaintiff Holly Winston

31. Plaintiff Holly Winston is a resident and citizen of Rancho Cordova, California (Sacramento County), in the Sacramento Division of the Eastern District of California.

32. Plaintiff Winston purchased a TCL Smart TV (model 55S421, an S-series TCL Roku TV) in approximately 2022, and has used it regularly since then while in her home in Rancho Cordova, California. Plaintiff Winston's home internet service is provided by T-Mobile (T-Mobile

Home Internet). The TCL Smart TV runs the Roku OS operating system, in which TCL's ACR functionality is enabled by default.

33. Plaintiff Winston, along with the six other members of her household (totaling seven people in her household), regularly uses the TCL Smart TV to access video-viewing content, including through a variety of streaming services, as well as through TCL's native "TCLtv+" and "TCL Channel" streaming services. The video-viewing content Plaintiff Winston selected and watched within the privacy of her home constitutes private, Sensitive Information.

34. Because Plaintiff Winston's TCL Smart TV is a TCL 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 and Roku's broader ad-tech and identity-resolution platform as alleged herein. On information and belief, the same ACR-derived data is also transmitted to or shared with Roku's downstream ad-tech, identity-resolution, and data-broker partners and, in light of TCL's Privacy Notice acknowledgment of cross-border data transfer to its China-based corporate-group entities, to or accessible by TCL's Chinese parents and affiliates.

35. Plaintiff Winston (and/or another member of her household, on information and belief) performed the assembly, installation, and initial configuration of the TCL Smart TV. At no time was Plaintiff Winston presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing TCL's, Roku's, or any third party's collection, interception, or use of her viewing activity or associated data.

36. Unbeknownst to Plaintiff Winston, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the TCL Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Winston never authorized Defendant TCL, Roku, or any other third party 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.

37. Plaintiff Winston intends to continue using her TCL Smart TV in her home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Winston to the same real-time interception and disclosure of her private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of her privacy rights with each viewing session.

Plaintiff Shelby Cooper

38. Plaintiff Shelby Cooper is a resident and citizen of Riverside, California (Riverside County), in the Eastern Division of the Central District of California.

39. Plaintiff Cooper purchased a TCL Smart TV (model 98Q51CG, a 98-inch Q-series TCL Google TV) in approximately 2025, and has used it regularly since then while in her home in Riverside, California. Plaintiff Cooper's home internet service is provided by AT&T. The TCL Smart TV runs the Google TV operating system, in which TCL's ACR functionality is enabled by default.

40. Plaintiff Cooper, along with one other member of her household (totaling two people in her household), regularly uses the TCL Smart TV to access video-viewing content, including through streaming services such as Netflix, Hulu, Disney+, Peacock, and Amazon Prime Video, as well as through TCL's native "TCLtv+" and "TCL Channel" streaming services. The video-viewing content Plaintiff Cooper selected and watched within the privacy of her home constitutes private, Sensitive Information.

41. Because Plaintiff Cooper's TCL Smart TV is a TCL Google TV running the Google TV operating system, the device's Google Advertising Identifier, signed-in Google account activity, application telemetry, and household and device identifiers are transmitted to Google LLC in real time and incorporated into Google's ad-tech and identity-graph systems (including Google Ads, Google Marketing Platform, and Display & Video 360) as alleged herein. The ACR-derived viewing communications captured by Plaintiff Cooper's TCL Smart TV at the firmware and

chipset level are operated by Defendant TCL itself (and any third-party ACR provider with which TCL contracts) and are transmitted in real time to Defendant TCL, to SpringServe, to TCL's Chinese parents and affiliates, and to additional downstream ad-tech partners as alleged herein.

42. Plaintiff Cooper personally performed the assembly, installation, and initial configuration of the TCL Smart TV. At no time was Plaintiff Cooper presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing TCL's, Google's, or any third party's collection, interception, or use of her viewing activity or associated data.

43. Unbeknownst to Plaintiff Cooper, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the TCL Smart TV (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Cooper never authorized Defendant TCL, Google, or any other third party 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.

44. Plaintiff Cooper intends to continue using her TCL Smart TV in her home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Cooper to the same real-time interception and disclosure of her private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of her privacy rights with each viewing session.

Plaintiff Shari Etchebarren

45. Plaintiff Shari Etchebarren is a resident and citizen of Diamond Bar, California (Los Angeles County), in the Western Division of the Central District of California.

46. Plaintiff Etchebarren purchased a TCL Smart TV (model 50S421, an S-series TCL Roku TV) in approximately 2019, and has used it regularly since then while in her home in

Diamond Bar, California. The TCL Smart TV runs the Roku OS operating system, in which TCL's ACR functionality is enabled by default.

47. 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 TCL 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 TCL's native "TCLtv+" and "TCL Channel" streaming services. The video-viewing content Plaintiff Etchebarren selected and watched within the privacy of her home constitutes private, Sensitive Information.

48. Because Plaintiff Etchebarren's TCL Smart TV is a TCL 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 and Roku's broader ad-tech and identity-resolution platform as alleged herein. On information and belief, the same ACR-derived data is also transmitted to or shared with Roku's downstream ad-tech, identity-resolution, and data-broker partners and, in light of TCL's Privacy Notice acknowledgment of cross-border data transfer to its China-based corporate-group entities, to or accessible by TCL's Chinese parents and affiliates.

49. Plaintiff Etchebarren personally performed the assembly, installation, and initial configuration of the TCL Smart TV. 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 TCL's, Roku's, or any third party's collection, interception, or use of her viewing activity or associated data.

50. Unbeknownst to Plaintiff Etchebarren, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of the TCL 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 TCL, Roku, or any other third party 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.

51. Plaintiff Etchebarren intends to continue using her TCL Smart TV in her home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Etchebarren to the same real-time interception and disclosure of her private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of her privacy rights with each viewing session.

Plaintiff India Price

52. Plaintiff India Price is a resident and citizen of San Diego, California (San Diego County), in the Southern District of California.

53. Plaintiff Price purchased two TCL Smart TVs (model 55S421 and model 32S31, both S-series TCL Roku TVs) in approximately 2020, and has used them regularly since then while in her home in San Diego, California. Plaintiff Price's home internet service is provided by AT&T and by Cox Communications. Both of Plaintiff Price's TCL Smart TVs run the Roku OS operating system, in which TCL's ACR functionality is enabled by default.

54. Plaintiff Price, along with the six other members of her household (totaling seven people in her household), regularly uses both TCL Smart TVs to access video-viewing content, including through streaming services such as Crunchyroll, Hulu, Netflix, HIDIVE, and CBS, as well as through TCL's native "TCLtv+" and "TCL Channel" streaming services. The video-viewing content Plaintiff Price selected and watched within the privacy of her home constitutes private, Sensitive Information.

55. Because both of Plaintiff Price's TCL Smart TVs are TCL Roku TVs running the Roku OS operating system, the ACR-derived viewing communications captured by both devices are transmitted to and processed by Roku, Inc. in real time and incorporated into Roku's OneView/dataxu identity graph and Roku's broader ad-tech and identity-resolution platform as alleged herein. On information and belief, the same ACR-derived data is also transmitted to or

shared with Roku's downstream ad-tech, identity-resolution, and data-broker partners and, in light of TCL's Privacy Notice acknowledgment of cross-border data transfer to its China-based corporate-group entities, to or accessible by TCL's Chinese parents and affiliates. Plaintiff Price's exposure to the ACR data-collection conduct alleged here is intensified by the fact that two TCL Smart TVs in a single household, both used regularly by seven people, multiply the volume of viewing data, persistent identifiers, and household-level inferences captured and disclosed.

56. Plaintiff Price personally performed the assembly, installation, and initial configuration of both TCL Smart TVs. At no time was Plaintiff Price presented with, or did she knowingly agree to, any terms of use, privacy disclosures, or consent mechanisms describing or authorizing TCL's, Roku's, or any third party's collection, interception, or use of her viewing activity or associated data.

57. Unbeknownst to Plaintiff Price, TCL's ACR Tools and related tracking technologies surreptitiously intercepted, transmitted, and disclosed her Sensitive Information during her use of both TCL Smart TVs (including the specific programs and content she viewed, applications she accessed, device-level identifiers, and her IP address). Plaintiff Price never authorized Defendant TCL, Roku, or any other third party 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.

58. Plaintiff Price intends to continue using her TCL Smart TV in her home, and unless TCL is enjoined from its ongoing ACR collection, transmission, and disclosure conduct, every continued use of that television will subject Plaintiff Price to the same real-time interception and disclosure of her private viewing communications and personal identifiers complained of herein, inflicting a fresh violation of her privacy rights with each viewing session.

Defendant TCL North America Inc

59. Defendant TCL North America Inc ("TCL") is a Delaware corporation regularly transacting, soliciting, and conducting business in California, with its principal place of business

at 189 Technology Drive, Irvine, California 92618. TCL North America may be served through its registered agent for service of process in California, Cogency Global Inc. (a California Corporations Code § 1505 corporate agent), c/o Erin Haggerty or Connie Mix, 1325 J Street, Suite 1550, Sacramento, California 95814, or through its registered agent in Delaware (its state of incorporation).

