common sense®

2021

PRIVACY OF STREAMING APPS AND DEVICES:

WATCHING TV THAT WATCHES US

Common Sense is the nation's leading nonprofit organization dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century.

common sense®

www.commonsense.org

Common Sense is grateful for the generous support and underwriting that funded this report from the Michael and Susan Dell Foundation, the Bill and Melinda Gates Foundation, and the Chan Zuckerberg Initative.

CREDITS

Authors: Girard Kelly, Common Sense Media
Jeff Graham, Common Sense Media
Jill Bronfman, Common Sense Media
Steve Garton, Common Sense Media

Data analysis: Girard Kelly, Common Sense Media
Jeff Graham, Common Sense Media

Copy editor: Jennifer Robb

Designer: Jeff Graham, Common Sense Media

Suggested citation: Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *Privacy of Streaming Apps and Devices: Watching TV that Watches Us*. San Francisco, CA: Common Sense Media This work is licensed under a Creative Commons Attribution 4.0 International Public License.

TABLE OF CONTENTS

Privacy of streaming apps and devices **1**

What are streaming services? . . . 1

Apps we rated . . . 1

How do streaming services make money? . . . 2

How we rate privacy . . . 2

What we found . . . 6

Compare privacy ratings . . . 6

What are streaming devices? . . . 7

How we test security . . . 7

Devices we rated . . . 8

What we found . . . 11

Compare privacy ratings . . . 11

Compare security practices . . . 12

Data sharing . . . 14

Data safety . . . 14

Account protection . . . 15

Parental consent . . . 16

Child privacy policy . . . 18

Advertisements, marketing, and tracking . . . 20

Software updates . . . 25

Security testing methodology . . . 25

Security framework . . . 25

Security testing . . . 26

Network testing environment . . . 27

Process overview . . . 28

What should parents and educators do? . . . 30

What should streaming apps and devices do? . . . 31

Children and data privacy . . . 32

Appendix **33**

Traffic analysis methodology 33

Tracking categories 33

App traffic analysis 34

Amazon Prime 34

Apple TV+ 34

Discovery+ 35

Disney+ 36

Hulu 37

Netflix 38

Paramount+ 39

HBO Max 41

Peacock 41

YouTube TV 43

Device traffic analysis 44

Amazon Fire TV Cube 44

Apple TV 48

Google TV 50

Nvidia Shield TV 53

Roku Smart Streaming Stick+ 56

"Do not sell" links 59

Apps 59

Devices 59

PRIVACY OF STREAMING APPS AND DEVICES

Consumers, parents, and educators are looking for streaming content services that can be used not only for entertainment and personal development, but also to support distance learning. However, many households don't have reliable high-speed internet or sufficient data plans to stream media content, let alone enough adequate devices, such as computers, laptops, TV sets, or tablets. Under these circumstances, children and students might use a parent's mobile device and parent's account to stream free media content or tutorials, which may result in the collection of behavioral information about their viewing habits and interactions with content that could lead to privacy risks[1] and harms that may affect children, students, and families. There are many articles available that compare all the "best" streaming apps and services on price, content catalog, and features. However, none of these articles adequately compares streaming apps and services on the most important feature—privacy. This report examines the privacy practices of the most popular streaming apps and devices.

What are streaming services?

Streaming media apps and services are typically free or paid subscription-based services that offer online streaming of TV shows and movies. Many paid streaming services offer a free trial period after giving a valid credit card number. Some streaming services are owned by major film studios that produce their own content, while other free streaming apps don't produce their own content, but simply integrate third-party apps to create content "channels." Some, of course, offer both original and shared content.

However, not all streaming apps are designed to be the same. There are easy-to-use streaming apps with only one type of subscription service, like Apple TV+ or Netflix, and more complex streaming apps that offer multiple subscription services with access to hundreds of other third-party content channels. There are even streaming apps designed only for one specific genre or type of content, like animated kids programming, cooking, sports or talk shows, or apps associated with only a particular film studio's content. Some streaming apps collect very little behavioral data, and some say they don't sell your data to third parties. But others are designed to collect as much behavioral data as possible, using thousands of data points to create a personalized profile about a user.

With so many apps to choose from, it was difficult to limit our selection, but we carefully selected the top 10 that we believe are representative of most types of streaming apps available across different platforms today. We chose streaming apps based on the film studios, features, type of content provided, Apple and Google App Store popularity, and the number of free and paid subscribers. We also chose streaming apps used by children and students in every major age group at home, on the go, and in the classroom.

