

**IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL DISTRICT
IN AND FOR COLLIER COUNTY, FLORIDA**

OFFICE OF THE ATTORNEY GENERAL,
STATE OF FLORIDA,
DEPARTMENT OF LEGAL AFFAIRS,

Plaintiff,

CIVIL DIVISION
CASE NO.:

v.

ROKU, INC., and FLORIDA ROKU, INC.,

Defendants.

_____ /

COMPLAINT

1. For over a decade, Roku has delivered children's video content to Florida homes. During that time, the company has grown into the dominant television content platform in the United States. It is in nearly half of all households and earns billions of dollars each year by collecting data about its users (children and adults) and using that data to facilitate targeted advertising.

2. Roku acknowledges processing, disclosing, and selling to third parties a wide variety of personal and sensitive data about its users. Yet Roku does not acknowledge that it continues processing, disclosing, and selling this personal data even when it has every reason to know the data was collected from children. Worse still, Roku shares with and sells this data to intrusive data brokers, including Kochava, a company that has constructed profiles of tens of millions of children and physically tracks and discloses individuals' precise geolocation data collected from their personal devices.

3. Roku knows that some of its users are children but has consciously decided not to implement industry-standard user profiles to identify which of its users are children. Roku buries

its head in the sand so that it can continue processing and selling children’s valuable personal and sensitive data. Even when a user waves a flag signaling to Roku that he or she is a child—such as by installing Roku’s “Kids Screensaver” or “Kids Theme Pack,” downloading apps from the “Kids & Family” section of Roku’s Streaming Store, viewing content from Roku’s “Kids and Family on The Roku Channel” streaming service, and receiving children’s content recommendations from Roku itself—Roku continues processing and selling data collected from that user across many parts of its platform. This violates Florida law.

4. Roku hides behind the assertion that it does not have “actual knowledge” that it processes or sells children’s personal information. But Florida law does not enable Roku to escape liability by feigning ignorance about its underage users. To the contrary, the Florida Digital Bill of Rights includes in its definition of “known child” the willful disregard of a child’s age, Fla. Stat. § 501.702(17), and Roku willfully disregards the age of its users when it “should reasonably have been aroused to question whether a consumer was a child and thereafter failed to perform reasonable age verification,” Fla. Admin. Code Ann. R. 2-3.003. Because Roku continues processing and selling users’ data when it should reasonably have been aroused to question the age of those users, and because Roku fails to get consent from all its users to process their sensitive data, it has violated (and continues to violate) multiple provisions of the Digital Bill of Rights. Fla. Stat. §501.701, *et seq.*

5. Finally, Roku forms partnerships and sharing agreements with third-party data brokers in an effort to avoid complying with Florida law. For example, in one such partnership, Roku sells and shares precise geolocation data about its users—including children—to Roku advertisers. Roku also shares purportedly “deidentified” data about its users with third parties knowing they will link that “deidentified” data with information (such as the user’s precise

geolocation information) and thereby reconstruct users' identities. The result is that Roku earns more money from advertisers by knowingly violating its users' privacy, again in violation of Florida law (e.g., Fla. Stat. § 501.715 (limiting sale of users' sensitive data) and Fla Stat. § 501.714 (requiring efforts to prevent reidentification of users' data)).

6. The Attorney General brings this enforcement action pursuant to the Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, Fla. Stat. ("FDUTPA") to protect Florida's children and families' privacy rights and end Roku's violations of Florida law. On behalf of all minor residents of Florida and Florida consumers, the Attorney General seeks to compel Defendants to comply with their obligations under Florida's privacy law, as well as FDUTPA, and to stop the unfair, deceptive, and unconscionable business practices that the Defendants have used to build a vast and lucrative Florida user base that includes vulnerable children.

PARTIES

7. The Office of the Attorney General, State of Florida, Department of Legal Affairs (the "Attorney General"), is authorized to enforce the Florida Digital Bill of Rights ("FDBR"), Fla. Stat. § 501.701 *et seq.*, and the FDUTPA. The Attorney General has investigated the matters alleged in this Complaint and determined that this enforcement action serves the public interest.

8. Defendant Florida Roku, Inc. ("Florida Roku") is a for-profit Delaware corporation with a principal address of 1701 Junction Court, Suite 100, San Jose, California 95112, and authorized to do business in Florida as a foreign corporation. Florida Roku is the name under which Roku, Inc., operates in the State of Florida.

9. Defendant Roku, Inc., is a for-profit Delaware corporation with a principal address of 1701 Junction Court, Suite 100, San Jose, California 95112, and operating in Florida under the name Florida Roku, Inc.

10. Because Defendants operate as one entity, this Complaint refers to Defendants collectively as “Roku.”

11. Roku conducts business in the State of Florida and elsewhere. In the course of that business, Roku collects personal data about its Florida users and third parties collect data about Roku’s Florida users on Roku’s behalf. Roku determines the purposes and means of processing personal data about Roku’s Florida users alone and/or jointly with others.

