Eugene Y. Turin (SB # 342413)
MCGUIRE LAW, P.C.
10089 Willowcreek Road, Suite 200
San Diego, CA 92131
Tel: (312) 893-7002 Ex. 3
Fax: 312-275-7895
eturin@mcgpc.com

Counsel for Plaintiffs and the Putative Class Members

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN BERNARDINO

E.A.R.R. & E.A.R., by and through their Guardian LYNETTE GONZALEZ, individually and on behalf of similarly situated individuals,

Plaintiffs,

v.

ROKU, INC., a Delaware corporation,

Defendant.

Case No. CIVSS2505433

CLASS ACTION COMPLAINT

1. **Violation of the Electronic Communications Privacy Act, 18. U.S.C. § 2510 *et seq.*;**
2. **Violations of California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.***

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiffs E.A.R.R. and E.A.R., minors, by and through their Guardian Lynette Gonzalez (collectively "Plaintiffs") bring this Class Action Complaint against Defendant Roku, Inc. ("Defendant" or "Roku"), to stop Defendant's unlawful tracking and disclosure of children's statutorily protected information from its streaming service and to seek redress for all those who have been harmed by Defendant's misconduct. In particular, Defendant shares and allows third parties to track children's personal information such as, video viewing data, location data, IP

addresses and voice recordings (hereinafter referred to as "Personal Information") without first obtaining the valid consent required under the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq.* Plaintiffs allege as follows based on their individual personal knowledge, acts, and experiences and as to all other matters, on information and belief, including an investigation by their attorneys.

NATURE OF THE CASE

1. This is a class action suit brought against Defendant for privacy violations pursuant to the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, in which it is liable for its underlying violations of COPPA, and the California Invasion of Privacy Act ("CIPA"), Cal. Pen. Code. § 630, *et seq*.

2. Roku is the number one television content platform in the United States, reaching nearly 145 million people.[1] By offering devices and smart TVs that run its proprietary Roku OS, Roku has created a pervasive presence in homes across the nation, including those in California. With that footprint, Roku capitalizes on the collection and monetization of vast quantities of user data, including highly sensitive Personal Information.

3. A substantial number of Roku users are children. Roku's platform offers a large library of programming aimed at minor viewers available via The Roku Channel and countless third-party channels. These programs are readily accessible not only through shared household TVs but also via personal tablets and mobile devices used by children (collectively the "Roku Platforms"). Despite representing itself as privacy-conscious, Roku collects, processes, discloses, and aids third parties in the tracking of sensitive Personal Information from children, including voice recordings, location data, IP addresses, and browsing histories.

4. Roku's platform design fails to distinguish between children and adult

[1] https://en.wikipedia.org/wiki/Roku#:~:text=As%20of%202024%2C%20Roku%20is,reaching%20nearly%20145%20million%20people.

users. Unlike its competitors, Roku does not offer user profiles that allow for age-based restrictions or parental controls capable of limiting data collection. This design ensures that children navigate the same interface and are exposed to the same third-party data trackers and behavioral advertising tools as adults.

5. Roku knowingly permits third-party advertisers and content providers to collect and track children's data through its Platform. It partners with entities that have faced regulatory scrutiny, including data brokers previously cited by the FTC for tracking individuals' precise geolocation. By cultivating an environment that favors minimal data safeguards, Roku boosts engagement with children's content, attracts advertisers, and drives up revenue.

6. Plaintiffs and other minor child Roku users, as well as their parents, thought they were communicating with Defendant, however, unbeknownst to them, Roku's illicit data practices and tracking results in the transmission and interception of Plaintiffs' sensitive data to third parties.

7. Accordingly, Plaintiffs bring this class action for legal and equitable remedies to redress and put a stop to Defendant's practices of illegally collecting, and knowingly disclosing and aiding the interception of its children users' statutorily protected information to third-parties.

JURISDICTION AND VENUE

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

9. This Court has personal jurisdiction over Defendant because a substantial part of the events giving rise to the claims asserted herein occurred in this County, as Plaintiffs reside in this County and were subject to Defendant's unlawful conduct in this County.

10. Venue is proper within this judicial district as the acts from which this dispute arose occurred within this judicial district.

PARTIES

11. Minor Plaintiffs E.A.R.R. and E.A.R. and their Guardian Lynette Gonzalez, are natural persons and residents of California.