Apps we rated

The streaming apps chosen for this report are listed in Table 1. All prices reflect the standard or basic streaming plan available as of the publication date of this report. Most streaming apps we tested offer free trial periods of varying lengths, and some include bundled discounts or add-ons if multiple streaming services are purchased together. Others have annual payment plan discounts, and most services have separate free, basic, or premium price plans based on the type of content available. In addition, many streaming services allow users to pay extra to stream additional content on-demand such as renting movies or TV shows that are not included in the product's main content catalog.

We evaluated the privacy policies of the top 10 streaming apps: Apple TV+,[2] YouTube TV,[3] Disney+,[4] Paramount+,[5] HBO Max,[6] Peacock,[7]

[1] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). Privacy risks and harms. San Francisco, CA: Common Sense Media, https://privacy.commonsense.org/resource/privacy-risks-harms-report.

[2] Apple TV+, https://www.apple.com/apple-tv-plus.
[3] YouTube TV, https://tv.youtube.com/welcome.
[4] Disney+, https://www.disneyplus.com.
[5] Paramount+, https://www.paramountplus.com.
[6] HBO Max, https://www.hbomax.com/.
[7] Peacock, https://www.peacocktv.com.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Amazon Prime Video,[8] Discovery+,[9] Hulu,[10] and Netflix.[11] There are also dozens of completely free and ad supported streaming services that aggregate third-party content such as Tubi TV[12], Crackle[13], IMDbTV[14], and PlutoTV[15]. Apple TV+ has only a single subscription plan, while Peacock has both free and paid price plans that include additional paid streaming content, such as live sports, original shows, and more channels. Paramount+ and Disney+ both have basic and premium subscription plans. HBO Max has both an "Ad Free" streaming plan and cheaper "With Ads" streaming plan with the same content. Hulu and Discovery+ have different levels of paid plans that still display limited advertisements, and plans that are more expensive but do not display any advertisements. Amazon Prime Video bundles its streaming service for free as part of its prime membership or as a paid stand-alone streaming service. YouTube TV is the most expensive streaming service we tested, but it is marketed differently than the other streaming services "except Hulu + Live TV" and is a replacement to a traditional cable television subscription. Lastly, Netflix has basic, standard, and premium subscription plans that are all tailored to the video quality of streaming content in SD, Full HD, or Ultra HD (4K).

Table 1: Streaming services price plans

Product	Price/mo.	Kids Content
Apple TV+	$4.99	Yes
YouTube TV	$64.99	Yes
Disney+	$7.99 to $29.99	Yes
Paramount+	$4.99 to $9.99	Yes
HBO Max	$9.99 to $14.99	Yes
Peacock	Free to $4.99	Yes
Amazon Prime Video	$8.99 to $12.99	Yes
Discovery+	$4.99 to $6.99	No
Hulu	$5.99 to $11.99	Yes
Netflix	$8.99 to $17.99	Yes

[8] Amazon Prime Video, https://www.amazon.com/Amazon-Video/b?node=2858778011.
[9] Discovery+, https://www.discoveryplus.com.
[10] Hulu, https://www.hulu.com/welcome.
[11] Netflix, https://www.netflix.com.
[12] Tubi TV, https://tubitv.com.
[13] Crackle, https://www.crackle.com/
[14] IMDB TV, https://www.imdb.com/tv.
[15] Pluto TV, https://pluto.tv/welcome.

How do streaming services make money?

Most streaming apps and services like traditional cable TV require a paid monthly subscription to stream unlimited content to any TV or device. There are also many free streaming apps that make money selling a user's behavioral or viewing data to third parties and displaying targeted advertisements. This data includes what shows or movies users watch, what devices are used to watch content, when users watch, what location users watch from, how often they watch, when they binge watch, and what recommended shows they choose to watch. Some companies use both "streams" of income, subscription plus data selling.

Most streaming apps also sell users' data to data brokers who serve targeted ads to users based on their viewing behavior and content they watched on other apps and services across the internet.

Many viewers know that free streaming apps are most likely selling their personal information, but most viewers may not know that most paid subscription streaming apps are also selling users' data. Even more expensive streaming plans with "no ads" or "limited ads" still collect viewing data from use of the app to track and serve users advertisements on other apps and services across the internet. Also, data brokers buy and sell users' data and share it with other companies for data recombination purposes.

How we rate privacy

Privacy and security are intertwined, and security is the foundation of effective individual privacy. When evaluating whether to have children use streaming apps at home or in the classroom, parents and teachers need to understand both the privacy policies and security practices of the device. To create a truly comprehensive evaluation process, the Common Sense Privacy Program completes a full, in-depth, 150-point inspection[16] of a product's privacy policies in order to offer privacy ratings[17] that are easy to understand.