60. TCL North America Inc is the principal U.S. arm of the Chinese global consumer-electronics manufacturer TCL Technology Group Corporation (and its publicly traded affiliate TCL Industries Holdings Co., Ltd.), a state-owned enterprise headquartered in Huizhou, Guangdong Province, People's Republic of China. TCL designs, manufactures, markets, distributes, and sells televisions, appliances, and other consumer electronics in the United States, including the TCL Smart TVs at issue in this Complaint. TCL designs, manufactures, markets, distributes, and sells TCL Smart TVs in the United States that incorporate ACR data-collection technology operated by TCL through its commercial relationships with third-party ad-tech and identity-resolution operators including Roku, Inc., Google LLC, Amazon.com Services LLC, and SpringServe, LLC.

III. JURISDICTION AND VENUE

61. 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.

62. 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*.

63. 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.

64. This Court has personal jurisdiction over Defendant TCL North America Inc 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 TCL 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 TCL 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.

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

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

67. 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.

68. 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.

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

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

71. Venue is proper in the San Francisco/Oakland Division of the Northern District of California pursuant to Civil Local Rule 3-2(c) and 3-2(d) because Plaintiff Rosenberg resides in Contra Costa County, used the TCL Smart TV at issue in his home located in Danville (Contra Costa County), California, and a substantial part of the conduct giving rise to his claims occurred within this Division.

IV. ARTICLE III STANDING

72. 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).

73. 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).

74. 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 TCL' 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 TCL's ACR pipeline.

75. Third, each Plaintiff has suffered economic injury, including (i) the loss of the benefit of the bargain (Plaintiffs would not have purchased their TCL 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.

76. 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.

77. 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 its own first-party conduct in designing, configuring, and operating TCL 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. TCL'S SMART TV BUSINESS

78. TCL manufactures and sells Smart TVs in the United States under the TCL Smart TV brand.

79. TCL'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.

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

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

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

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

84. This household-level surveillance allows TCL 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

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

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

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

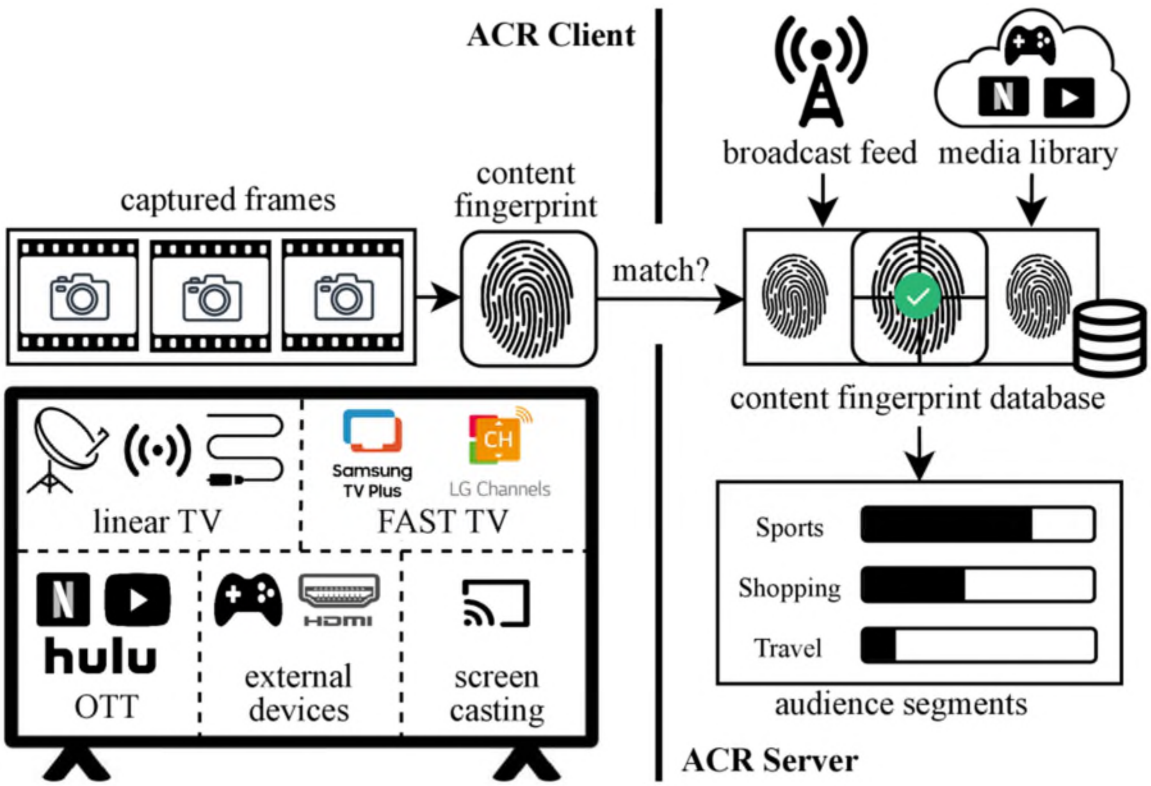

Figure 1: Overview of ACR tracking in Smart TVs

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.

88. Regulators have specifically recognized the intrusive nature of TCL's ACR practices. On December 15, 2025, the Texas Attorney General filed an Original Petition and Application for Temporary and Permanent Injunctions against TCL North America, Inc. in Williamson County, Texas, alleging that TCL Smart TVs "aren't just entertainment devices—they're mass surveillance systems" and that, through ACR technology, TCL "secretly monitors what consumers watch across streaming apps, cable, and even connected devices like gaming consoles or Blu-ray players." The Texas Attorney General's Petition 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.[2]

89. The Texas Attorney General's Petition specifically alleges that TCL 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 "Performance and Analysis Data" (Google TV) or "Smart TV Experience" / "Use Info from TV Inputs" (Roku)) 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. TCL'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."

90. The Texas Attorney General's Petition against TCL is one of a series of state and federal regulatory actions targeting the Smart TV ACR industry generally and Chinese state-linked Smart TV manufacturers in particular. In a parallel December 2025 enforcement action filed in Comal County, Texas, against TCL's primary Chinese-headquartered Smart TV competitor, Hisense USA Corporation, the Texas Attorney General secured what his office publicly described as a "first-of-its-kind" temporary restraining order prohibiting Hisense, during the pendency of the Hisense enforcement 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 Hisense order, the Texas Attorney General specifically described Hisense as a "CCP-aligned smart TV company" and emphasized that the Chinese Communist Party has access to all of the ACR data collected — conduct materially identical to the conduct alleged against TCL in this Complaint and in the Texas Attorney General's parallel TCL enforcement action. The Texas Attorney General's pattern of

---

[2] *See State of Texas v. TCL N. Am., Inc.* (Williamson Cnty. Dist. Ct. filed Dec. 15, 2025) (the "Texas Petition"), available at https://www.texasattorneygeneral.gov/sites/default/files/images/press/TCL%20TV%20Petition%20Filed.pdf.

enforcement against PRC-headquartered Smart TV manufacturers reflects an independent governmental finding that ACR-data collection and disclosure practices of TCL's type are sufficiently unlawful, deceptive, and dangerous to warrant aggressive injunctive relief.[3]

91. Notably, in a separate enforcement action, the Texas Attorney General 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."[4] Shortly thereafter, the Texas Attorney General secured a similar agreement from LG.[5]

92. 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. TCL's ACR practices are materially the same as the practices for which Vizio was sanctioned, and TCL's business model—selling

---

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

[4] Press Release, Off. of the Tex. Att'y Gen., *Attorney General Paxton Secures Major Agreement With Samsung To Ensure Texans Are Protected With Smart TVs*, available at https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-secures-major-agreement-samsung-ensure-texans-are-protected-smart-tvs.

[5] Press Release, Off. of the Tex. Att'y Gen., *Attorney General Ken Paxton Secures Major Agreement With LG To Protect Texans' Privacy And Stop Their Data From Being Sold*, available at https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-major-agreement-lg-protect-texans-privacy-and-stop-data-being.

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. TCL'S ACR SURVEILLANCE PROGRAM

93. TCL has incorporated ACR technology into its Smart TVs since at least 2017, when it began shipping TCL Roku TVs with Roku's ACR functionality enabled by default. On January 5, 2023, TCL publicly announced a research-and-development partnership with Samba TV, Inc. for AI-powered Smart TV features.

94. TCL implements this ACR functionality through ACR firmware operated by Defendant TCL itself (and any third-party ACR provider with which TCL contracts) on TCL Smart TVs across all three Smart TV operating systems on which TCL ships its Smart TVs in the United States. TCL Smart TVs ship with one of three operating systems—Google TV, Roku OS, or Amazon Fire TV. On TCL Roku TVs, ACR fingerprinting (covering content from antenna, HDMI inputs, and applications) is additionally performed by Roku at the operating-system level pursuant to Roku's publicly admitted "Smart TV Experience" ACR program. On TCL Fire TVs, ACR fingerprinting (covering content from, at a minimum, antenna and Fire TV applications) is additionally performed by Amazon at the operating-system level pursuant to Amazon's publicly admitted Fire TV ACR program. On TCL Google TVs, the Google TV operating system does not perform operating-system-level ACR fingerprinting; instead, TCL Google TVs are configured by TCL to transmit to Google, in real time, the device's Google Advertising Identifier, signed-in Google account activity, application telemetry, and household and device identifiers, which Google incorporates into its identity- and audience-resolution infrastructure. Across all three operating-system variants, the ACR-derived viewing data captured at the firmware level by Defendant TCL (and any third-party ACR provider with which TCL contracts) is transmitted in real time to Defendant TCL itself and to Defendant's downstream ad-tech and identity-resolution partners, including SpringServe, each of which in turn shares data with its further commercial partners.