12. Defendant Roku, Inc. is a Delaware corporation headquartered in San Jose, California.

COMMON FACTUAL ALLEGATIONS

13. Roku operates one of the most widely used television content platforms in the nation, integrating its Roku OS into both standalone devices and smart televisions. Its services span across The Roku Channel and extensive third-party channel marketplaces, including streaming apps such as Netflix or Hulu.

14. Roku's platform has expanded beyond televisions, allowing users to access The Roku Channel and its other services on a computer, tablet, or mobile device.

15. By purchasing Roku OS enabled devices, users gain access to a variety of programming. Notably, Roku offers all of its users access to The Roku Channel, an ad supported streaming service. Roku also offers ad-free premium streaming subscriptions through The Roku Channel.

16. The Roku Channel offers children's programming under the label "Kids and Family on The Roku Channel." As demonstrated by its name, most of the content on the Kids and Family section of The Roku Channel is intended to be consumed by children.

17. Roku knows that a significant portion of its userbase consists of children and advertises its Kids and Family on The Roku Channel as containing thousands of free kids' shows and movies.[2]

18. In addition to its own content, Roku also delivers content aimed at

[2] https://channelstore.roku.com/details/1e8d1835d430a48f2f60f3684cd952ac:9c466f4f485451066b3c289b8f709baa/kids-and-family-on-the-roku-channel

children viewers through a wide variety of third-party channels that offer programming and games. Such third-party channels are accessible in Roku's Channel Store under the heading "Kids & Family" and includes some of the same content available on The Roku Channel.

19. Roku also aggregates content in sections it calls "Roku Zones," which are selections of children's specific programming and games. Roku Zones are presented on the Roku platform pages and also populate when users search for child-directed content.

20. Thus, there is a variety of children specific content available on The Roku Channel.

21. Critically, parents or adults are not required to be present for children to consume Roku's children's content. All of Roku's children's content is available on any Roku Platform. Competing services use separate adult and child profiles to enable the implementation of parental controls, restrict access to age-inappropriate content, and obtain parental consent before collecting personal information from minors. For example, Google TV prompts parents to authorize data collection when setting up a child's profile. However, Roku has deliberately chosen not to implement such features which allows the company to apply its most aggressive data collection practices toward its child users.

22. Its refusal to offer child-specific user profiles not only enables the tracking of children's Personal Information, but also ensures that children are targeted with advertisements based on that data. As a result, Roku delivers behavioral ads to children just as it does to its adult users.

23. Roku fails to implement industry standard children's profiles because it knows that implementing such profiles would prevent it from collecting, and allowing third parties to track, the Personal Information of its child viewers in the manner described throughout this complaint.

24. For example, when children access content on the Kids and Family page, Roku collects their interaction driven Personal Information. In addition, Roku allows, aids, and abets third parties to track the Personal Information of child users viewing content on its platform.

25. Thus, Roku has failed to segregate its data practices between children and adults, as well as between the children's content and adult content channels, in order to monetize the sensitive Personal Information of children.

26. In fact, Roku has acknowledged that advertising and data collection regulations with respect to children's programming pose a threat to its business. In its 2023 SEC Form 10-K, the company wrote, "Finally, there is political or regulatory pressure in some countries to limit streaming TV advertising (including limiting the advertising that may be associated with children's content) or impose local content requirements on streaming TV services, which could pose a threat to our services."[3] The company went on to acknowledge that it "could be at risk for violation or alleged violation of . . . privacy, advertising, children's online protection, or similar laws."[4]

27. Because of its nature as an ad supported streaming service, Roku's business is driven on user data, including the significant amount of data collected from child users. Thus, because Roku has certain children specific sections of its platform, Roku ensures that it monetizes the Personal Information of its child users. Roku then turns and uses that Personal Information for targeted advertising delivered across its Roku Platforms and services, as well as shares, discloses, sells, and aids and abets in the collection of, its children users' data to third-parties.

28. Specifically, a live data-traffic analysis performed by Plaintiffs' expert shows that Defendant subjects its child users to its illicit data practices where it aids

---

[3] Roku 2023 SEC Form 10-K at 16 (chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://image.roku.com/c3VwcG9ydC1B/Roku-Inc-2023-Annual-Report.pdf).

[4] *Id*. at 42.

and abets in the interception of data by third-party advertising trackers whose technologies Roku has installed on its Roku Platforms.