[16] *See* Common Sense, Evaluation Questions, https://privacy.commonsense.org/resource/evaluation-questions.
[17] *See* Common Sense Privacy Ratings, https://privacy.commonsense.org/resource/privacy-ratings.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

	Apple TV+	YouTube TV	Disney+	Paramount+	HBO Max
Rating	**79%** Pass	**81%** Warning	**68%** Warning	**65%** Warning	**63%** Warning
Bottom Line	Apple TV+ is the only streaming service with privacy built-in by design.	YouTube TV is the best livestreaming service with over 85 top channels of entertainment and cloud DVR storage.	Disney+ has the latest releases, original series, movies, classic films, and TV shows from Disney, Pixar, Marvel, Star Wars, and National Geographic.	Paramount+ provides streaming access to TV series, stand-up shows, movies, reality, and kids shows from Nickelodeon, Comedy Central, BET, MTV, and Smithsonian Channel.	HBO Max is the streaming option for all of HBO, including original series, movies, specials, and more such as Sesame Workshop, DC Comics, Looney Tunes, and the Cartoon Network.
Pros	Apple says they don't sell users' data to third parties, don't display targeted advertisements, and don't track users on other apps and services across the internet.	YouTube TV received the highest overall numerical score, even with an orange "warning" rating, because Google TV had a more transparent policy despite engaging in some worse privacy practices.	Disney has some of the best practices in the categories of Parental Consent and Data Safety that includes safe interactions and privacy controls.	Paramount+ says they protect student data privacy if the product is used by students in K–12 schools and districts.	Parents can create a separate "Kids profile" for children to watch curated kid-friendly content without targeted advertisements.
Cons	Apple does not provide any information about how they protect student data privacy if the product is used by students in K–12 schools and districts.	YouTube TV says they don't sell users' data to third parties, but they do target users with advertisements and track users on other apps and services across the internet.	Disney's policy says it sells users' data, targets users with advertisements, and tracks users on other apps and services across the internet.	The Paramount+ policy says it sells users' data, targets users with advertisements, and tracks users on other apps and services across the internet.	The HBO policy says it sells users' data, targets users with personalized advertisements, and tracks users on other apps and services across the internet.

	Peacock	Amazon Prime Video	Discovery+	Hulu	Netflix
Rating	**59%** Warning	**57%** Warning	**54%** Warning	**53%** Warning	**46%** Warning
Bottom Line	Peacock provides free access to streaming movies and TV shows from *The Office*, *Parks & Rec*, *Yellowstone*, and NBCUniversal shows from Bravo, SYFY, USA, E!, and Oxygen.	Amazon Prime Video gives members a large selection of "included with Prime" streaming TV shows, Amazon originals, and movies without the need to subscribe to other third-party services.	Discovery+ provides streaming access to popular TV brands and personalities including HGTV, Food Network, TLC, ID, Animal Planet, and Discovery Channel.	Hulu provides streaming access to thousands of shows and movies, and live TV with over 65 channels with premium networks like HBO, Showtime, Cinemax, and Starz.	Netflix provides streaming access to award-winning original series, movies, documentaries, and stand-up specials.
Pros	Peacock says the service is intended for users of all ages, but individuals under the age of 13 may use the service with the consent of a parent or legal guardian.	Users can create separate profiles for personalized content recommendations and parents can create a separate "Kids" profile for children to watch curated kid-friendly content.	Discovery+ says in its privacy policy that it is only directed to adults and not intended for children under the age of 13.	Users can create separate profiles for personalized content recommendations and parents can create a separate "Kids" profile for children to watch curated kid-friendly content.	Users can create separate profiles for personalized content recommendations and parents can create a separate "Kids" profile for children to watch curated kid-friendly content.
Cons	Peacock's policy says it sells users' data, targets users with advertisements, and tracks users on other apps and services across the internet.	Amazon's policy says it does not sell users' data, but Amazon does say it targets users with advertisements, and tracks users on other apps and services across the internet.	The Discovery+ policy says it sells users' data, targets users with advertisements, and tracks users on other apps and services across the internet.	Hulu's policy says it sells users' data, targets users with advertisements, and tracks users on other apps and services across the internet.	Netflix's policy says it does not sell users' data, but Netflix does say it targets users with advertisements, and tracks users on other apps and services across the internet.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Table 2: Top 10 streaming apps
The information in this table provides a snapshot of each product's Common Sense privacy rating from February 1, 2021. Expert evaluators assessed different privacy-related concerns and ranked a product's practices from "best" to "poor," with special attention given to how these privacy practices affect kids and families. Score Key: Best (81–100); Good (61–80); Average (41–60); Fair (21–40); Poor (0–20). Rating Key: Pass (Meets our minimum requirements for privacy and security practices comprised of the Data Sold and Ads & Tracking concern categories); Warning (Does not meet our recommendations for privacy and security practices that includes at least one or more worse privacy practices or does not clarify certain practices in the Data Sold or Ads & Tracking concern categories); Fail (Does not have a privacy policy and/or does not use encryption and should not be used). Note that in addition to the qualitative portion of the rating,[18] the score is a quantitative measure and not an aggregate of the concern scores.[19] For an explanation on the score and rating for Apple TV+ and YouTube TV, reference the following section.