12. Roku generates in excess of \$1 billion in global gross annual revenue. Roku derives 50 percent or more of its global gross annual revenue from the sale of advertisements online, including through the provision of targeted advertising and the sale of ads in Florida. Roku operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation through their “Roku Voice Remote Pro (2nd Edition).” This qualifies Roku as a Controller under Fla. Stat. § 501.702(9), and therefore subjects Roku to the requirements set forth in FDBR. Fla. Stat. § 501.701 *et seq.*

JURISDICTION AND VENUE

13. This is an action for statutory and equitable relief for violations of FDBR and FDUTPA. Fla. Stat. § 501.207(1)(b). The Attorney General seeks relief in an amount greater than Fifty Thousand Dollars (\$50,000), exclusive of fees and costs.

14. Roku’s statutory violations occurred in or affect more than one judicial circuit in the State of Florida, including the Twentieth Judicial Circuit in and for Collier County.

15. This Court has subject matter jurisdiction pursuant to its general jurisdiction and FDUTPA.

16. This Court has personal jurisdiction over Roku pursuant to Fla. Stat. § 501.72(10) because Roku meets the definition of a “controller” under FDBR and Roku collects and shares the

personal data of Florida consumers. This Court also has personal jurisdiction over Roku pursuant to Florida's long-arm statute, Fla. Stat. § 48.193(1)(a)(1), because Roku operates, conducts, engages in, and carries on a business in this state. Roku has millions of users in the State of Florida, and likely more than one million child users. These users have Roku accounts that list Florida addresses. The conduct and violations of law described in this Complaint arise from Roku's conduct in Florida and its contacts with users in Florida.

17. The Roku platform is present in nearly half of American households and, as a result, there are likely Roku accounts registered to users in every county in the State of Florida, including in Collier County. Some of those accounts in Collier County are used by—and are known by Roku to be used by—children. Roku processes, sells, and enables the reidentification of personal and sensitive data of Roku users in Collier County, including children in Collier County, as alleged below. Roku also sells and enables the sale of targeted advertising to Roku users in Collier County, including on Roku platform pages, and through its partnerships with data broker Kochava enables advertisers to gain access to the precise geolocation data of Roku users, including children, in Collier County. Accordingly, the causes of action alleged herein accrued against Roku in Collier County and venue is therefore proper in this Court pursuant to Fla. Stat. § 47.051.

18. At all times material hereto, Roku has engaged in “trade or commerce” as defined in Fla. Stat. § 501.203(8).

FACTUAL ALLEGATIONS

I. Overview of Roku

19. Roku operates a content platform for connected televisions (“CTVs” or “smart TVs”). Users may gain access to Roku's content by purchasing a Roku streaming stick or box, by purchasing a television that has the Roku platform preinstalled, or by accessing Roku content from a computer or Roku's mobile app.

20. Upon launching the Roku platform on a smart TV, users are presented with a number of platform pages that provide different ways to access television content. These platform pages include the “Home” page, the “What to Watch” page, the “Search” page, the “Featured Free” page, and the “Streaming Store.”

21. From these platform pages, Roku customers can access a variety of apps and content. Apps available on Roku include third-party streaming services such as Netflix or Disney+; Roku’s own free, ad-supported streaming services, such as The Roku Channel; and countless other third-party apps dedicated to sports, news, or even particular YouTube celebrities. Roku users download these apps so that they are permanently displayed on the Roku Home screen, providing a quick shortcut to streaming content. Users can also access these apps by using the “Search” page to search for an app or particular content within an app, or by clicking a link or advertisement for an app or specific app content presented on any of the platform pages. Roku’s voice-enabled remotes also allow users to search for and select content using voice commands.

A. Roku’s Business Model

22. Upon information and belief, Roku earns most of its revenue by selling and delivering advertisements. The Roku platform pages discussed above are a significant source of advertising revenue for Roku, as it sells and displays advertisements for third-party apps and streaming services, for paid programming, and for consumer brands across the Home, What to Watch, Search, Featured Free, and other platform pages. Roku also sells advertising on the Roku screensaver that displays when Roku devices are left idle.

23. In addition to advertising on platform pages, Roku earns revenue by selling and delivering advertisements to viewers of its ad-supported streaming services, such as The Roku Channel, and to viewers of ad-supported third-party apps. Under its default “Inventory Split”

model, Roku is entitled to serve 30% of all advertising on third-party Roku apps, and to keep the revenue it earns. With respect to many third-party apps, Roku also reserves the right to serve 100% of the app's advertising and then split the revenue earned with the app's owner.

24. In total, Roku's "Platform" segment, which includes its advertising business, earned \$3.5 billion in 2024. Roku's platform segment operates at approximately a 50% gross profit margin. C.J. Leonard, Director of Ad Operations and Technology at media consulting firm Infinitive, has described Roku as "sitting on a gold mine of audience and content/context data." In recent years, Roku has increasingly used users' data to sell more and better targeted advertisements.