29. For example, Roku deploys tracking technology from companies including Google, LinkedIn, Facebook, YouTube, Display & Video 360, CJ Affiliate, New Relic, and Innovid.

30. To further illustrate the technical details of the unlawful conduct at issue, one of the tracking technologies implemented by Roku and listed above is New Relic. New Relic is an advertising and internet tracking company whose cookie exists on the Roku Platforms. New Relic receives information from Roku users when they view content available on the Kids and Family on The Roku Channel, including a URL containing the specific title of the movie the user is watching alongside personal identifiers.

31. New Relic has even designed software specifically for the Roku Channels in the "New Relic Roku observability agent" which acknowledges that it offers "[c]ustomer journey tracking" so that channels may "[f]ollow customers as they navigate the application towards their content."[5]

32. Similarly, Innovid is another advertising and analytics company whose cookie exists on the Roku Platforms. Innovid receives information from Roku users when they view content available on the Kids and Family on The Roku Channel, including Personal Information in the form of identifiers, as well as precise geolocation data.

33. Google's cookie also operates in the same manner. When a user interacts with the Roku Platforms to view children's content, Google receives URL information that identifies the title of the children's video content requested, along with personal identifiers, such as Client ID, User ID, and a browser fingerprint.

34. The Meta Pixel is also another tracking pixel installed on The Roku

[5] https://newrelic.com/instant-observability/roku

Channel. The Meta Pixel tracks users' personal information and the type of actions they take on the Roku Platforms and disseminates that information to Facebook. Therefore, when one of Roku users requests to watch a video on one of its platforms in which the Meta Pixel is deployed, it sends that user interaction, along with the persons' personally identifying information in the form of a Facebook ID, to Facebook.

35. On information and belief all the above listed third party tracking companies receive sensitive Personal Information from Roku about its users, including users' names, addresses, email addresses, precise geolocation information, IP addresses, Roku IDs, and other persistent identifiers.[6]

36. The above allegations are further substantiated by Roku admitting that its website uses third-party cookies to gather information from Roku users.[7] Such information includes personally identifying information that is distributed to Roku's third party partners. Roku identifies that it partners with these companies for advertising purposes and acknowledges in its privacy policy that it shares users' names, addresses, email addresses, precise geolocation information, IP addresses, Roku IDs, and other persistent identifiers with such companies. Using third party cookies from its partners allows Roku to benefit from its users' sensitive Personal Information.

37. Roku's *own* privacy policy details the information that it collects and discloses to third parties, including[8]:

a. Identifiers, including advertising identifiers, device identifiers, IP address, browser cookies, and other unique online identifiers;

b. Account registration Information, i.e., name, address, email address,

[6] https://docs.roku.com/published/cookiepolicy/en/us

[7] https://docs.roku.com/published/cookiepolicy/en/us

[8] https://docs.roku.com/published/userprivacypolicy

telephone number;

c. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

d. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement;

e. Precise geolocation;

f. "Audio" and "visual" information from users, which, until December 2024, Roku explicitly acknowledged to include "consumers' photos, videos, and audio recordings." Roku amended its privacy policy in December 2024 and removed these examples.

38. In addition, Roku collects and discloses highly sensitive voice data from its users, including children.

39. Roku provides several forms of voice functionality on its Roku Platforms. In doing so, Roku collects and retains voice recordings from its users by default as long as the user does not disable this functionality. Roku uses these voice recordings to improve its targeted advertising and develop its products, and also shares these voice recordings with third parties.

40. As shown above, Roku's privacy policy explains that it uses customers' "[a]udio" information to, among other things, "improve and enhance the Roku Services (including building correlations for use in Roku's advertising services in order to better serve our advertisers), and to develop new products, services, features and functionality."[9] Roku's privacy policy also states that it collects "audio information when [users] use voice-enabled features." Roku goes on to acknowledge

[9] https://docs.roku.com/published/userprivacypolicy/en/us

that it shares its customers' audio data with "[channel] and content providers," "Voice assistant providers," and "Service providers and vendors."[10]

41. Roku routinely captures, stores, and shares voice recordings of children when they engage with its voice command features and even actively promotes the use of these voice features to child users, including prompting them to "Use your voice!" upon launching the Kids and Family section of The Roku Channel.