Product	Privacy Rating	Data Collection	Data Sharing	Data Security	Data Rights	Data Sold	Data Safety	Ads & Tracking	Parental Consent	School Purpose
Apple TV+	79% Pass	Good	Best	Good	Best	Average	Average	Good	Good	Poor
YouTube TV	81% Warning	Good	Best	Best	Best	Average	Good	Average	Good	Average
Disney+	68% Warning	Average	Good	Fair	Best	Fair	Good	Average	Best	Poor
Paramount+	65% Warning	Average	Good	Fair	Best	Fair	Poor	Average	Good	Average
HBO Max	63% Warning	Average	Good	Fair	Best	Fair	Average	Average	Best	Poor
Peacock	59% Warning	Average	Good	Fair	Best	Fair	Average	Average	Good	Poor
Amazon Prime Video	57% Warning	Average	Good	Average	Best	Average	Fair	Average	Average	Poor
Discovery+	54% Warning	Average	Good	Fair	Best	Average	Average	Average	Fair	Poor
Hulu	53% Warning	Average	Good	Average	Good	Fair	Fair	Average	Poor	Poor
Netflix	46% Warning	Fair	Average	Fair	Good	Poor	Poor	Average	Poor	Poor

[18] *See* Privacy Ratings, https://privacy.commonsense.org/resource/privacy-ratings.
[19] *See* Evaluation Scores, https://privacy.commonsense.org/resource/evaluation-scores.

What we found

The ratings and scores in Table 2 are from our privacy evaluation results of the top 10 streaming apps. Table 2 illustrates a range of privacy practices from "best" to "poor" based on our privacy ratings and evaluation concerns.[20] Products that score a "poor" are not necessarily unsafe, but they have a higher number of privacy problems than the "average" product. Similarly, products that score "best" are not necessarily problem free, but they had relatively fewer problems compared with other products.

From Table 2, you can see that YouTube TV[21] received our highest overall score, but Apple TV+[22] was the only product to earn a "pass" rating for better privacy practices that protect everyone. Netflix[23] received the lowest overall score with a "warning" rating. Specifically, Apple did better than Netflix in every category. YouTube TV received the highest overall score, even with a "warning" rating, because YouTube TV had the most comprehensive policy, despite engaging in some worse privacy practices which earned them a "warning" rating. How did this split occur? We give points for transparency.

YouTube TV's comparatively higher score, in other words, speaks to their transparency in telling us that they use our data and share it for advertising. Apple is less comprehensive and transparent in its policies (and could raise their score if they addressed more issues in their policies), but the fact that Apple's policy says that they do not share or use personal data for any advertising, marketing, or tracking earns them our highest "pass" rating.

In addition, Hulu[24] and Netflix did not have better practices than most other streaming apps in the category of Data Rights, which includes the user's ability to access, edit, delete, and export data. However, Apple TV+, YouTube TV, Amazon Prime Video[25], and Netflix were the only streaming apps that say they don't sell users' data. YouTube TV and Disney+[26] also have the best practices in the category of Data Safety that includes safe interactions and privacy controls, but Apple has the best practices in the category of Ads and Tracking than all of the other streaming apps. Also, most streaming apps including Peacock[27] and Discovery+[28] have either fair or average data collection and security practices.

Finally, Disney+ and HBO Max[29] have the best practices in the category of Parental Consent, but all of the streaming apps—except YouTube TV and Paramount+[30]—did not provide any information about how they protect student data privacy when used in K–12 schools and districts in the School Purpose category. However, use of streaming apps in schools or districts for educational purposes that require students to view documentaries or learning tutorials are typically outside the scope of the terms of use and license agreement of many streaming apps. This may change as streaming companies realize that their products are being used more and more in lesson plans at home and in the classroom by students.[31]

Compare privacy ratings

Table 3 compares the privacy practices of all the streaming apps we tested, as described in their privacy policies. These practices can put children's and students' privacy at risk if they sell personal data to third-party companies or use personal information for third-party marketing, targeted advertising, tracking, or ad-profiling purposes. In Table 3, "Yes" is considered a worse practice that puts children, students', and consumers' privacy at risk.