25. Roku earns revenue in other ways as well. Roku keeps a portion of the purchase price when its users subscribe to certain third-party streaming services or purchase video content from within the Roku platform. Roku also earns limited revenue from the sale of Roku devices, but upon information and belief loses money on the sale of its devices overall in order to keep device prices low and grow the userbase to which it can deliver targeted advertising.

B. Children's Video Content on Roku

26. Roku includes an enormous quantity of children's video content. Roku's own "Kids and Family on The Roku Channel," a section of Roku's streaming service dedicated to children and also a separate app, advertises that it provides "instant access to 10,000+ FREE kids' shows and movies including Ryan's World, Cocomelon, Sesame Street, My Little Pony, LEGO, Minecraft, Thomas & Friends, Barbie and more."

27. Roku also includes a huge variety of third-party apps targeted to children. One popular app, for example, is "HappyKids – Kids TV Shows and Movies," which invites users to "[d]ive into a treasure trove of 100,000+ free videos, featuring beloved family-friendly movies and

shows like Cocomelon, Pokémon, Sesame Street, Blippi, Paw Patrol, Peppa Pig, LEGO, K-city Gaming, and more.” Roku also includes apps targeted to teens, such as “Fawesome Teen,” an app that describes itself as providing “teen-centric movies” and “an endless array of content that speaks to the interests and experiences of teens.”

28. In December 2024, Roku reported the “most-searched” franchises on Roku that year. These were: (1) Inside Out; (2) SpongeBob SquarePants; (3) Bluey; (4) Yellowstone; and (5) The Super Mario Bros. Movie. With the exception of one franchise (Yellowstone), the most-searched franchises on Roku in 2024 were all children’s video content.

29. Roku users’ Home screens are frequently dominated by apps directed to children because users download Roku apps to their Home page. When users view children’s content on Roku, they also receive targeted recommendations and advertisements for children’s content based upon their viewing history.

30. Children’s content on Roku may be accessed without first navigating to a children’s app or clicking on a content recommendation or advertisement. Children can use Roku’s Search page to search for particular children’s content, or for children’s content generally. Children may also access children’s content from Roku’s What to Watch page; by clicking on one of the many Roku-aggregated categories of children’s content, such as “Popular Free Kids Movies and TV Shows”; or by clicking on content in “Roku Zones,” which organize content into child-directed themes such as “Jungle Fun” or “Nursery Rhymes.”

31. Roku also enables users to modify their Roku platform pages for children. Roku users can download a “Kids Theme Pack” that modifies the Roku platform pages, the Roku screensaver, and Roku platform sounds to appeal to young children. Users can also modify only the screensaver to display Roku’s immensely popular “Kids Screensaver.” The Kids Screensaver

replaces the “Roku City” screensaver that displays by default when a Roku device is left idle for a period of time. This Roku City screensaver is itself designed to appeal to children, as it includes a cartoon city with aliens and other comic characters, and frequently incorporates advertisements for children’s programming such as SpongeBob SquarePants. The Roku Kids Screensaver, meanwhile, appeals to an even younger audience, and incorporates cartoon references to popular animated children’s movies.

II. Roku’s Willful Disregard of Child Users on its Platform

32. Roku has every reason to know that children are among its users, and its failure to implement reasonable safeguards demonstrates **willful disregard** of the presence of children on its platform, within the meaning of Fla. Stat. § 501.702(17).

33. As detailed above, Roku’s own data show that child-directed programming is among the most searched and most viewed content on its platform and Roku actively promotes that content, including with “Kids & Family on The Roku Channel,” curated age-banded categories such as “Ages 1–3,” “Ages 4–6,” and “Ages 7–9,” and the “Kids Screensaver” and “Kids Theme Pack” features designed to appeal to young children.

34. Despite these obvious indicators, Roku collects and processes personal and sensitive data from these users without performing reasonable age verification or seeking affirmative authorization, as required by Fla. Stat. § 501.71(2)(d).

35. Publicly available demographic data further confirm what Roku’s own business experience demonstrates: approximately 40% of U.S. households include children under the age of 18, and households with children average nearly two children per family. Roku is present in millions of Florida households and therefore cannot plausibly claim ignorance of the fact that a substantial portion of its Florida user base includes children.

36. By ignoring clear indicia of the presence of children on its platform, Roku has **willfully disregarded** the fact that it is collecting, processing, and selling the personal data of Florida children, in violation of Fla. Stat. §§ 501.71, 501.715.

III. Roku's Collection of Users' Personal Data

37. Roku has developed a reputation as a company that invades its users' privacy. The Mozilla Foundation has called Roku the "nosy, gossipy neighbor of connected devices."