42. Roku collects and allows third parties to track all of the aforementioned Personal Information from children using its service when they access content within the Kids and Family on The Roku Channel, and when they access other child-directed content on the Roku Platforms, and uses that Personal Information for targeted advertising on its platform pages and other services to build detailed profiles of such user children's behaviors.

43. Roku acknowledges in its privacy policy that it collects such children's Personal Information when users interact with Roku provided content as well as with "streaming services on a Roku device or Roku's Channels on other devices," when they watch or access any content on any Roku OS capable device (via "Automatic Content Recognition,") which identifies content displayed on the TV screen even outside the Roku platform, and from "websites, apps, streaming services, and connected devices (including Smart TVs and mobile devices) to which Roku provides advertising or measurement and analytics services."[11]

44. The Children's Online Privacy Protection Act (COPPA) requires, among other things, that Roku refrain from collecting, using, and disclosing certain categories of personal information from users on sections of its platform directed to children without parental notice and consent. *See* 15 U.S.C. § 6502(a)(1); 16 C.F.R. § 312.3(a)-(b). Despite this obligation, Roku collects and discloses Personal

[10] *Id.*

[11] *Id.*

Information from all users of its Roku Platforms by default, including specifically from viewers of its children's content. Roku also actively aids and abets, or allows, third parties to track the Personal Information of users who view its children's content by accessing it from child-directed sections of its Roku Platforms. Even when children access content by first navigating to Kids and Family on The Roku Channel it collects and aids third parties in the tracking of their Personal Information without parental notice and consent and uses that information to deliver targeted advertising to children on Roku platform pages.

45. The FTC confirmed in its 2017 Enforcement Policy Statement that it is a violation of COPPA for operators such as Roku to collect *and retain* children's voice recordings, and it put operators on notice that they could be subject to COPPA enforcement for retaining children's voice recordings.[12] Furthermore, the FTC explained that an operator would be subject to COPPA enforcement if it did not "provide clear notice of its collection and use of the audio files and its deletion policy in its privacy policy," and if the operator made "any other use of the audio file in the brief period before the file is destroyed—for example, for behavioral targeting or profiling purposes, for identification purposes through voice recognition, or for posting, selling, or otherwise sharing the file with third parties." 82 Fed. Reg. 58076-77. Roku violates this Enforcement Policy Statement by collecting and retaining voice recordings from portions of its service that are directed to children, by sharing voice recordings of viewers of Kids and Family on The Roku Channel (and third-party channels identified as child-directed) with third parties, and by failing to provide clear notice in its privacy policy of its collection, use, and deletion policy with respect to children's voice recordings.

46. As a result, Defendant has violated the prohibitions of COPPA, subjecting it to liability under the ECPA, as well as CIPA.

[12] https://www.govinfo.gov/app/details/FR-2017-12-08/2017-26509

FACTS SPECIFIC TO PLAINTIFF

47. Plaintiffs are both minor children under the age of 10.

48. Plaintiffs have access to, and use, multiple Roku enabled devices through their Guardian's Roku account, including a Roku streaming stick and multiple Roku TVs.

49. Plaintiffs have used Roku enabled devices available in their household to view and request child-directed content including content on the Kids and Family on The Roku Channel, children's movies, and games. Plaintiffs have also used Roku's voice enabled features on Roku's Platforms.

50. Each time Plaintiffs requested content on Defendant's Roku Platforms, Defendant collected, and knowingly and intentionally disclosed to third-parties, and aided and abetted third-parties in the interception and tracking of, Plaintiffs' sensitive Personal Information, including but not limited to video viewing data, activity of the Roku Platforms, location data, IP addresses and voice recordings.

51. Plaintiffs never specifically and separately consented, agreed, authorized, or otherwise permitted Defendant to collect and disclose, or aid and abet third parties in the tracking of, the aforementioned sensitive Personal Information. Nor did Defendant obtain COPPA compliant parental notice and consent prior to its collection, disclosure, and tracking of Plaintiffs' sensitive Personal Information.

52. By deploying its illicit data practices specifically designed to collect, disclose, and track the sensitive Personal Information of Plaintiffs and other child users, Defendant has intentionally and knowingly violated Plaintiffs' privacy rights.