Our privacy evaluations of the top 10 streaming apps indicate that all streaming apps (except Apple TV+) have privacy practices that put consumers' privacy at considerable risk including selling data, sending third-party marketing communications, displaying targeted advertisements, tracking users across other sites and services, and creating advertising profiles for data brokers.

[20] *See* Common Sense Evaluation Concerns, https://privacy.commonsense.org/resource/evaluation-concerns.
[21] *See* Privacy Evaluation of YouTube TV https://privacy.commonsense.org/evaluation/YouTube-TV
[22] *See* Privacy Evaluation of Apple TV+ https://privacy.commonsense.org/evaluation/AppleTV
[23] *See* Privacy Evaluation of Netflix https://privacy.commonsense.org/evaluation/Netflix
[24] *See* Privacy Evaluation of Hulu https://privacy.commonsense.org/evaluation/Hulu
[25] *See* Privacy Evaluation of Amazon Prime Video https://privacy.commonsense.org/evaluation/Amazon-Prime-Video
[26] *See* Privacy Evaluation of Disney+ https://privacy.commonsense.org/evaluation/Disney
[27] *See* Privacy Evaluation of Peacock TV https://privacy.commonsense.org/evaluation/Peacock-TV
[28] *See* Privacy Evaluation of Discovery+ https://privacy.commonsense.org/evaluation/Discovery
[29] *See* Privacy Evaluation of HBO Max https://privacy.commonsense.org/evaluation/HBO-Max
[30] *See* Privacy Evaluation of Paramount+ https://privacy.commonsense.org/evaluation/Paramount
[31] *See* Swank K–12 Streaming, https://www.swank.com/k-12-streaming.

Table 3: Privacy rating criteria of streaming apps
Rating Key: Pass (Meets our minimum requirements for privacy and security practices comprised of the Data Sold and Ads & Tracking concern categories); Warning (Does not meet our recommendations for privacy and security practices that includes at least one or more worse privacy practices or does not clarify certain practices in the Data Sold or Ads & Tracking concern categories); Fail (Does not have a privacy policy and/or does not use encryption and should not be used). Note that in addition to the qualitative portion of the rating, the score is a quantitative measure and not an aggregate of the concern scores.

Product	Privacy Rating	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Apple TV+	79% Pass	No	No	No	No	No	No
YouTube TV	81% Warning	No	No	Yes	Yes	Yes	Yes
Disney+	68% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Paramount+	65% Warning	Yes	Yes	Yes	Yes	Yes	Yes
HBO Max	63% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Peacock	59% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Amazon Prime Video	57% Warning	No	Unclear	Yes	Yes	Yes	Yes
Discovery+	54% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Hulu	53% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Netflix	46% Warning	No	Yes	Yes	Yes	Yes	Yes

What are streaming devices?

Parents and educators are not just looking for streaming content services, but also streaming devices that can be used for entertainment, personal development, and to support distance learning. Streaming devices are hardware-based technology that have their own operating system software and remote control that allows users to easily connect the device to a TV and allow online streaming of shows and movies from streaming apps and services directly to their TV. Our hands-on security testing reveals which smart streaming devices are more protective of the privacy and security of kids', students', and consumers' personal information.

How we test security

We also do hands-on security testing of each smart device using Consumer Reports' Digital Standard.[32] The Digital Standard is a set of expectations for how smart tech manufacturers should handle privacy, security, and other digital rights. The goal of the Digital Standard testing criteria is to educate consumers about a product's privacy policy and security practices, and to influence smart tech manufacturers to take these concerns into consideration when developing their products.

The Privacy Program uses the Digital Standard to do hands-on basic security testing[33] of the 10 most critical security practices that parents and educators say they need to make an informed decision. These security practices include information collection from a smart device and its companion mobile application, and the transmission of information between the device and the internet.

In addition to basic security testing of these critical security practices, Common Sense created an 80-point security assessment[34] that incorporates Consumer Report's Digital Standard[35] with the Ranking Digital Rights[36] questions and OWASP IoT Security[37] questions.

[32] *See* Consumer Reports' Digital Standard, https://www.thedigitalstandard.org.

[33] *See* Common Sense Privacy Program: Security testing, https://privacy.commonsense.org/resource/security-testing.

[34] *See* Common Sense Privacy Program: Full Security Questions, https://privacy.commonsense.org/resource/full-security-assessment-questions.

[35] *See* Consumer Reports' Digital Standard, http://www.thedigitalstandard.org.

[36] *See* Ranking Digital Rights, https://rankingdigitalrights.org.

[37] *See* Open Web Application Security Project, https://owasp.org/.