38. Indeed, in its Privacy Policy, Roku admits collecting, processing, and disclosing to third parties an enormous quantity of data from its users, including:

- (a) "device identifiers";
- (b) "internet protocol addresses";
- (c) "browser cookies";
- (d) "unique online identifiers";
- (e) a user's "name, address, email address, [and] telephone number";
- (f) "records of personal property";
- (g) "products or services purchased, obtained, or considered";
- (h) "purchasing or consuming histories or tendencies";
- (i) certain "[c]haracteristics of protected classifications under Federal law";
- (j) "browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement";
- (k) "Audio" information, such as voice recordings collected from Roku voice remotes; and
- (l) "Precise geolocation."

39. With respect to all of the above data except users' names, addresses, email addresses, phone numbers, audio information, and precise geolocation data, Roku forthrightly admits processing, disclosing, and *selling* the data to "Advertisers, ad networks, advertising partners, and ad measurement providers," as well as to app providers and other third parties. Roku expressly acknowledges that it *sells* this data by listing the categories of businesses to which it sells each type of data beneath the header, "Categories of Third Parties to Whom the Personal Information is 'Sold' and the Purpose." With respect to users' names, addresses, email addresses, phone numbers, audio information, and precise geolocation data, Roku still acknowledges processing the data and disclosing it to unnamed "Service providers and vendors." Roku does not obtain consent to process users' precise geolocation data or other sensitive data as required by FDBR. Fla. Stat. §§ 501.71(d) (prohibiting the processing of "the sensitive data of a consumer without obtaining the consumer's consent"); 501.702(7) (defining "[c]onsent" to mean "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer" and not to include "[a]cceptance of a general or broad terms of use or similar document").

A. Roku's Processing of Personal and Sensitive Data from Known Children

40. Roku collects the above categories of data from users as they navigate Roku platform pages, as they view Roku video content, and as they use apps from Roku and third parties. Roku also collects users' personal information as they browse the internet.

41. Roku does not restrict its collection or processing of the above categories of data in many circumstances where it has every reason to know that children are using its platform and that the data it is collecting and processing comes from children. Instead, Roku willfully disregards these facts, declines to investigate further, and carries on collecting, processing, and selling the

child user's personal and sensitive data. For instance, a Roku user who has downloaded exclusively children's apps, or watches exclusively children's content in Kids and Family on The Roku Channel, is subject to collection of the above categories of data as he or she navigates the Roku platform or other websites. The same is true for a Roku user who has added the "Kids Screensaver" or installed the "Kids Theme Pack." Roku even subjects users to widespread data collection when it delivers targeted advertisements and content recommendations based upon those users' history of viewing content from Kids and Family on The Roku Channel and/or third-party apps from Roku's "Kids & Family" section.

42. Roku also collects and receives from third parties information allowing it to determine when a *particular device* used to access Roku is used exclusively or primarily by children. In its Privacy Policy, Roku explains that it "associate[s] the browsers and devices (such as smartphones, tablets, streaming players, connected TVs, and computers) used by the same individual . . . to that individual . . . on different browsers or devices," allowing Roku to ensure that "ads you see on your tablet [are] based on activities you engaged in on your Roku TV." Families commonly provide their children with tablets, smartphones, or televisions from which a given child alone views Roku content. Roku's sophisticated data collection allows it to differentiate these users and thus know when it is processing data from (and delivering advertisements to) particular users on particular devices. Yet when it comes to a user who Roku has every reason to know is a child, Roku willfully disregards that knowledge and continues processing that child's personal and sensitive data.

43. Roku's failure to limit its processing of data from users it should know are children but for its willful disregard is apparent from one of the few limits it does acknowledge placing on the collection of children's data in its Privacy Policy. With respect to voice recordings collected

from Roku voice remotes, Roku says that when users are visiting Kids and Family on The Roku Channel, or viewing content Roku has determined to be child-directed, Roku immediately deletes what it assumes to be children's voice recordings. Yet Roku does not claim to stop its collection, processing, and retention of voice recordings when those same Roku users exit Kids and Family on The Roku Channel or simply stop viewing the particular third-party content Roku has identified as child-directed. Even if these users return to Roku platform pages solely to navigate to new child-directed content, Roku will collect and process their personal data as if they were an adult under Florida law.

44. In each of the above-described circumstances, as well as many others, Roku should be "aroused to question whether a consumer [is] a child." Fla. Admin. Code Ann. R. 2-3.003. But instead of seeking to verify the user's age, obtain the user's affirmative authorization, or otherwise process the user's data in accordance with FDBR, Fla. Stat. § 501.71(2)(d), Roku willfully disregards the presence of children on its platform and continues processing children's personal data.

B. Roku's Partnerships with Third-Party Data Brokers

45. In addition to Roku's widespread processing of data collected from known children, Roku also sells its data to third parties—who subsequently reidentify Roku's data in order to deliver a detailed picture of Roku customers without implicating Roku directly.