53. As such, Plaintiffs are entitled to statutory damages.

CLASS ALLEGATIONS

54. Plaintiffs bring this action individually and on behalf of a Class and California Subclass (collectively the "Classes") defined as follows:

> Class: All persons who, before reaching the age of majority, requested child-directed content, or used any voice function, on any Roku enabled device, during the relevant limitations period.
>
> The California Subclass: All persons within the state of California who, before reaching the age of majority, requested child-directed content, or used any voice function, on any Roku enabled device, during the relevant limitations period.

55. Excluded from the Classes are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officers or directors.

56. Upon information and belief, there are thousands if not millions of members of the Classes, making the members of the Classes so numerous that joinder of all members is impracticable. Although the exact number of members of the Classes are currently unknown to Plaintiffs, the members can be easily identified through Defendant's records.

57. Plaintiffs' claims are typical of the claims of the members of the Classes Plaintiffs seek to represent, because the factual and legal bases of Defendant's liability to Plaintiffs and the other members are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to the Classes. As alleged herein, Plaintiffs and the Classes have all suffered damages as a result of Defendant's privacy violations.

58. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not limited to, the following:

(a) Whether Defendant collected the Classes members' sensitive personal information;

(b) Whether Defendant disclosed the Classes members' sensitive personal information to third parties;

(c) Whether Defendant disclosed the contents of Classes members' electronic communications to third-parties;

(d) Whether the Classes members provided consent to Defendant's collection and disclosure of their sensitive personal information to third parties;

(e) Whether the Classes members' parents and/or guardians provided consent for the collection and disclosure of their sensitive personal information to third parties;

(f) Whether Defendant aided third parties in the interception of Classes members' communications and sensitive personal information;

(g) Whether the Classes members are entitled to damages and other relief as a result of Defendant's conduct.

59. Absent a class action, most members of the Classes would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions in that it conserves the resources of the courts and the litigants and promotes consistency of adjudication.

60. Plaintiffs will adequately represent and protect the interests of the members of the Classes. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action on behalf of the other members of the Classes and have the financial resources to do so. Neither Plaintiffs nor

Plaintiffs' counsel have any interest adverse to those of the other members of the Classes.

61. Defendant has acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Classes, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Classes and making injunctive or corresponding declaratory relief appropriate for the Classes as a whole.

FRAUDULENT CONCEALMENT AND TOLLING

62. The applicable statute of limitations are tolled by virtue of Defendant's knowing and active concealment of the facts alleged above. Plaintiffs and the other Classes members were ignorant of the information essential to the pursuit of these claims, without any fault or lack of diligence on their own part.

63. At the time the action was filed, Defendant was under a duty to disclose the true character, quality, and nature of its activities to Plaintiffs and the Classes. Defendant is therefore estopped from relying on any statute of limitations.

64. Defendant's fraudulent concealment is common to the Classes.

COUNT ONE
Violations of the Electronic Communications Privacy Act
18 U.S.C. § 2510 *et seq.*
(On Behalf of Plaintiffs and the Classes)

65. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

66. The ECPA protects both the sending and the receipt of electronic communications.

67. The ECPA provides a private right of action to any person whose wire, oral, or electronic communications are intercepted. 18 U.S.C. § 2520(a).

68. A violation of the ECPA occurs where any person/entity "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or

endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

69. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

70. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

71. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

72. Plaintiffs and the other members of the Classes' interactions with Defendant's Roku enabled devices, including the Roku streaming sticks, Smart TV, and Roku Platforms, and the Personal Information collected, disclosed, and tracked as a result of those interactions are electronic communications under the ECPA.

73. Whenever Plaintiffs and the other members of the Classes interacted with Defendant's Roku Platforms, Defendant contemporaneously and intentionally intercepted, allowed third parties to intercept, and endeavored to intercept their electronic communications without authorization or consent through its use of the aforementioned third party tracking technologies.

74. Whenever Plaintiffs and the other members of the Classes interacted

with Defendant's Roku Platforms, Defendant contemporaneously and intentionally disclosed, allowed to be tracked, and endeavored to disclose the contents of their electronic communications to Roku's third party partners, as well as potentially other entities, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

75. Whenever Plaintiffs and the other members of the Classes interacted with Defendant's Roku Platforms, Defendant contemporaneously and intentionally used, and endeavored to use the contents of their electronic communications without authorization or consent.

76. Whenever Plaintiffs and the other members of the Classes interacted with Defendant's Roku Platforms, Defendant contemporaneously and intentionally redirected the contents of their electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including to its third party partners.