95. Within TCL Smart TVs, this ACR functionality is presented to consumers during device setup and in subsequent menus under benign-sounding labels such as "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs"—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.

96. TCL describes this feature as providing personalization, recommendations, or enhanced viewing experiences.

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

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

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

100. 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.

101. TCL aggregates this data to create household-level viewing profiles.

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

VIII. TCL'S COLLECTION OF HIGHLY SENSITIVE VIEWING DATA

103. The viewing information captured through TCL's ACR system is highly sensitive and revealing.

104. 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.

105. TCL aggregates this viewing data into consumer profiles used for targeted advertising and behavioral segmentation.

106. 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.

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

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

109. The Sensitive Information collected and derived through TCL's ACR data-collection conduct alleged in this Complaint thus includes, but is not limited to: (i) the specific audiovisual content displayed on Plaintiffs' and Class Members' TCL Smart TVs, including the programs, episodes, advertisements, applications, and external-input content (e.g., from HDMI-connected gaming consoles, Blu-ray players, streaming sticks, and personal computers) viewed; (ii) device-level and network identifiers tied to those TCL Smart TVs, including IP address, MAC address, advertising identifier, household identifier, and operating-system identifier; (iii) cross-device identifiers and linkages associating those TCL Smart TVs with other devices used in the same household or by the same individual user (including smartphones, tablets, and computers); (iv) timestamped logs of viewing activity and device usage; and (v) inferences drawn from the foregoing, including inferences regarding consumers' interests, habits, preferences, household composition, demographics, lifestyle, and other personal characteristics.

IX. ROKU'S ACR AND IDENTITY-GRAPH BUSINESS ON TCL ROKU TVS

110. Roku, Inc. is a publicly traded U.S. company headquartered in San Jose, California, that operates the Roku OS smart-television operating system and the Roku ad-tech and identity-resolution platform. TCL has shipped TCL Smart TVs running the Roku OS as one of its principal Smart TV product lines since at least 2014, making TCL one of Roku's longest-running and largest OEM partners.

111. Roku has integrated automatic-content-recognition technology into TCL Roku TVs since at least 2017. Roku's ACR system is enabled by default on TCL Roku TVs and operates through the Roku OS and Roku-supplied components on the device. Roku's ACR system captures audiovisual content displayed on the television screen, generates fingerprints of that content, and transmits the fingerprints, together with persistent identifiers, to Roku-controlled servers in real time.

112. Roku ingests the resulting ACR data into its identity-graph and ad-tech platform, which Roku publicly markets under product names including "OneView" (Roku's demand-side platform, formerly dataxu) and the Roku Audience Network. Roku assigns and maintains a persistent unique identifier called the Roku Advertising Identifier ("RIDA") for each Roku-powered device. Roku uses RIDA, IP address, MAC address, and other persistent identifiers to construct cross-device household identity graphs that link TCL Roku TVs to other devices used in the same household, including smartphones, tablets, and computers.

113. Roku monetizes the resulting ACR-derived data and identity-graph outputs through targeted advertising, audience products, and licensing arrangements with brands, agencies, ad-tech intermediaries, and data brokers. Roku's commercial model is publicly described, including in Roku's filings with the U.S. Securities and Exchange Commission, as built around monetizing user-level viewing data, advertising-identifier data, and cross-device identity-graph products that originate, in substantial part, from ACR data captured on Roku-powered Smart TVs, including TCL Roku TVs.

X. GOOGLE'S AND AMAZON'S AD-TECH AND IDENTITY-RESOLUTION SYSTEMS ON TCL GOOGLE TVS AND TCL FIRE TVS

114. TCL Smart TVs running the Google TV operating system are configured by TCL to integrate with Google's ad-tech and identity-resolution systems, including Google Ads, Google Marketing Platform, Display & Video 360, and Google's cross-device identity graph. As configured by TCL, TCL Google TVs transmit to Google, in real time and on a continuous basis during device use, the device's Google Advertising Identifier, signed-in Google account activity, application telemetry (including which applications are launched, the duration of in-app sessions, the search and recommendation queries entered into the Google TV launcher, and on-device interaction events), and household and device identifiers, which Google incorporates into its identity- and audience-resolution infrastructure, enabling Google to target individual users and households across devices and contexts. The ACR fingerprinting captured from TCL Google TVs at the firmware and chipset level is operated by Defendant TCL itself (and any third-party ACR provider with which TCL contracts) and is transmitted in real time to Defendant TCL and to Defendant's downstream ad-tech and identity-resolution partners, including SpringServe.

115. TCL Smart TVs running the Amazon Fire TV operating system are configured by TCL to enable Amazon's ad-tech and identity-resolution systems, including Amazon DSP, Amazon Marketing Cloud, Amazon Publisher Services, and Amazon Ads. Amazon publicly admits that the Fire TV operating system performs automatic content recognition by capturing audio and pixel fingerprints of audiovisual content displayed on TCL Fire TVs from over-the-air broadcast sources and from Fire TV applications (including third-party streaming applications), matching those fingerprints against Amazon-controlled content databases, and incorporating the resulting viewing data, together with the device's Amazon Advertising Identifier, signed-in Amazon account activity, and household and device identifiers, into Amazon's cross-device identity-resolution infrastructure, enabling Amazon to target individual users and households across devices and contexts. ACR fingerprinting captured from TCL Fire TVs at the firmware and chipset level outside the scope of Amazon's admitted Fire TV ACR (including audiovisual content

received via HDMI inputs from cable boxes, satellite boxes, gaming consoles, and other external sources) is operated by Defendant TCL itself (and any third-party ACR provider with which TCL contracts) and is transmitted in real time to Defendant TCL and to Defendant's downstream ad-tech and identity-resolution partners, including SpringServe.

XI. TCL'S INTEGRATED ACR SURVEILLANCE ARCHITECTURE

116. TCL's Smart TVs and the operating-system-level ad-tech and identity-resolution platforms of Roku, Google, and Amazon (and, where integrated, Samba TV) operate together as an integrated surveillance and advertising architecture designed to capture, identify, and monetize consumers' in-home viewing activity.

117. Upon receipt, Roku (for TCL Roku TVs) and Amazon (for TCL Fire TVs, within the scope of Amazon's admitted Fire TV ACR) each independently match the captured ACR fingerprints to identify viewed content and associate that information with device- and household-level identifiers, including IP address, MAC address, advertising identifier, and operator-specific household identifier. Defendant TCL (and any third-party ACR provider with which TCL contracts) likewise matches ACR fingerprints captured from TCL Smart TVs across all three operating-system variants (including content captured outside the scope of Roku's and Amazon's ACR coverage and content captured from TCL Google TVs) and associates that information with the same categories of identifiers, transmitting the resulting viewing data to TCL-controlled servers and to Defendant's downstream ad-tech and identity-resolution partners. Google (for TCL Google TVs) receives, in real time, the device's advertising identifier, signed-in account activity, application telemetry, and household and device identifiers, which Google associates with its account- and device-level identity graph. The ACR transmissions and associated identifier transmissions include content- and identifier-derived information sufficient to identify the specific programs, advertisements, or audiovisual material viewed by Plaintiffs and Class Members and to attribute that viewing activity to particular households and devices in real time or near-real time.

118. Each of those operators integrates the captured ACR data into broader identity-resolution systems that link TCL Smart TVs to other devices associated with the same household

or user, including smartphones, tablets, and computers, using deterministic and probabilistic matching techniques and identifiers obtained from third-party identity-resolution providers (such as LiveRamp), and demand-side and supply-side platforms.

119. 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.

120. The TCL Smart TV serves as a primary data-collection endpoint—and the anchor of this identity-resolution architecture—capturing viewing activity from the "first screen" in the home. 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 the operating-system-specific operator (Roku, Google, or Amazon) 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 Roku, Google, Amazon, SpringServe, and other downstream ad-tech, identity-graph, data-broker, and measurement partners as alleged herein.

121. 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 performed a black-box audit of the ACR network traffic generated by Samsung and LG Smart TVs (LG Smart TVs use the Alphonso ACR system, now part of LG Ad Solutions; Samsung Smart TVs use Samsung's in-house ACR system). The researchers confirmed that ACR-enabled Smart TVs continuously capture content displayed on the screen, generate fingerprints of that content, 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). They further

found that ACR transmissions occurred even when the Smart TV was used as a “dumb” HDMI display for laptops, gaming consoles, and other personal devices, and that opting out of ACR features through the Smart TV’s privacy menus stopped (or substantially reduced) network traffic to ACR-vendor servers. *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; see also Ramon Lobato, Automated content recognition (ACR), smart TVs, and ad-tech infrastructure, Convergence: The International Journal of Research into New Media Technologies (July 15, 2025) (peer-reviewed academic study documenting the integration of ACR into the Samsung, LG, and Vizio Smart TV ad-tech ecosystems and tracing the development of the same ACR-as-ad-tech business model across the broader Smart TV industry). Although the Anselmi audit was scoped to Samsung and LG Smart TVs, the architectural pattern it documents (continuous on-device fingerprint generation; transmission to vendor-controlled servers; input-source-agnostic capture, including for HDMI sources) is the same architectural pattern that Defendant TCL itself, Roku (on TCL Roku TVs), and Amazon (within Amazon’s admitted Fire TV ACR scope on TCL Fire TVs) (and, where integrated into specific TCL Smart TV models, Samba TV) employ. On information and belief, TCL Smart TVs transmit ACR fingerprints and associated identifiers to TCL-, Roku-, Amazon-, and SpringServe-controlled server endpoints in real time and near-real time during use, in materially the same manner as documented by Anselmi for Samsung and LG. Plaintiffs reserve the right to identify the specific endpoints in discovery.