46. One example of Roku's data broker partnerships are its partnerships with Kochava, a data broker with a long history of privacy violations and public scrutiny. Kochava is a company whose business model was built on hiding software inside widely downloaded third-party apps and using that software, along with other data sources, to build a database of detailed profiles covering nearly the entirety of the U.S. population, including millions of children. Among the data

Kochava compiles is precise geolocation data showing where Floridians move as they go about their day.

47. In August 2022, the FTC sued Kochava for collecting, selling, and freely distributing a variety of sensitive and personal information, including precise geolocation information tracking individuals' movements. *See* Complaint ¶ 1, *FTC v. Kochava Inc.*, No. 22-cv-377 (D. Idaho Aug. 29, 2022) (“Defendant’s violations are in connection with acquiring consumers’ precise geolocation data and selling the data in a format that allows entities to track the consumers’ movements”); *id.* ¶ 7 (“Kochava is, among other things, a location data broker that provides its customers massive amounts of precise geolocation data collected from customers’ mobile devices.”); *id.* ¶ 12. The location data Kochava collects and sells is “not anonymized.” *Id.* ¶ 21. Kochava’s datasets “directly link[] this precise geolocation data to identifying information about individual consumers, such as names, addresses, email addresses, and phone numbers.” Second Amended Complaint ¶ 4, *FTC v. Kochava Inc.*, No. 22-cv-377 (D. Idaho July 15, 2024). As explained below, Roku has partnered with Kochava in multiple ways so that Kochava and Roku can take advantage of this data to deliver to Roku advertisers some of the same personal and sensitive data regarding Roku users that Roku claims not to disclose to advertisers and other third parties.

48. Since 2021, Kochava has claimed to have profiles covering “over 320 million unique people” in the United States, thus covering 95% of the U.S. population and tens of millions of children. Kochava promoted these profiles to be used by its customers to “enhance targeting for connected TV” advertising campaigns. Kochava has also advertised that it collects “rich geo data spanning billions of devices globally,” and that it “delivers raw latitude/longitude data with volumes around 94B+ geo transactions per month.” Second Amended Complaint ¶ 33, *FTC v.*

Kochava Inc., No. 22-cv-377 (D. Idaho July 15, 2024). Kochava’s precise geolocation data “can often pinpoint a consumer’s location to within less than 10 meters,” “tracks consumers’ movements for at least the past year,” “is updated regularly as new information is obtained,” and “includes consumers’ movements as recent as the prior day.” *Id.* ¶ 29.

49. Roku and Kochava’s partnership runs deep. Grant Cohen was GM of Kochava from 2015 to 2019 before leaving Kochava to join Roku as its Global Head of Endemic Media. In 2021, Kochava was added to Roku’s Measurement Partner Program, where it remains today. As of February 2024, Roku claimed to have “evaluated and vetted” its Measurement Partners for, among other things, “their compliance with consumer privacy policies.” Of course, even the most limited vetting by Roku would have exposed that Kochava’s business practice—and indeed its business model—was to link the data Roku provided advertisers with the identifying and precise geolocation data that Roku claimed not to provide advertisers.

50. The services Kochava provides for Roku and its partners go beyond measuring the performance of advertisements or Roku’s Measurement Partner Program. Roku app makers can use Kochava to “measure user engagement across their applications” in order to better understand what devices and individuals in a given household are accessing their Roku app. On a webpage describing “common use cases” for the Kochava Roku software development kit (SDK), Kochava advertises that its Roku SDK allows apps to “[t]rack user behavior and actions beyond the install,” “[t]rack in-app purchases and revenue,” and “[t]rack user subscriptions and [f]ree trials.”

51. Mr. Cohen has since *returned* to Kochava, where he is now the Head of Measurable Extension. Since then, Roku has integrated Kochava into its own advertising sales platform, Roku OneView, and Kochava currently highlights Roku as one of its “Key Partners” in its Measurable Extension business. Kochava describes on its website how users can go about “creating a Roku

OneView campaign within Kochava.” And Roku is listed among the companies that uses “Kochava for Publishers,” which is a service that allows *Roku* to provide advertisers with data such as “footfall visitation”—precise geolocation data used to determine when Roku users visit an advertiser’s physical store after seeing an advertisement. Kochava describes such “offline outcome[]” analytics as providing “near real-time insights.” Kochava promises that by using its services Roku will “[c]ommand higher CPM rates”—and thus earn higher advertising revenue—“for premium inventory and ad placements.”

52. Kochava’s Measurable Extension for Publishers claims to improve ad delivery as well, including to help “[d]eliver the right ad, to the right user, on the right device, at the right time.” Kochava for Publishers also enables Roku to provide additional features to advertising buyers, such as the ability to “[s]upport more flexible currency options for transacting media (e.g., CPI and CPA),” so that Roku can *charge* advertisers on a different basis (cost-per-install or cost-per-action). Moreover, Kochava advertises that it provides Roku app creators the ability to “measure user engagement across all Roku device types.” And in describing Kochava for Roku OneView, Kochava explains that it enables advertisers to use its “proprietary device scoring technology through a third-party identity graph” to create a model of an advertising control group and allow advertisers to avoid “holding back a 10%-20% audience segment as a control group.” In other words, as part of the package of services it provides, Kochava uses its third-party identity graph to estimate how an advertisement would perform against a control group, obviating the need for advertisers to deliver their advertisements to a control group.