77. Whenever Plaintiffs and the other members of the Classes interacted with Defendant's Roku Platforms, Defendant contemporaneously and intentionally divulged the contents of their electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication.

78. Defendant intentionally intercepted the contents of Plaintiffs' and the other members of the Classes' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

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

80. Defendant is a "party to the communication" with respect to the other members of the Classes' communications with its Roku Platforms. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and the other minor members of the Classes' sensitive Personal Information created from their interactions with children's content on the Roku Platforms does not qualify for the party exemption.

81. Defendant's collection and disclosure to its third party partners of Plaintiffs' and other members of the Classes' communications with its Roku Platforms was done for the purposes of committing criminal or tortious acts in violation of the laws of the United States and California, including violation of COPPA, 15 U.S.C. § 6502 and violation of CIPA, Cal. Pen. Code § 631(a).

82. Roku is an "operator" under COPPA because it is an "online service" that "collects or maintains personal information from or about the users of . . . [the] online service." 16 C.F.R. § 312.2.

83. Roku is also an "operator" under COPPA with respect to third-party channels because those channels collect personal information on Roku's behalf, as Roku "benefits by allowing [those third-party channels] to collect personal information directly from users." *Id.*

84. Roku is also an "operator" under COPPA with respect to third-party channels because Roku collects personal information on those channels' behalf, and those channels "benefit[] by allowing [Roku] to collect personal information directly from users." *Id*.

85. Roku's robust catalog of children's content, and the distribution of this content across Roku Platform pages, renders Roku an online service "directed to children" under COPPA. *Id*.

86. Roku's "Kids and Family on The Roku Channel" section, the "Kids & Family" and "Games" sections of Roku's Channel Store, Roku Zones, and other

children's content sections such as "Animated Adventures" and "Popular Free Kids Movies and TV Shows," as well as the channels and content in each of these sections, are "directed to children." 16 C.F.R. § 312.2.

87. The channels and content in these sections, and the sections themselves, include, among other things, "animated characters," "child-oriented activities," "child celebrities," "celebrities who appeal to children," and "advertising . . . directed to children." *Id*.

88. Roku collects the "personal information" of Plaintiffs and other children under the age of 13 who used the Roku platforms generally, including The Roku Channel, the "Kids and Family on The Roku Channel" section, the "Kids & Family" and "Games" sections of the Roku Channel Store, and other child-directed content sections of the Roku platform.

89. Roku has "actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children," because it knows that the "Kids & Family" and "Games" sections of its Channel Store, "Kids and Family on The Roku Channel," and other child-directed sections of the Roku platform are directed to children.

90. Third-party channels in the "Kids & Family" and "Games" sections of Roku's Channel Store, and third-party channels in other child-directed sections of the Roku platform such as "Animated Adventures" and "Popular Free Kids Movies and TV Shows," collect the "personal information" of children on Roku's behalf.

91. This collection and tracking of children's personal information by Roku and third-party channels includes "[p]assive tracking of a child online," "[e]nabling a child to make personal information publicly available in identifiable form," and "[r]equesting, prompting, or encouraging a child to submit personal information online." 16 C.F.R. § 312.2. This "personal information" includes persistent identifiers such as cookies, IP addresses, device serial numbers, and unique device identifiers;

geolocation information sufficient to identify children's "street name and name of a city or town"; files containing a child's voice; and "[i]nformation concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier." 16 C.F.R. § 312.2.

92. This collection and tracking of children's personal information includes the collection, retention, and disclosure to third parties of voice recordings. Roku does not provide clear notice of this collection and use of voice data, or of its deletion policy, in its privacy policy.

93. Roku also has "actual knowledge that it is collecting or maintaining personal information from a child" when it collects, retains, and discloses to third parties voice recordings from users who are identifiably children under the age of 13. *Id*.

94. This collection of children's personal information also includes the collection of, and passive tracking of, children's "personal information" by third-party analytics companies and data brokers, including Google, New Relic, Meta, LinkedIn, and Innovid, which collect the "personal information" of children on Roku's behalf because they are agents or service providers for Roku and because Roku benefits by allowing them to collect the personal information.

95. Roku does not "[p]rovide notice" of "what information it collects from children, how it uses such information, and its disclosure practices for such information." 16 C.F.R. § 312.3.