XII. TCL’S CORPORATE TIES TO THE PEOPLE’S REPUBLIC OF CHINA AND UNDISCLOSED DATA-TRANSFER OBLIGATIONS

122. TCL’s ACR surveillance is not merely a domestic privacy problem. TCL is, at its corporate core, a Chinese state-owned enterprise under the control of the Huizhou municipal government in the People’s Republic of China (“PRC”).

123. The ultimate parent corporations of Defendant include TCL Technology Group Corporation and TCL Industries Holdings Co., Ltd., partially state-owned holding companies

headquartered in Huizhou, Guangdong Province, China, whose shares are held, directly and indirectly, by the Huizhou municipal government (through Huizhou Investment Holding Ltd. and other state-affiliated investment vehicles) and by other Chinese government and Chinese-state-affiliated entities. TCL Technology Group Corporation's founder, current chairman, Li Dongsheng ("Li") (who served as the company's CEO until January 2026, when he was succeeded by Wang Cheng), is a member of the Chinese Communist Party. Under PRC "Company Law" (1993, as amended), all PRC enterprises with three or more CCP-member employees are required to form CCP cells, branches, or committees composed of company employees; as of 2021, all PRC enterprises with 50 or more employees are required to form Party cells regardless of CCP-member headcount. As one of the largest PRC enterprises (and the corporate parent of Defendant), TCL Technology Group Corporation falls within these requirements. On information and belief, TCL Technology Group's internal Party-affiliated corporate-governance structure exercises operational influence over TCL's data-handling decisions, including the design, configuration, and ongoing operational support of TCL's ACR data-collection apparatus; TCL's selection of downstream data-recipient partners; the structure and routing of TCL's cross-border data transfers; and the data-handling relationship between TCL North America's United States operations and TCL's Chinese parents and affiliates. In addition, TCL Technology Group has received substantial PRC central- and provincial-government subsidies to support its global expansion in the consumer-electronics market, including, on information and belief and based on contemporaneous Bloomberg and other public reporting: approximately 552 million yuan in subsidies from the municipality of Shenzhen as of 2010 (consisting of 210 million yuan that year on top of 342 million yuan previously); more than $2 billion in PRC government aid in 2013; and approximately $1 billion in additional PRC government aid earmarked for TCL in 2015.

124. 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." The 2021 PRC Data Security Law imposes parallel obligations on

PRC data handlers: Article 29 requires PRC enterprises to inform PRC authorities of data breaches and vulnerabilities, and Article 35 obligates PRC enterprises to cooperate with PRC public-security and national-security authorities by "providing data access" "for the purpose of safeguarding national security and investigating crimes." In practical effect, TCL and its corporate parents and affiliates can be compelled to turn over any data they hold—including data collected from TCL Smart TVs in the United States—to the Chinese government and the Chinese Communist Party on demand.

125. The U.S. Department of Homeland Security has specifically flagged TCL Smart TVs as presenting national-security concerns. In December 2020, public reporting based on federal-government sources, including DHS, disclosed that TCL Smart TVs had been identified as a vector for undisclosed data collection and transmission, and that TCL's Smart TVs contained software functionality that posed national-security and consumer-privacy risks. The DHS-sourced public reporting expressly named TCL as a Chinese-state-linked manufacturer whose Smart TVs were being used in ways that could be exploited for foreign-intelligence purposes—a public warning that no other major U.S. Smart TV manufacturer has received from the federal government. That December 2020 DHS-sourced warning predated, and is materially consistent with, the Texas Attorney General's December 2025 enforcement action against TCL described above and the academic ACR forensics described below.

126. TCL's own publicly published Privacy Notice expressly states that TCL "may transfer or allow limited access to [users'] Personal Data globally with the companies within [TCL's] corporate group" and that TCL's "corporate group entities located in China may have limited remote access to [TCL's] data centers" holding that data. TCL's consumer-facing Terms of Service for TCL Smart TVs sold in the United States are, on their face, governed by the laws of the People's Republic of China, as demonstrated by the TCL Smart TV setup screen cited by the Texas Attorney General's enforcement Petition:

(E) if we decide to discontinue any part of the TCL Smart Services or replace it with an alternative service; and/or

(F) for any other reasons with 30 days' prior notice subject to applicable laws.

Unless otherwise specified in these Terms, termination will not affect rights, obligations and liabilities accrued before the date of termination.

12. **Governing Law and Jurisdiction**

12.1 These Terms are governed by the laws of the People's Republic of China (excluding the laws of Hong Kong SAR, Macao SAR and Taiwan) **(China)**, except as otherwise provided by any mandatory applicable law in your jurisdiction, in which case the governing law in relation to all or particular rights and obligations of the parties shall be the laws of your usual place of residence.

12.2 The United Nations Convention on the International Sale of Goods is specifically excluded from application to these Terms.

12.3 To the extent permitted by applicable law, in the event of a dispute arising out of or in connection with your use of TCL Smart Services, TCL and you shall attempt, promptly and in good faith, to resolve any such dispute. In the event that no resolution can be concluded within 30 days from the date when such dispute has first been raised by either party, either party shall have the right to submit the dispute (which may be contractual or non-contractual) to **the competent courts of China as the exclusive dispute resolution venue**, unless applicable mandatory consumer protection laws in your jurisdiction prohibits from conferring such jurisdiction in which case the court of your usual place of residence will apply to such disputes related to these Terms. This does not affect your right to start proceedings to protect your legal position.

12.4 If you are a citizen of any European Union member states, after prior written request to TCL, you may also submit any claims on the dispute resolution platform by the European Commission at the following address: https://ec.europa.eu/info/live-work-travel-eu/consumers/resolve-your-consumer-complaint_en. The European Commission will transfer your claim to the notified competent national

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

128. Nor does TCL disclose that every image and sound captured by ACR on a TCL 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.

129. The combination of (i) TCL's continuous, frame-by-frame ACR capture of audiovisual content within the home, (ii) TCL's aggregation of that data with persistent and cross-device identifiers, (iii) TCL's status as a Chinese state-owned enterprise, and (iv) TCL's express acknowledgment in its publicly published Privacy Notice that TCL may transfer or allow access to user data by its Chinese corporate-group entities, and TCL's consumer-facing Terms of Service' choice of Chinese law as the law governing those terms, 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.

130. Reasonable consumers, including Plaintiff, would consider it material to their decision to purchase or use a TCL 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 Plaintiff known these facts, she would not have purchased the TCL Smart TV, or would have paid substantially less for it.

131. TCL'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.

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

132. 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.

133. 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.

134. "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.

135. The TCL 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 TCL Smart TVs feed Defendant's ACR pipeline, plainly meets the "bulk" threshold under 28 C.F.R. § 202.205.

136. 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. TCL holds, on information and belief, approximately 14% of the U.S. Smart TV installed base. TCL 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 TCL's share of those households translates to multiple millions of U.S. households running TCL Smart TVs at any given time. The Texas Attorney General has alleged that approximately 1.09 million Texas households alone own TCL Smart TVs, equivalent to approximately 2.95 million Texans (assuming a 2.7-person average household)—in a single state. TCL'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 TCL's ACR system collects and disseminates is bulk U.S. sensitive personal data within the meaning of 28 C.F.R. § 202.206.

137. Defendant TCL North America Inc 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.

138. TCL's ultimate corporate parents and affiliates—including TCL Technology Group Corporation and TCL Industries Holdings Co., Ltd., each headquartered in Huizhou, Guangdong Province, People's Republic of China and majority-owned and controlled, directly and indirectly, by the Huizhou 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.

139. TCL's own publicly published Privacy Notice acknowledges that TCL "may transfer or allow limited access to personal data globally with companies within its corporate group," including "TCL's corporate group entities located in China," and identifies the data controller as TCL New Technology Co., Ltd., headquartered in Shenzhen, China (the TCL data controller TCL identifies in its Privacy Notice for TCL websites, Smart TVs, and smart-service applications). TCL's consumer-facing Terms of Service for TCL Smart TVs sold in the United States are, on their face, governed by the laws of the People's Republic of China. Together, those TCL-published disclosures 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—TCL'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.

140. TCL North America 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. TCL

North America Inc 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.

141. 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.

142. 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). TCL'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.

XIV. TCL'S REAL-TIME AND NEAR-REAL-TIME DISCLOSURE OF ACR DATA TO ROKU, GOOGLE, AMAZON, SPRINGSERVE, AND OTHER DOWNSTREAM AD-TECH PARTNERS

143. Roku. TCL's portfolio includes TCL Smart TVs configured with Roku's Roku OS operating system (commonly marketed as "TCL Roku TVs"). On information and belief, Roku, Inc. (a Delaware corporation headquartered in San Jose, California) operates its own ACR pipeline on TCL 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."