Table 4: Streaming devices and technical specifications

Product	Price	Output	Processor	RAM	Storage	GPU
Apple TV HD	$149.00	1080p	A8 chip with 64-bit architecture	2 GB	32 GB	A8 Integrated Graphics
Google TV	$49.99	4K	Amlogic S905D3 (1.9 GHz quad-core ARM Cortex-A55)	2 GB	8 GB	Mali-G31 MP2 GPU
Amazon Fire TV Cube	$119.99	4K	Hexa-core (Quad-core at up to 2.2GHz + Dual-core at up to 1.9GHz	2 GB	16 GB	ARM Mali G52-MP2 (3EE), 800MHz
Roku Streaming Stick+	$39.99	4K	ARM Cortex A53	1 GB	512 MB	ARM Cortex Integrated Graphics
Nvidia Shield TV	$149.99	4K	Nvidia Tegra X1+ processor	2 GB	8 GB	256-core Nvidia GPU

Devices we rated

We tested the most popular smart streaming devices to identify the potential privacy risks and harms that may affect the children, students, and families who use these devices. It was difficult to limit our selection with so many smart streaming devices to choose from, but we selected the top five for this report that we believe are representative of most types of streaming devices available in the marketplace today. We chose smart streaming devices based on the company, product features, operating system, price, and popularity. We also chose smart streaming devices used by children and students in every major age group at home and in the classroom. We tested the following five devices: Apple TV,[38] Google TV,[39] Amazon Fire TV Cube,[40] Roku Streaming Stick+,[41] and Nvidia Shield TV.[42]

Regarding price, the Apple TV HD and Nvidia Shield TV are the most expensive streaming devices we tested. Apple's streaming device has the most storage capacity of any device we tested. All the streaming devices support 4K HDR output except for the Apple TV HD, but Apple also offers a more expensive Apple TV 4K model that was not included in our testing. Nvidia's streaming device is designed to work best for games with its GeForce Now streaming platform and includes additional accessories like the Shield Controller. The Chromecast with Google TV ("Google TV") is a low-cost streaming device compared to Apple and Nvidia that also allows users to play streaming games with Google Stadia. The Amazon Fire TV Cube is a mid-range cost streaming device but is more expensive than other Amazon Fire TV stick streaming devices because of its expanded storage capacity and faster processor. Lastly, the Roku Streaming Stick+ is the cheapest streaming device we tested with the least amount of RAM and storage capacity that is designed primarily to stream third-party content or "channels."

[38] *See* Apple TV, https://www.apple.com/tv.
[39] *See* Google TV, https://tv.google.
[40] *See* Amazon Fire TV Cube, https://www.amazon.com/all-new-fire-tv-cube-with-alexa-voice-remote/dp/B07KGVB6D6.
[41] *See* Roku Products, https://www.roku.com/products/streaming-stick-plus.
[42] *See* Nvidia Shield TV, https://www.nvidia.com/en-us/shield/shield-tv.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

	Apple TV	Google TV	Amazon Fire TV	Roku Streaming Stick+	Nvidia Shield TV
Rating	**79%** Pass	**81%** Warning	**57%** Warning	**51%** Warning	**43%** Warning
Bottom Line	The Apple TV is the easiest way to experience Apple TV+, and Apple's policy for this product says they do not collect data for any other purpose.	The Google TV integrates everything with your Google Account and brings all your streaming services together in one place.	Amazon's Fire streaming devices give members a large selection of "included with Prime" streaming TV shows, Amazon originals, and movies.	The Roku Streaming Stick+ allows users to easily integrate all the free and paid third-party subscription services they use.	By design, the Shield TV works with Android TV and integrates Google Account, Google Assistant, and streaming game services like Geforce Now.
Pros	Apple says they don't sell users' data to third parties, don't display targeted advertisements, and don't track users on other apps and services across the internet.	Google TV received the highest overall numerical score, even with an orange "warning" rating, because Google TV had a more transparent policy despite engaging in some worse privacy practices.	Users can create separate profiles for personalized content recommendations and parents can create a separate "Kids" profile for children to watch curated kid-friendly content.	The Roku Streaming Stick is intended for users of all ages and easy to set up.	Nvidia Shield TV is an Android TV-based streaming device that can stream both media and gaming content with Nvidia Geforce Now and Android gaming through the Google Play Store.
Cons	Apple did not receive the highest numerical score because they don't provide any information about how they protect student data privacy if the product is used in K–12 schools and districts.	Google says they don't sell users' data to third parties, but they do target users with advertisements and track users on other apps and services across the internet.	Amazon's policy says that they target users with advertisements, however, the service does not display interest-based ads to children when they are using a registered Amazon child profile.	Roku says they sell users' data to third parties, target users with advertisements, and track users on other apps and services across the internet.	Shield TV has the same privacy practices as Google's Android TV that target users with advertisements and track users on other apps and services across the internet.