96. Roku does not "[o]btain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children." *Id*.

97. Roku does not "[p]rovide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance." *Id*.

98. Roku has not established and does not maintain "reasonable procedures

to protect the confidentiality, security, and integrity of personal information collected from children." 16 C.F.R. § 312.3.

99. Accordingly, Defendant's illicit data practices constitute a violation of COPPA.

100. Furthermore, and as explained in detail below, Defendant's illicit data practices constitute a violation of CIPA.

101. Defendant's criminal and tortious actions are demonstrated by Attorney General Dana Nessel's complaint asserted against Roku, which alleges in detail how Roku has committed violations of COPPA; the Video Privacy Protection Act, 18 U.S.C. § 2710; Michigan's Preservation of Personal Privacy Act, M.C.L. § 445.1711; the Michigan Consumer Protection Act, M.C.L. § 445.901; Intrusion Upon Seclusion; and Unjust Enrichment. (Attached hereto as Exhibit A.)

102. Defendant cannot viably claim any exception to ECPA liability.

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

COUNT TWO
Violations of the California Invasion of Privacy Act
Cal. Pen. Code § 631(a)
(On behalf of Plaintiffs and the California Subclass)

104. Plaintiffs hereby incorporate the above allegations by reference as though fully set forth herein.

105. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Therefore, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant "by means of any machine, instrument, contrivance, or in any other manner," committed any of the following:

(i) intentionally tapped, or made any unauthorized connection, whether

physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, cable, or instrument of any internal telephonic communication system;

or

(ii) willfully and without consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

or

(iii)

uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained;

or

(iv) aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit or cause to be done any of the acts or things mentioned above in this section. Cal. Pen. Code. § 631 (a).

106. The third-party activity tracking technologies Defendant implemented on its Roku Platforms are each a "machine, instrument, contrivance, or … other manner" used to read or learn the contents or meaning of messages, reports, or communications between Plaintiffs and the other Subclass members and Defendant.

107. Defendant's third-party tracking providers were third parties to communications between Plaintiffs and the other Subclass members and Defendant.

108. Defendant's third-party tracking providers willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic

communications between Plaintiffs and the Subclass members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at a place within California.

109. Defendant aided and conspired, agreed with, employed, permitted, or otherwise enabled its third-party tracking providers to wiretap Plaintiffs' and the other Subclass members' sensitive personal information from their interactions with the Roku Platforms, including but not limited to personal information, video viewing data, location data, IP addresses and voice recordings and the contents of their electronic communications with Defendant. Defendant knew that the third-party tracking technology it installed on its Roku Platforms would result in the disclosure of user communications to third parties, as increasing its ability to perform more effective targeted advertising and generate revenue off Subclass members' data was one of Defendant's purposes for implementing such technology.

110. Plaintiffs and the other Subclass members did not provide their prior consent to such third parties' access, interception, reading, learning, recording, collection, and usage of their electronic communications. Nor did Plaintiffs and the other Subclass members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling its third-party vendors' conduct.

111. Plaintiffs and the other members of the Subclass seek all relief available under Cal. Pen. Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of and the Classes, pray for the following relief:

1. An order certifying the Classes as defined above;
2. An order declaring that Defendant's conduct violates the ECPA;
3. An order declaring that Defendant's conduct violates CIPA;

4. An order enjoining Defendant from continuing to engage in the unlawful conduct and practices described herein;
5. An award of statutory damages under the ECPA to the Class;
6. An award of statutory damages under CIPA to the Subclass;
7. For punitive damages, as warranted, in an amount to be determined at trial;
8. An award of attorney's fees and costs; and
9. Award such further relief as the Court deems reasonable and just.

JURY DEMAND

Plaintiffs request trial by jury of all claims that can be so tried.

DATED: August 4, 2025

Respectfully submitted,

E.A.R.R. & E.A.R., by and through their Guardian LYNETTE GONZALEZ, individually and on behalf of similarly situated individuals,

By: /s/ *Eugene Y. Turin*
One of Plaintiffs' Attorneys

Eugene Y. Turin (SB # 342413)
10089 Willowcreek Road, Suite 200
San Diego, CA 92131
Tel: (312) 893-7002 Ex. 3
Fax: 312-275-7895
eturin@mcgpc.com

Attorneys for Plaintiffs and the Putative Class

ClassAction.org