144. Roku's receipt and use of ACR data from TCL Roku TVs makes Roku a separate, third-party recipient of consumers' viewing communications, distinct from TCL North America Inc. TCL's manufacture, sale, configuration, software updates, and ongoing operational support of TCL 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.

145. Google. TCL North America Inc has, since at least 2017, configured certain TCL Smart TVs to ship with the Google TV operating system, which integrates Google's ad-tech and identity-graph systems by default. Google operates one of the largest ad-tech and identity-resolution systems in the world, including Google Ads, Google Marketing Platform, and Display & Video 360. As configured by TCL, TCL Google TVs transmit to Google, in real time and on a continuous basis, the device's Google Advertising Identifier, signed-in Google account activity, application telemetry (including which applications are launched, the duration of in-app sessions, the search and recommendation queries entered into the Google TV launcher, and on-device interaction events), and household and device identifiers, which Google associates with its account- and device-level identity graph and uses to target individual users and households across devices and contexts. Google is a separate corporate person whose contemporaneous receipt and processing of consumers' viewing-related communications and identifying data TCL aids, agrees with, employs, and conspires with within the meaning of CIPA § 631(a) and the federal Wiretap Act.

146. Amazon (Fire TV). TCL's portfolio also includes TCL Smart TVs configured with Amazon's Fire TV smart-TV operating system (commonly marketed as "TCL Fire TVs" or "TCL 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 TCL 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.

147. Amazon's receipt and use of ACR data from TCL Fire TVs makes Amazon a separate, third-party recipient of consumers' viewing communications, distinct from TCL North America Inc. TCL's manufacture, sale, configuration, software updates, and ongoing operational support of TCL Fire TVs—which TCL 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.

148. Other ad-tech, data-broker, identity-resolution, and measurement partners. On information and belief, TCL'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.

XV. TCL'S MARKETING AND REPRESENTATIONS REGARDING SMART TV FUNCTIONALITY AND PRIVACY

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

150. In its marketing materials and user-facing disclosures, TCL represents that features such as "Smart TV Experience" or "personalized recommendations" enhance the user experience by tailoring content suggestions to the viewer.

151. TCL promotes these features as tools that help users discover content, enhance viewing, and personalize their entertainment experience.

152. 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.

153. TCL 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.

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

155. TCL 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.

156. To the extent TCL 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.

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

158. Reasonable consumers, including Plaintiff, 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.

159. Had Plaintiff known the true nature and scope of TCL's data collection and sharing practices, she would not have purchased the TCL Smart TV or would have paid substantially less for it.

XVI. TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN.

160. TCL does not meaningfully disclose its ACR surveillance practices to consumers.

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

162. For example, TCL labels the ACR feature "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs," terminology that does not convey that the feature enables continuous monitoring of television viewing.

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

164. Most consumers click "Agree" simply to complete the setup process and begin using the television.

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

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

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

168. 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.

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

170. As a result, millions of consumers have unknowingly enabled TCL's ACR surveillance.

XVII. TCL PROFITS FROM ITS SURVEILLANCE OF CONSUMERS.

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

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

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

173. The data collected through TCL'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.

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

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

176. Through these practices, TCL 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.

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

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

178. 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.

179. 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."[6]

180. 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.

181. 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 SavvyConnect are all companies that pay for browsing history information.

182. If given the choice, each Plaintiff could have sold or licensed their valuable Sensitive Information to TCL or its partners for monetary compensation, but they were not given that choice. By contrast, TCL obtained Plaintiffs' and Class Members' Sensitive Information without compensation and without informed consent, while retaining the full economic benefit of that data.

183. 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.

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

---

[6] 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).

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

A. The Video Privacy Protection Act (VPPA)

185. 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).

186. 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).

187. 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.[7]

188. 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).

---

[7] *See also The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY, SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW (Jan. 31, 2012), *available online at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-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.").

189. 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).

190. 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).

191. TCL 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 TCL's own video content offerings, including TCL TV Plus.

192. As alleged herein, TCL, 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.

193. 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.

194. TCL makes these disclosures to third parties, including advertising and analytics partners, for commercial purposes, including targeted advertising, audience segmentation, and measurement.

195. TCL 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.

196. 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")

197. TCL represents its Smart TVs and associated features, including "Smart TV Experience" and similar functionality, as tools designed to enhance the user experience through personalization and content recommendations.

198. These representations are materially misleading because TCL 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.

199. TCL 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.

XIX. CLASS ALLEGATIONS

200. 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 TCL 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 TCL Smart TV on which ACR technology was enabled and that captured, analyzed, or transmitted information regarding audiovisual content displayed on the device.

Nationwide Roku Identity Graph Class: All natural persons in the United States whose viewing activity on a TCL Smart TV was used by Defendant TCL 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 TCL Smart TVs configured with the Roku OS operating system (commonly marketed as "TCL Roku TVs").

California Roku Identity Graph Subclass: All natural persons in California whose viewing activity on a TCL Smart TV was used by Defendant TCL 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 TCL Smart TVs configured with the Roku OS operating system (commonly marketed as "TCL Roku TVs").

Nationwide Google Identity Graph Class: All natural persons in the United States whose viewing activity on a TCL Smart TV was used by Defendant TCL and/or Google LLC, 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 Google Ads / Google Marketing Platform / Display & Video 360 advertising-resolution systems operated by Google using the device's Google Advertising Identifier, signed-in Google account activity, application telemetry, household and device identifiers, and (where applicable) ACR-derived data obtained from TCL Smart TVs configured with the Google TV operating system (commonly marketed as "TCL Google TVs").

California Google Identity Graph Subclass: All natural persons in California whose viewing activity on a TCL Smart TV was used by Defendant TCL and/or Google LLC, 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 Google Ads / Google Marketing Platform / Display & Video 360 advertising-resolution systems operated by Google using the device's Google Advertising Identifier, signed-in Google account activity, application telemetry, household and device identifiers, and (where applicable) ACR-derived data obtained from TCL Smart TVs configured with the Google TV operating system (commonly marketed as "TCL Google TVs").

Nationwide Amazon Identity Graph Class: All natural persons in the United States whose viewing activity on a TCL Smart TV was used by Defendant TCL 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 TCL Smart TVs configured with the Amazon Fire TV operating system (commonly marketed as "TCL Fire TVs").

California Amazon Identity Graph Subclass: All natural persons in California whose viewing activity on a TCL Smart TV was used by Defendant TCL 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 TCL Smart TVs configured with the Amazon Fire TV operating system (commonly marketed as "TCL Fire TVs").

201. The Nationwide ACR Class and the three Nationwide Identity Graph Classes (the Nationwide Roku, Google, and Amazon Identity Graph Classes) are collectively referred to as the "Nationwide Classes." The California ACR Subclass and the three California Identity Graph Subclasses (the California Roku, Google, 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 three 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 three identity-graph systems.

202. 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.

203. 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 TCL ACR data in discovery.

204. **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.

205. **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.

206. **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.

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

208. **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.

209. **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.

210. 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.

211. 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 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.

212. 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.

XX. TOLLING AND ESTOPPEL

213. 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 TCL Smart TVs.

214. The ACR systems on TCL 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 Roku, Google, Amazon, SpringServe, TCL's Chinese parents and affiliates, or any other downstream recipient.

215. Defendant had exclusive knowledge that TCL 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 Roku, Google, Amazon, SpringServe, and TCL's Chinese parents and affiliates), and to facilitate access to that data by TCL'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.

216. 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 "Smart TV Experience" or "Performance and Analysis Data" or "Use Info from TV Inputs" (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; (c) the dispersion of opt-out controls across four or more separate menus requiring more than 200 clicks; and (d) the divergence between the End User Terms of Use and Privacy Policy currently in effect for TCL Smart TVs sold in the United States, which obscured the practices in operation at the time of each Plaintiff's purchase.

217. Under these circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection, use, and disclosure of users' Sensitive Information. To date, Defendant has not fully disclosed or acknowledged the extent to which it captured, identified, and transmitted users' viewing activity and associated identifiers to third parties such as Roku, Google, Amazon, SpringServe, and TCL's Chinese parents and affiliates.

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

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

220. 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 TCL North America, Inc. in Williamson County, Texas, alleging in detail the existence, scope, and operation of TCL'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, TCL's specific ACR practices, TCL's specific third-party-disclosure pipelines, TCL's specific deceptive labeling and dark-pattern consent architecture, or TCL's specific data-transfer relationships with its Chinese parents and affiliates.

221. Although prior reports suggested that certain smart televisions collected viewing data, those generic reports did not reveal the nature, scope, or recipients of TCL's specific ACR-based interceptions. Defendant did not disclose that TCL 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 Roku, Google, Amazon, and SpringServe, or that the resulting bulk data was transferred or facilitated for access to TCL'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.