53. Roku sells its users’ personal data to advertisers who use its Kochava-enhanced services. Through Kochava for Publishers, Roku sells Kochava-enhanced data about its users directly to advertisers. This includes, upon information and belief, its users’ sensitive data such as

their precise geolocation information. As Kochava acknowledges, publishers such as Roku command higher advertising rates when they enhance their available advertising with Kochava's tools.

54. Upon information and belief, as part of its partnership with Kochava, Roku also sells to Kochava the personal data of known children. Kochava has explained that it "require[s] each data supplier to contractually represent and warrant their obtainment of appropriate end-user consents and authorization . . . to sell data to [Kochava]." Kochava Inc.'s and Collective Data Solutions, LLC's Amended Answer to Plaintiff's Second Amended Complaint, No. 22-cv-377 (D. Idaho July 22, 2025), Dkt. 122 at 32. As a "data supplier" to Kochava, Roku has to "contractually represent and warrant" that it has customers' consent to "sell data to [Kochava]." *Id.*

55. Roku also receives monetary consideration in exchange for sharing data with Kochava through increased advertising prices. By providing Kochava with data, Roku elicits higher prices for Roku advertising and earns more in advertising revenue. Kochava notes that the goal of its Measurable Extension business is to "Provide More Value for [Publishers'] Advertisers" by delivering them "key benefits" and thereby allow publishers to "[i]ncrease ad revenue without increasing ad load."

56. Roku's sale of data to Kochava is evident in other aspects of Kochava for Publishers' business model. Kochava provides publishers monetary consideration to use its platform in the form of a "deep discount" on its retail price, which is consideration for, among other things, the user data that results from the publisher's partnership with Kochava.

57. In addition to selling user data, Roku relies on data brokers to reidentify the deidentified data it shares with advertisers. Roku does not share certain limited categories of user data with advertisers and other third parties, including users' names, addresses, email addresses,

telephone numbers, and precise geolocation information. Instead, Roku relies on third-party data brokers that match the data Roku does share—including device identifiers, IP addresses, and unique online identifiers—to the sensitive, identifying, and personal data Roku claims not to share, and thereby reidentify Roku users. In addition to precise geolocation data, upon information and belief, Roku’s partnerships with Kochava enable Roku advertisers to learn identifying personal and sensitive data about the Roku users to which their advertisements are delivered, including those device holders’ “ethnicity,” gender, “date of birth,” “status as a minor,” “status as a parent and number of children,” “political association,” and “marital status”—all categories of data Kochava makes available to customers. Second Amended Complaint ¶ 52, *FTC v. Kochava Inc.*, No. 22-cv-377 (D. Idaho July 15, 2024).

58. Upon information and belief, Roku’s data sharing with Kochava has already led to the public, functionally unrestricted disclosure of Roku users’ identifying information, including precise geolocation data. As recently as June 2022, Kochava offered a free “Data Sample” on the Amazon Web Services marketplace. Second Amended Complaint ¶¶ 34-35, *FTC v. Kochava Inc.*, No. 22-cv-377 (D. Idaho July 15, 2024). This Data Sample contained “sensitive categories of information” for over 61 million mobile devices and disclosed those mobile devices’ precise geolocation information over a seven-day period. *Id.* ¶¶ 36-37. The FTC reports being able to use this free data sample to track individuals’ movements between their homes, houses of worship, medical appointments, domestic violence shelters, and addiction recovery centers. *Id.* ¶¶ 42-45. Upon information and belief, the data could readily be used to identify children based upon, among other things, their school attendance, and to then track those children to their homes.

59. Roku’s partnerships with Kochava serve as examples of Roku’s broader privacy practices with respect to user data when dealing with data brokers generally. Roku shares users’

personal data with at least 75 known data brokers, including one other data broker (InMarket) that has been subject to an FTC enforcement action related to its collection of precise geolocation information from tens of millions of people, and at least four other data brokers (Acxiom, Comscore, Experian, and Viant) that are known to collect the personal information of children.

IV. Conclusion

60. Roku has uniquely broad access to the personal data of Florida's children and families through its privileged position inside millions of Florida homes. It has used this privileged position to illegally process, sell, and enable reidentification of some of Florida consumers' most private and sensitive personal data. The Attorney General brings this action to protect Florida residents and stop Roku's ongoing privacy violations that affect millions of children and adults throughout the state.