Table 5: Top five streaming devices
The information in this table provides a snapshot of each product's Common Sense privacy rating from February 1, 2021. Expert evaluators assessed different privacy-related concerns and ranked a product's practices from "best" to "poor," with special attention given to how these privacy practices affect kids and families. Key: Best (81–100); Good (61–80); Average (41–60); Fair (21–40); Poor (0–20). Rating Key: Pass (Meets our minimum requirements for privacy and security practices comprised of the Data Sold and Ads & Tracking concern categories); Warning (Does not meet our recommendations for privacy and security practices that includes at least one or more worse privacy practices or does not clarify certain practices in the Data Sold or Ads & Tracking concern categories); Fail (Does not have a privacy policy and/or does not use encryption and should not be used). Note that in addition to the qualitative portion of the rating, the score is a quantitative measure and not an aggregate of the concern scores.

Product	Privacy Rating	Data Collection	Data Sharing	Data Security	Data Rights	Data Sold	Data Safety	Ads & Tracking	Parental Consent	School Purpose
Apple TV	79% Pass	Good	Best	Good	Best	Average	Average	Good	Good	Poor
Google TV	81% Warning	Good	Best	Best	Best	Average	Good	Average	Good	Average
Amazon Fire TV	57% Warning	Average	Good	Fair	Best	Fair	Good	Average	Best	Poor
Roku Streaming Stick+	51% Warning	Average	Good	Poor	Good	Fair	Fair	Average	Poor	Poor
Nvidia Shield TV	43% Warning	Average	Average	Poor	Good	Fair	Fair	Fair	Fair	Poor

What we found

From Table 5, you can see that Google TV[43] received our highest overall score but Apple TV[44] was the only product to earn a "pass" rating for better privacy practices that protect everyone. Apple, Google, and Amazon streaming devices all received the same overall score and privacy rating as their respective streaming apps (Apple TV+ YouTube TV, and Amazon Prime Video) because they all use the same policies to apply to both their streaming device hardware and their streaming app software. Nvidia Shield TV[45] received the lowest overall score with a "warning" rating. In fact, Nvidia had lower scores than Apple in every category. Google TV received the highest overall score even with a "warning" rating, because Google TV had the most comprehensive policy despite engaging in some worse privacy practices, which earned them a "warning" rating.

Google's comparatively higher score, in other words, speaks to their transparency in telling us that they use data and share it for advertising. Apple is less comprehensive in its transparency (and could raise their score if they addressed more issues in their policies), but the fact that Apple does not share or use personal data for any advertising, marketing, or tracking earns them our highest "pass" rating.

In addition, Apple TV, Google TV, and Amazon Fire TV[46] had better practices than the other streaming devices in the category of Data Rights, which includes the ability to access, edit, delete, and export data. Most importantly, the Roku Streaming Stick+[47] was the only streaming device that says they sell users' data. The Google TV and Amazon Fire TV have the best practices in the category of Data Safety that includes safe interactions and privacy controls, but Apple has the best practices in the category of Ads and Tracking than all of the other streaming devices.

Finally, Apple TV, Google TV, and the Amazon Fire TV have the best practices in the category of Parental Consent. Roku does allow parents to create child profiles on the streaming device, yet does not discuss this practice in their policies. All of the streaming apps—except Google TV—did not provide any information about how they protect student data privacy when used in K–12 schools and districts in the School Purpose category.

It is also important to understand that additional third-party installed "channels" or apps have different privacy practices than the default streaming device itself. Only the streaming devices' privacy practices were evaluated, but not the privacy practices of any third-party apps that may be installed by a user. Additional research has observed numerous Smart TV streaming apps that exfiltrate personally identifiable information (PII) to third parties and platform-specific parties, mostly for nonfunctional advertising and tracking purposes.[48] Therefore, before installing any third-party additional apps, parents and educators should check their privacy policies or Common Sense privacy ratings to understand how these apps may treat data differently than the streaming device.

Compare privacy ratings

Table 6 compares the privacy practices of all the streaming devices we tested which are used to determine their privacy ratings. These practices can put children's and students' privacy at risk by selling personal data to third-party companies or by using personal information for third-party marketing, targeted advertising, tracking, or ad-profiling purposes. In Table 6, "Yes" is considered a worse practice that puts children, students', and consumers' privacy at risk.

Our privacy evaluations of the top five streaming devices indicate that all streaming devices—except Apple TV—have privacy practices that put consumers' privacy at considerable risk including selling data, sending third-party marketing communications, displaying targeted advertisements, tracking users across other sites and services, and creating advertising profiles for data brokers. The collection of behavioral information about viewing habits and interactions with streaming devices for advertising and tracking purposes could lead to privacy risks and harms that may affect consumers and their children, students, and families.