222. Defendant may contend that Plaintiffs were on inquiry notice based on (i) TCL'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; (v) the 2017 putative class action *White v. LG Electronics*; (vi) the Federal Trade Commission and New Jersey Attorney General's 2017 settlement with Vizio for similar Smart TV ACR conduct; (vii) then-Acting DHS Secretary Chad F. Wolf's December 21, 2020 Heritage Foundation speech identifying TCL by name as a national-security concern; (viii) the April 8, 2025 effective date of the DOJ Bulk

Sensitive Data Transfer Rule; or (ix) the Texas Attorney General's December 15, 2025 enforcement Petition against TCL; (x) the December 12, 2023 Markup investigation entitled "Your Smart TV Knows What You're Watching" (Mohamed Al Elew & Gabriel Hongsdusit); or (xi) the June 25, 2025 New York Times Wirecutter article entitled "Yes, Your TV Is Probably Spying on You. Your Fridge, Too." (Cericola, Chase, & Neikirk). None of those sources put a reasonable TCL Smart TV owner on inquiry notice of the specific conduct alleged here. TCL's own disclosures used misleading terminology (including "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs," 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 TCL, did not name TCL, did not identify TCL's specific ACR vendors (Roku, Google, Amazon, or SpringServe), and did not disclose TCL's transfer of bulk TCL 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). The 2017 FTC—Vizio settlement involved a different manufacturer and did not identify TCL, TCL's ACR vendors, or TCL's data-transfer relationships with its Chinese parents and affiliates. The December 2020 DHS Wolf warning, while a federal-cabinet-level public statement that TCL Smart TVs were a national-security concern, did not disclose to consumers TCL's specific ACR data-collection apparatus, the identities of TCL's downstream third-party recipients, the specific Chinese-government-access risks at issue here, or any consumer cause of action against TCL—and Defendant's subsequent decision to deepen its ACR exposure (rather than dismantle it) in January 2023 in fact compounded, rather than dispelled, the very secrecy this Court should now refuse to credit. The DOJ Rule's effective date concerns federal enforcement against bulk-data transfers and did not disclose, and was not reasonably understood by consumers as disclosing, TCL's specific consumer-facing privacy violations. The Markup and New York Times Wirecutter articles, like the earlier consumer-press coverage, did not name TCL specifically, did not identify TCL's specific ACR vendors or third-party data recipients, did not disclose TCL's transfer of ACR-derived data to its Chinese state-affiliated parents and affiliates in violation of the DOJ Bulk Sensitive Data Transfer Rule, and in any event post-date the purchases by Plaintiffs Etchebarren (2019), Moore (2020), and Winston (2022) and the limitations period for at least some Plaintiffs and Class Members. Each of items (vi)—(xi) above either named a different defendant, addressed a different legal theory, post-dated the relevant limitations period for at least some Plaintiffs and Class Members, or some combination of the foregoing, and none was a "storm warning" of consumer-side liability sufficient to commence the limitations period as a matter of California or federal law.

223. Beyond the discovery rule and equitable estoppel, Defendant's continuing course of conduct independently tolls the applicable limitations periods. TCL'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 TCL Smart TV in operation, every time a Plaintiff or Class Member turns on a TCL Smart TV, every time a Plaintiff or Class Member watches content on a TCL Smart TV, and continuously in the background during ordinary household use, to the present day. Each new audiovisual fingerprint captured (every 500 milliseconds, in real time), each new transmission of that fingerprint and associated persistent identifiers to Defendant TCL, Roku, Amazon (within Amazon's admitted Fire TV ACR scope), SpringServe, or any other downstream recipient (and, with respect to TCL Google TVs, each new transmission of the device's Google Advertising Identifier, signed-in account activity, application telemetry, and household and device identifiers to Google), and each new re-disclosure or re-use of that data by Defendant or its downstream partners, is an independent and separately actionable 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).

XXI. CLAIMS FOR RELIEF

COUNT I

Invasion of Privacy – Intrusion Upon Seclusion

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

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

225. Plaintiffs bring this claim under California common law.

226. 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.

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

228. Defendant TCL, through its Smart TVs and embedded ACR technology, intentionally intruded upon Plaintiffs' and Class Members' private affairs.

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

230. TCL'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.

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

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

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

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

235. Defendant's third-party ad-tech partners (Roku, Google, Amazon, and SpringServe) 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 those partners to track Plaintiffs' and Class Members' viewing activity as it occurred.

236. In connection with this conduct, those third-party recipients 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, and used these identifiers, together with additional data obtained from third-party partners (including identity-resolution providers and data brokers), to associate Plaintiffs' and Class Members' Smart TV activity with other devices and identities.

237. Through these practices, Defendant's third-party ad-tech partners 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. Those identity graphs and related systems enabled the partners 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.

238. Through this aggregation and profiling, those third-party recipients were 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, and to use these profiles to create audience segments, enable targeted advertising, and facilitate cross-device tracking, and to disclose or make the resulting information available to other ad-tech partners, advertisers, data brokers, and identity-resolution providers for commercial purposes.

239. 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.

240. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

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

242. 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.

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

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

245. 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 TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

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

247. Plaintiffs bring this claim under California common law.

248. 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.

249. Defendant TCL, through its Smart TVs and embedded ACR technology, collected and disclosed private, Sensitive Information concerning Plaintiffs' viewing behavior.

250. Specifically, TCL 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.

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

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

253. 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 Roku, Google, Amazon, and SpringServe, 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).

254. 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 (Roku, Google, Amazon, SpringServe, TCL's Chinese parents and affiliates) and, through Roku's, Google's, Amazon's, and SpringServe'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 *Harris v. iHeartMedia, Inc.*, 2026 WL 247875, at *1–2.

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

256. TCL disclosed this private, Sensitive Information to third parties, including advertisers, analytics providers, and other commercial entities.

257. Defendant's third-party ad-tech partners (Roku, Google, Amazon, and SpringServe) 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, those partners 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.

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

259. Those third-party recipients 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 by re-distributing 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.

260. Upon information and belief, TCL 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.

261. TCL'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.

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

263. TCL's disclosures were made without Plaintiffs' consent.

264. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

265. TCL also failed to adequately disclose the scope and nature of the information being disclosed.

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

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

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

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

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

271. TCL's conduct therefore constitutes a public disclosure of private facts.

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

273. 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 TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

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

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

277. 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.

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

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

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

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

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

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

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

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

286. TCL thereby monitored Plaintiffs' viewing activity across all inputs and sources.

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

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

289. TCL's conduct constituted a serious invasion of Plaintiffs' privacy.

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

291. TCL's conduct enabled the collection of detailed and Sensitive Information about Plaintiffs' private life.

292. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

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

294. 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.

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

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

297. TCL's conduct therefore violated Plaintiffs' right to privacy under the California Constitution.

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

299. 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.

COUNT IV

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

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

301. 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."

302. Defendant is a person under CIPA § 631.

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

304. Defendant TCL—directed from and within California—through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including Roku, Inc., Google LLC, Amazon.com Services LLC, and SpringServe, LLC—to intercept Plaintiffs' communications while they were in transit.

305. Specifically, TCL 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.

306. 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.

307. 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.

308. More specifically, TCL'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. TCL's ACR software (developed and operated through Defendant's relationships with Roku, Inc., Google LLC, Amazon.com Services LLC, and SpringServe, LLC) generates content-identifying digital "fingerprints" on the TCL 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.

309. Once transmitted, the fingerprints are matched in real time or near-real time against TCL-, Roku-, Amazon-, or SpringServe-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 TCL 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 (Roku, Amazon, and SpringServe) incorporate the identified content into household-level audience segments, identity-graph nodes, and real-time bidding inventories before the consumer finishes watching the content—and that Google likewise incorporates the identifier-, account-, and application-telemetry data it receives from TCL Google TVs into household-level audience segments, identity-graph nodes, and real-time bidding inventories on the same contemporaneous basis—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).

310. Accordingly, TCL'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).

311. 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.

312. TCL knowingly aided, agreed with, employed, and conspired with each of multiple separate third parties—including Roku, Inc. (with respect to TCL Smart TVs configured with the Roku OS operating system); Google LLC (with respect to TCL Smart TVs configured with the Google TV operating system); Amazon.com Services LLC and Amazon Advertising LLC (with respect to TCL Smart TVs configured with the Amazon Fire TV operating system); SpringServe, LLC; 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. TCL's status as a party to certain of those communications therefore does not shield it from liability, because TCL's conduct falls within the "aids, agrees with, employs, or conspires with any person or persons" clause of § 631(a). TCL's aiding was undertaken knowingly and intentionally, with full awareness that Roku, Google, Amazon, SpringServe, 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. TCL 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 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.

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

314. TCL 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.

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

316. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

317. Because CIPA requires the consent of all parties to a communication, the real-time and near-real-time interception of communications by TCL's third-party partners—including Roku, Inc., Google LLC, Amazon.com Services LLC and Amazon Advertising LLC, SpringServe, LLC, and additional downstream demand-side platforms, supply-side platforms, identity-resolution providers, and measurement and attribution providers—was unlawful.

318. 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 TCL.

319. TCL's conduct constitutes an egregious invasion of privacy and a violation of California law.

320. As a direct and proximate result of TCL'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.

321. 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 TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

323. 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.

324. At all relevant times, Plaintiffs and members of the Class engaged in communications through their use of TCL Smart TVs, including audiovisual transmissions

delivered through streaming applications, broadcast signals, and external devices connected via HDMI.