COUNT I **Unfair or Deceptive Practice – Unauthorized Processing of** **Sensitive Data Under Florida Digital Bill of Rights** **(Fla. Stat. §§ 501.204, 501.71(2)(d))**

61. The Attorney General incorporates the allegations set forth in complaint paragraphs 1 through 60, inclusive, as if fully set forth herein.

62. Roku is a "controller" for the purposes of the Florida Digital Bill of Rights. Fla. Stat. § 501.702(9).

63. Roku processes "personal data" under FDBR, Fla. Stat. § 501.702(19), from Florida users across the Roku platform, including on the Roku Home page, Search page, What to Watch page, Featured Free page, and Streaming Store, from Florida users navigating or viewing content within third-party apps, and from Florida users navigating or viewing content within The Roku Channel and Kids and Family on The Roku Channel. This personal data includes device identifiers; internet protocol addresses; browser cookies; unique online identifiers; a user's name,

address, email address, and telephone number; products or services purchased, obtained, or considered; purchasing or consuming histories or tendencies; characteristics of protected classifications under Federal law; browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement; voice recordings; and precise geolocation.

64. Some of the personal data Roku processes from Florida users across its platform constitutes "sensitive data" under FDBR, Fla. Stat. § 501.702(31), including precise geolocation information.

65. "Personal data" under FDBR includes "any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual." Fla. Stat. § 501.702(19). All of the personal data Roku collects and processes from Florida users across its platform is "sensitive data" when it is collected from a "known child." *Id.* § 501.702(31)(c). That is because "sensitive data" includes any "[p]ersonal data collected from a known child." *Id.* § 501.702(31)(c). Roku also collects and processes sensitive data from a known child whenever it collects precise geolocation data or other categories of sensitive data from a known child on its platform.

66. FDBR defines "child" to mean "an individual younger than 18 years of age." Fla. Stat. § 501.702(6). Roku collects and processes data from a known child whenever it knows or willfully disregards that a Roku user is under age 18, *id.* § 501.702(17), including in circumstances where Roku "should reasonably have been aroused to question whether a consumer was a child and thereafter failed to perform reasonable age verification." Fla. Admin. Code Ann. R. 2-3.003(4)(a).

67. Roku knows or willfully disregards that Florida users of its platform are under age 18, and processes personal and sensitive data from those users, in a variety of circumstances, including when Florida users or accounts have: downloaded or installed Roku's "Kids Screensaver"; downloaded or installed Roku's "Kids Theme Pack"; downloaded or installed one or more apps for children, including but not limited to Kids and Family on The Roku Channel and any app included in the "Kids & Family" section of Roku's Streaming Store or Channel Store; or downloaded and/or installed primarily or exclusively apps for children, including but not limited to Kids and Family on The Roku Channel and any app included in the "Kids & Family" section of Roku's Streaming Store or Channel Store.

68. Roku also knows or willfully disregards that Florida users of its platform are under age 18, and processes personal and sensitive data from those users, when those users, in a given browsing session, view: content in Kids and Family on The Roku Channel; content organized into Roku's "Ages 1-3," "Ages 4-6," and "Ages 7-9" age bands; third-party apps and content in the "Kids & Family" section of Roku's Streaming Store or Channel Store; content organized into child-directed sections such as "Animated Adventures" and "Popular Free Kids Movies and TV Shows"; content included in any of these sections but accessed from the Roku Home page, Search page, Featured Free page, or What to Watch page; content on channels that self-identify in their title or description as targeting "kids," "kidz," "boys," "girls," or "teens"; or content identified to Roku as child-directed or Made for Kids.

69. Roku also knows or willfully disregards that Florida users of its platform are under age 18, and processes personal and sensitive data from those users, when Roku itself delivers targeted advertisements and content recommendations to those same users or their accounts for child-directed content based upon their history of viewing content from Kids and Family on The

Roku Channel and/or third-party apps from the “Kids & Family” section of Roku’s Streaming Store or Channel Store, when Roku has collected information sufficient to determine that a particular device used to access its content is used by children, or when Roku has collected information sufficient to determine that a particular user accessing Roku has viewed content from Kids and Family on The Roku Channel or third-party apps in the “Kids & Family” section of Roku’s Streaming Store or Channel Store in the past.

70. Roku processes the sensitive data of known children under age 13 without performing any age verification, without obtaining any affirmative authorization or consent, and without complying with the requirements of Fla. Stat. § 501.71(2)(d).

71. Roku also does not obtain affirmative authorization or consent to process the sensitive data of known children between ages 13 and 18 as required by Fla. Stat. § 501.71(2)(d).

72. Roku also fails to obtain consent from users ages 18 and older to process their sensitive data, including precise geolocation data, as required by Fla. Stat. § 501.71(2)(d).