325. Defendant TCL, through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including Roku, Inc., Google LLC, Amazon.com Services LLC, and SpringServe, LLC—to eavesdrop upon and record Plaintiffs' confidential communications.

326. Specifically, TCL 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.

327. TCL 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.

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

329. 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 TCL.

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

331. TCL 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.

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

333. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

334. Because CIPA requires the consent of all parties to a communication, the recording of communications by TCL's third-party partners—including Roku, Google, Amazon, and SpringServe—was unlawful.

335. 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 TCL.

336. TCL's conduct constitutes an egregious invasion of privacy and a violation of California law.

337. As a direct and proximate result of TCL'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.

338. 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 VI

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

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

340. 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.

341. 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.

342. 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.

343. 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.

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

345. 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.

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

347. Specifically, TCL'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.

348. 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.

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

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

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

352. TCL'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.

353. TCL installed and used these devices and processes without obtaining a court order or lawful authorization.

354. TCL also installed and used these devices and processes without the consent of Plaintiffs and members of the Class.

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

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

357. TCL obscured the nature of its data collection through misleading terminology, including labeling its surveillance features as "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs."

358. Defendant TCL, through its Smart TVs and embedded ACR technology, enabled, facilitated, and caused third parties—including Roku, Inc., Google LLC, Amazon.com Services

LLC, and SpringServe, LLC—to eavesdrop upon and record Plaintiffs' confidential communications.

359. Specifically, TCL 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.

360. TCL 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.

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

362. 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 TCL.

363. TCL's conduct constitutes an egregious invasion of privacy and a violation of California law.

364. As a direct and proximate result of TCL'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.

365. 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 TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

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

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

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

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

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

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

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

374. TCL'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.

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

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

377. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

378. As a direct and proximate result of TCL'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.

379. TCL's conduct was knowing, intentional, and wrongful.

380. *Pleading expressly in the alternative to Plaintiffs' invasion of privacy claims*, 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 Roku,

Google, Amazon, and SpringServe (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).

381. 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 TCL 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 (Roku, Google, Amazon, and SpringServe) without authorization.

382. 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 TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes)

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

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

385. 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.

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

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

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

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

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

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

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

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

394. TCL'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.

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

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

397. TCL's conduct was intentional.

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

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

400. Even if TCL 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 TCL intercepted such communications for the purpose of committing tortious and unlawful acts.

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

402. TCL'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).

403. TCL'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).

404. The crime-tort exception to § 2511(2)(d) is independently satisfied by TCL'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, TCL North America, Inc. is a "U.S. person" under the DOJ Rule, 28 C.F.R. § 202.256, and TCL's Chinese parents and affiliates—including TCL Technology Group Corporation and TCL Industries Holdings Co., Ltd.—are "covered persons" under the DOJ Rule, 28 C.F.R. § 202.211. The TCL 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 TCL Smart TVs feed Defendant's ACR pipeline, plainly meets the "bulk" threshold under 28 C.F.R. § 202.205. TCL'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.

405. TCL's violation of the DOJ Rule is willful. TCL 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. TCL 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.

406. 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). TCL’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).

407. TCL’s real-time and near-real-time disclosure of intercepted communications and associated identifiers to multiple separate third-party recipients—including Roku, Inc. (with respect to TCL Smart TVs configured with the Roku OS operating system), Google LLC (with respect to TCL Smart TVs configured with the Google TV operating system), Amazon.com Services LLC and Amazon Advertising LLC (with respect to TCL Smart TVs configured with the Amazon Fire TV operating system), SpringServe, LLC, and additional downstream demand-side platforms, supply-side platforms, identity-resolution providers, and measurement and attribution providers—further confirms that, even if TCL were deemed a “party” to certain of those communications, TCL 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.

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

409. TCL’s disclosures further obscured the nature of its surveillance through misleading terminology, including labeling its ACR features as “Performance and Analysis Data” or “Smart TV Experience” / “Use Info from TV Inputs.”

410. TCL 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 TCL would intercept, record, analyze, and monetize the content of their communications.

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

412. As a direct and proximate result of TCL'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.

413. 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 TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes)

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

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

416. 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.

417. Defendant TCL 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.

418. More specifically, TCL 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) TCL markets, distributes, and operates the "TCLtv+" (a/k/a "TCL Channel" or "TCL Channel Channels") streaming-video service that is pre-installed and prominently featured on TCL Smart

TVs, including a curated catalog of advertising-supported video content delivered to consumers directly by TCL; (ii) TCL's Smart TV home screens and content-discovery rails curate and surface specific audiovisual content from TCL-controlled video sources to the consumer; and (iii) TCL makes available to consumers an integrated platform through which audiovisual content is delivered. TCL's video-content-delivery business constitutes a substantial focus of Defendant's work.

419. Plaintiffs are "consumers" under 18 U.S.C. § 2710(a)(1) because each Plaintiff is, at minimum, a "subscriber" of TCL's video goods or services. Each Plaintiff registered their TCL Smart TV with TCL on initial device setup; each Plaintiff provided personal information to TCL in connection with that registration; and each Plaintiff has accessed audiovisual content delivered through TCL's integrated streaming services. These commitments and exchanges of value satisfy the "subscriber" definition.

420. The information TCL has knowingly disclosed constitutes "personally identifiable information" under 18 U.S.C. § 2710(a)(3) and the "ordinary person" test. Specifically, TCL has disclosed to Roku, Google, Amazon, SpringServe, and other downstream recipients—in real time and near-real time, in transmissions transmitted from each Plaintiff's TCL 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, and TCL account 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 Roku, Google, Amazon, and SpringServe construct identity-graph profiles, target consumers across devices, and measure advertising attribution at the household and individual level.

421. Each Plaintiff was a "consumer" within the meaning of 18 U.S.C. § 2710(a)(1), as Plaintiffs used TCL's Smart TV services to obtain video content.

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

423. Specifically, TCL 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.

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

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

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

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

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

429. The information disclosed by TCL therefore constituted "personally identifiable information" within the meaning of the VPPA.

430. TCL made these disclosures knowingly.

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

432. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

433. TCL also failed to disclose the scope, nature, and purpose of such disclosures.

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

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

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

437. As a direct and proximate result of TCL'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.

438. 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 TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

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

440. Plaintiffs bring this claim under California common law and, if necessary, in the alternative to Plaintiffs' counts for intentional torts and statutory violations.

441. At all relevant times, Defendant TCL 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.

442. 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 TCL 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.

443. 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.

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

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

446. TCL 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.

447. TCL 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.

448. TCL 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.

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

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

451. Plaintiffs and members of the Class did not consent to TCL's conduct.

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

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

454. As a direct and proximate result of TCL'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.

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

COUNT XI

Breach of Implied Contract

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

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

457. Plaintiffs bring this claim under California common law.

458. At all relevant times, Plaintiffs and Defendant TCL entered into implied contracts under which TCL agreed to provide Smart TVs and related services in exchange for Plaintiffs' payment and use of the devices.

459. The implied contract between each Plaintiff and TCL is established by, inter alia, the following TCL-specific conduct constituting offer and acceptance: (a) TCL's marketing materials, advertising, packaging, on-device branding, and on-screen user-interface representations that the TCL Smart TV is a premium personal entertainment device for in-home use, with personalization features designed to enhance the user's viewing experience; (b) TCL's End User Terms of Use and Privacy Policy currently in effect for TCL Smart TVs sold in the United States, which is presented to the consumer directly by TCL (not by the retailer) during initial device setup and which the consumer must accept by clicking "Agree" before being permitted to use the TCL Smart TV; (c) TCL's continuing post-sale interactions with Plaintiffs, including over-the-air firmware and software updates pushed by TCL to Plaintiffs' devices, TCL-account registration prompts, customer-support touchpoints, and the on-device Google TV / Roku OS / Amazon Fire TV application stores curated and configured by TCL; and (d) the TCL-direct registration of each Plaintiff's Smart TV on TCL's servers as a precondition for accessing core Smart TV functionality.

460. Each Plaintiff accepted that implied offer by purchasing a TCL Smart TV (with the consumer purchase price flowing in substantial part to TCL as wholesale revenue, even where the immediate point-of-sale transaction was through a retailer), by registering the device with TCL's servers, and by using the device in their home in the manner contemplated by TCL's marketing

and disclosures. The implied contract included reciprocal terms reflecting the reasonable expectations of an ordinary TCL Smart TV consumer, including: (i) TCL would provide a Smart TV that delivered the marketed personal entertainment functionality; (ii) TCL would not collect, intercept, transmit, or re-distribute consumers' in-home audiovisual viewing data, and associated household-level and cross-device identifiers, beyond what was reasonably necessary to provide the core Smart TV functionality; (iii) TCL would make accurate, complete, and meaningful disclosures of any data-collection practices that did exceed those reasonable expectations; and (iv) TCL would not facilitate the transfer of consumers' bulk sensitive personal data to a foreign adversary in violation of federal national-security law.

461. These implied contracts included an understanding that TCL would not collect, access, use, or disclose Plaintiffs' personal information—including detailed viewing activity—beyond what was necessary to provide the core functionality of the Smart TV, and would do so only with adequate disclosure and authorization.

462. Plaintiffs reasonably expected that TCL would not surreptitiously monitor, record, or monetize the audiovisual content displayed on Plaintiffs' television.

463. Plaintiffs further reasonably expected that TCL would not share or make available such information to third parties without clear and informed consent.

464. In exchange for these promises, Plaintiffs provided valuable consideration, including payment for the Smart TV and the provision of access to data generated through use of the device.

465. TCL accepted and retained this consideration.

466. TCL breached the implied contract by, among other things:

- collecting detailed information about Plaintiffs' viewing activity through ACR technology;
- continuously monitoring audiovisual content displayed on Plaintiffs' television;
- accessing and extracting data from Plaintiffs' Smart TV for purposes unrelated to core device functionality;

- using Plaintiffs' data for advertising, analytics, and profiling purposes; and
- disclosing or making available Plaintiffs' viewing information to third parties.

467. TCL's conduct exceeded the scope of any reasonable expectations arising from its relationship with Plaintiffs.

468. TCL did not adequately disclose these practices or obtain valid authorization from Plaintiffs.

469. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

470. As a direct and proximate result of TCL's breach, Plaintiffs and members of the Class have suffered damages, including the loss of the benefit of their bargain and the unauthorized use and exploitation of their personal information.

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

COUNT XII

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

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the California Subclasses)

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

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

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

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

Unlawful Prong

476. TCL'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*.).

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

Unfair Prong

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

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

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

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

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

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

484. TCL collected, analyzed, and monetized detailed information about Plaintiffs' viewing activity.

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

486. TCL's conduct therefore constituted an unfair business practice.

Fraudulent Prong

487. TCL's conduct was fraudulent because it was likely to deceive reasonable consumers.

488. TCL misrepresented and omitted material facts regarding its data collection and surveillance practices.

489. TCL used misleading terminology, including labeling its ACR features as "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs," which did not disclose that the feature enabled continuous monitoring of on-screen content.

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

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

492. TCL presented disclosures during a forced, multi-step setup process that pressured consumers (or third parties who set up the TV) to agree to all terms in order to use the television.

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

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

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

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

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

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

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

500. Plaintiffs and members of the Class have suffered injury in fact and lost money or property as a direct result of TCL's unfair, unlawful, and fraudulent business practices. Specifically, Plaintiffs paid for their TCL Smart TVs (with the consumer purchase price flowing in substantial part to TCL 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 TCL 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) TCL's continuous, frame-by-frame ACR surveillance, (ii) TCL's real-time and near-real-time disclosure of consumers' viewing communications and identifiers to multiple separate third parties (Roku, Google, Amazon, SpringServe), and (iii) TCL's transfer of, and facilitation of access to, that data by TCL'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).

501. TCL's misrepresentations and material omissions are precisely the kind that satisfy the UCL "fraudulent" prong: TCL's marketing materials, packaging, and on-device disclosures portray the TCL 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 "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs" labels, (b) the real-time disclosure of viewing data to Roku, Google, Amazon, and SpringServe, and (c) the transfer of, and facilitation of access to, bulk consumer data by TCL's Chinese parents and affiliates. These misrepresentations and omissions were material to Plaintiffs' purchasing decisions, and Plaintiffs reasonably relied on TCL's representations and the absence of disclosure of these practices.

502. 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 have been deprived of the ability to license, monetize, or otherwise control their viewing data through that market because Defendant's interception of Plaintiffs' viewing data and the re-distribution of that data through the broader CTV advertising ecosystem have already extracted, segmented, and monetized that data without Plaintiffs' consent. *See Brown v. Google LLC*, 2021 WL 6064009, at *15 (N.D. Cal. Dec. 22, 2021).

503. 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).

504. 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.

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

COUNT XIII

Unjust Enrichment

(Against Defendant TCL North America Inc on Behalf of Plaintiffs and the Nationwide Classes, or in the alternative, the California Subclasses)

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

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

508. Defendant TCL received and retained benefits at the expense of Plaintiffs and members of the Class.

509. Specifically, TCL received two distinct categories of benefit at Plaintiffs' expense. First, TCL received the consumer purchase price for the TCL 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 TCL as wholesale revenue, and TCL would not have realized that wholesale revenue but for Plaintiffs' consumer-side purchases. Second, TCL received—directly and through its commercial relationships with Roku, Google, Amazon, and SpringServe—the substantial commercial benefit of the bulk ACR-derived data captured from Plaintiffs' in-home use of the TCL 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.

510. TCL's retention of these benefits is unjust because Defendant secured them through misrepresentation, omission, and dark-pattern consent architecture: TCL's marketing, packaging, EULA, and on-device disclosures concealed the true nature, scope, and downstream uses of TCL's ACR-data collection (including the deceptive "Performance and Analysis Data" or "Smart TV Experience" / "Use Info from TV Inputs" labels and the omission of the Chinese-parent / DOJ-Rule data-transfer risk), and TCL's consent architecture obtained Plaintiffs' ostensible

"agreement" (or that of third parties who set up the TV) through 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.

511. In the alternative, Plaintiffs seek disgorgement of Defendant's ill-gotten gains as an independent remedy. Even if any individual Plaintiffs are 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.

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

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

514. TCL knowingly accepted and retained these benefits.

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

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

517. TCL used Plaintiffs' data for commercial purposes, including advertising, analytics, profiling, and data monetization.

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

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

520. TCL collected and used Plaintiffs' data without valid consent.

521. Plaintiffs and members of the Class did not consent to the conduct alleged in this Count, and any consent purportedly obtained by TCL 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 "TCL PURPORTS TO OBTAIN—BUT DOES NOT OBTAIN—CONSUMER CONSENT THROUGH DECEPTIVE DESIGN" above.

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

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

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

COUNT XIV

Injunctive Relief

(Against Defendant TCL North America Inc on Behalf of Plaintiffs, the Nationwide Classes, or in the alternative, the California Subclasses)

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

526. Plaintiffs bring this claim for injunctive and declaratory relief as a remedy that is independently authorized by, and integral to, each of the substantive statutory and common-law claims pleaded herein. Specifically, Plaintiffs seek injunctive relief under (i) Cal. Bus. & Prof. Code § 17203 (UCL), (ii) Cal. Penal Code § 637.2 (CIPA), (iii) Cal. Penal Code § 502(e)(1) (CDAFA), (iv) 18 U.S.C. § 2520(b)(1) (federal Wiretap Act), (v) 18 U.S.C. § 2710(c)(2)(D) (VPPA), and (vi) the Court's equitable powers in connection with Plaintiffs' common-law privacy, negligence, breach-of-implied-contract, and unjust-enrichment claims. To the extent the Court determines that injunctive relief is not properly pleaded as a stand-alone count, Plaintiffs incorporate the injunctive-relief allegations of this Count into each of the foregoing substantive counts as a remedial component.

527. Defendant TCL engaged in, and continues to engage in, unlawful, unfair, and deceptive acts and practices as alleged herein.

528. TCL's conduct included the ongoing collection, interception, recording, use, and disclosure of Plaintiffs' and Class Members' viewing data through its Smart TVs and embedded ACR technology.

529. Absent injunctive relief, TCL will continue to engage in the unlawful and deceptive practices described herein.

530. Plaintiffs and members of the Class face a real and immediate threat of continued injury, as TCL's Smart TVs continue to operate with ACR functionality enabled or available.

531. Plaintiffs lack an adequate remedy at law because monetary damages alone cannot fully compensate for the ongoing invasion of privacy and loss of control over personal information.

532. Plaintiffs seek injunctive relief requiring TCL to, among other things:

- cease intercepting, recording, collecting, using, and disclosing viewing data without valid, informed, and express consent;
- implement clear, conspicuous, and truthful disclosures regarding its data collection and sharing practices;
- obtain affirmative, informed, and standalone consent before engaging in ACR-based data collection;
- provide users with a simple, effective, and easily accessible mechanism to disable ACR functionality;
- delete or permanently de-identify previously collected viewing data associated with Plaintiffs and Class Members; and
- refrain from using deceptive terminology or dark patterns in connection with its data practices.

533. The balance of equities favors granting injunctive relief because TCL's practices harm consumers' privacy rights and provide no countervailing benefit that outweighs that harm.

534. The public interest would be served by enjoining TCL's unlawful, unfair, and deceptive conduct.

535. Plaintiffs and members of the Class are therefore entitled to injunctive and declaratory relief as requested herein.

536. To the extent that this Court finds that Plaintiffs' request for injunctive relief is not properly pleaded as a stand-alone count, Plaintiffs hereby incorporate this request for injunctive relief into their prayer for relief, below.

RELIEF REQUESTED

WHEREFORE, Plaintiffs respectfully request the Court enter judgment in their favor and against TCL as follows:

a. An award of damages, including actual, statutory, compensatory, general, special, incidental, consequential, punitive damages, disgorgement, and restitution, in an amount to be determined at trial;

b. Injunctive, declaratory, and other equitable relief as is appropriate;

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

d. Attorneys' fees to the extent provided by law;

e. Costs to the extent provided by law; and

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

JURY TRIAL DEMAND

Plaintiffs demand a jury trial for all claims so triable.

Dated: May 15, 2026

Respectfully submitted,

By: *<u>/s/ Melisa A. Rosadini-Knott</u>*

PEIFFER WOLF CARR
KANE CONWAY & WISE LLP

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

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

Counsel for Plaintiffs and the Proposed Class