73. A violation of FDBR is a *per se* unfair and deceptive trade practice actionable under FDUTPA. Fla. Stat. § 501.72(1). Roku’s processing of the sensitive data of its users, including the sensitive data of known children, violates FDBR and therefore violates FDUTPA, Fla. Stat. §§ 501.204, 501.72(1). Roku is subject to civil penalties of up to \$50,000 per violation and up to \$150,000 per violation involving known children. *Id.* § 501.72(1). Each of the above acts constitutes a separate violation with respect to each Roku user in Florida affected.

COUNT II
Unfair or Deceptive Practice – Processing and Sale of
Sensitive Data Under Florida Digital Bill of Rights
(Fla. Stat. §§ 501.204, 501.715)

74. The Attorney General incorporates the allegations set forth in complaint paragraphs 1 through 60, and 62 to 73, inclusive, as if fully set forth herein.

75. As alleged above, Roku collects and processes sensitive data from its users, including known children under the age 18, and does so without performing any age verification, or obtaining any affirmative authorization or consent, as required by Fla. Stat. § 501.71(2)(d).

76. Roku processes and sells this sensitive data to advertisers and data brokers without obtaining affirmative authorization from children between ages 13 and 18 and without performing any age verification, obtaining affirmative authorization or consent, or otherwise complying with Fla. Stat. § 501.715(1) with respect to the sensitive data of children under age 13.

77. Roku also sells the sensitive data of all its Florida users, including its Florida users' precise geolocation information, without obtaining the consent of those Florida users.

78. Roku also fails to properly disclose to Roku Florida users that it engages in the sale of their sensitive data by including the required notice reading, "NOTICE: This website may sell your sensitive personal data." Fla. Stat. § 501.715(2).

79. A violation of FDBR is a *per se* unfair and deceptive trade practice actionable under FDUTPA. Fla. Stat. § 501.72(1). Roku's processing and sale of sensitive data in violation of the FDBR therefore violates FDUTPA. Fla. Stat. §§ 501.204, 501.715. Roku is subject to civil penalties of up to \$50,000 per violation and up to \$150,000 per violation involving known children. *Id.* § 501.72(1). Each of the above acts constitutes a separate violation with respect to each Roku user in Florida affected.

COUNT III
Unfair or Deceptive Practice – Failure to Prevent Data
Reidentification Under Florida Digital Bill of Rights
(Fla. Stat. §§ 501.204, 501.714)

80. The Attorney General incorporates the allegations set forth in complaint paragraphs 1 through 60, 62 to 73, and 75 to 79, inclusive, as if fully set forth herein.

81. Roku's collection and processing of Florida users' personal data includes the collection of deidentified data.

82. Roku shares deidentified data with third parties, including advertisers and data brokers such as Kochava.

83. Data brokers and advertisers use other data sources to associate the deidentified data Roku shares with an individual.

84. Roku fails to take "reasonable measures to ensure that the data" it shares with data brokers and advertisers "cannot be associated with an individual." Fla. Stat. § 501.714(1)(a).

85. Roku fails to "[c]ontractually obligate any recipient of the deidentified data" it supplies, including data brokers and advertisers, "to comply with this part." Fla. Stat. § 501.714(1)(c).

86. A violation of FDBR is a *per se* unfair and deceptive trade practice actionable under FDUTPA. Fla. Stat. § 501.72(1). Roku's failure to take reasonable measures to ensure that individual Florida users' data shared with data brokers and advertisers cannot be associated with those individuals, and Roku's failure to contractually obligate data brokers and advertisers to comply with § 501.714 with respect to individual Florida users' data, violate FDUTPA. Fla. Stat. §§ 501.204, 501.72(1). Roku is subject to civil penalties of up to \$50,000 per violation and up to \$150,000 per violation involving known children. *Id.* § 501.72(1). Each of the above acts constitutes a separate violation with respect to each Roku user in Florida affected.

PRAYER FOR RELIEF

Wherefore, the Attorney General requests that this Court:

- A. Enter judgment in favor of the Attorney General and against Defendants;
- B. Temporarily and permanently enjoin Defendants from engaging in the acts and practices set forth above that violate FDBR and FDUTPA;

- C. Award civil penalties as authorized by FDBR (Fla. Stat. § 501.72(1)) up to \$150,000 per violation and FDUTPA (Fla. Stat. §§ 501.2105; 501.2075) up to \$10,000 per violation, and attorney's fees;
- D. Order Defendants to pay court costs and all costs associated with distributing or executing on any restitution or judgment made by this Court;
- E. Grant such other and further legal or equitable relief as justice requires.

Dated: October 13, 2025

Respectfully submitted,

**JAMES UTHMEIER
ATTORNEY GENERAL
STATE OF FLORIDA**

GRADYLAW™

By: /s/ Thomas R. Grady
Thomas R. Grady (Fla. Bar No. 350702)
720 Fifth Avenue South, Suite 200
Naples, Florida 34102
trgrady@gradylaw.com and
jap@gradylaw.com

*Attorneys for Office of the Attorney General,
State of Florida, Department of Legal
Affairs*