[43] *See* Privacy Evaluation of Google TV https://privacy.commonsense.org/evaluation/Google-TV

[44] *See* Privacy Evaluation of Apple TV https://privacy.commonsense.org/evaluation/Apple-TV

[45] *See* Privacy Evaluation of Nvidia https://privacy.commonsense.org/evaluation/NVIDIA

[46] *See* Privacy Evaluation of Amazon Fire TV https://privacy.commonsense.org/evaluation/Amazon-Fire-TV

[47] *See* Privacy Evaluation of Roku https://privacy.commonsense.org/evaluation/Roku

[48] *See* J. Varmarken, H. Le, A. Shuba, A. Markopoulou, Z. Shafiq, "The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking", Proceedings of the Privacy Enhancing Technologies Symposium (PoPETs) 2020, Issue 2. July 2020, Montreal, Canada. https://petsymposium.org/2020/files/papers/issue2/popets-2020-0021.pdf

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

Table 6: Privacy rating criteria of streaming devices
Rating Key: Pass (Meets our minimum requirements for privacy and security practices comprised of the Data Sold and Ads & Tracking concern categories); Warning (Does not meet our recommendations for privacy and security practices that includes at least one or more worse privacy practices or does not clarify certain practices in the Data Sold or Ads & Tracking concern categories); Fail (Does not have a privacy policy and/or does not use encryption and should not be used). Note that in addition to the qualitative portion of the rating, the score is a quantitative measure and not an aggregate of the concern scores.

Product	Privacy Rating	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Apple	79% Pass	No	No	No	No	No	No
Google	81% Warning	No	No	Yes	Yes	Yes	Yes
Amazon	57% Warning	No	Unclear	Yes	Yes	Yes	Yes
Roku	51% Warning	Yes	Yes	Yes	Yes	Yes	Yes
Nvidia	43% Warning	No	Unclear	Yes	Yes	Yes	Yes

Compare security practices

Our hands-on security testing of the following streaming apps and devices focused on the 10 most critical security practices around the collection of information from the device and on the transmission of information between the device and the internet.

Table 7: Streaming device software and voice assistant integration

Device	Software	Voice Assistant
Apple TV	Apple tvOS	Siri
Google TV	Android TV	Google
Amazon Fire TV	Fire OS	Alexa
Roku Streaming Stick	Roku OS	Alexa
Nvidia Shield TV	Android TV	Google

All the streaming devices we tested use different operating systems, with the exception of the Nvidia Shield TV, which is a value-add retailer that runs a custom version of Google's Android TV operating system that is optimized for Nvidia's GeForce Now gaming platform. Amazon's Fire OS is Amazon's proprietary operating system that is available on Amazon's entire product line of Fire TV streaming devices. Google uses its Android TV operating system on its own Google TV device and its product line of Google Chromecast and Chromecast Ultra devices. The Roku OS proprietary operating system is used on all Roku streaming devices that include its streaming player devices and Roku TV, which is installed on various third-party smart TV manufacturers.

There is a clear differentiation between the integration of three different voice assistants, depending on the streaming device manufacturer and operating system. Apple integrates its own voice assistant "Siri"[49] into its streaming devices, which is exclusive to Apple products and not available to any third party for use. However, Amazon's "Alexa"[50] voice assistant is integrated into all of its Fire TV streaming devices and is available for integration into any third-party manufacturer's device, such as Roku's streaming products. Similarly, Google's voice assistant, "Google"[51] is integrated into all of its streaming devices and is also available for integration into any third-party manufacturer's device, such as Android TV based streaming products, including the Nvidia Shield TV.

[49] *See* Privacy Evaluation of Apple Siri, https://privacy.commonsense.org/evaluation/Apple-Siri.
[50] *See* Privacy Evaluation of Amazon Alexa, https://privacy.commonsense.org/evaluation/Amazon-Alexa.
[51] *See* Privacy Evaluation of Google Assistant, https://privacy.commonsense.org/evaluation/Google-Assistant.

Table 8: Privacy policy notice displayed during device setup

Device	Notice Provided
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	Yes
Nvidia Shield TV	Yes

During the Apple TV device set-up process Apple requires users to consent to its Privacy Policy,[52] Apple tvOS Terms and Conditions,[53] Apple TV Warranty,[54] iCloud Terms and Conditions,[55] and Game Center Terms and Conditions.[56] For the Google TV, the set-up process is also quick, and Google requires users consent to its Terms of Service,[57] Play Terms of Use,[58] and Privacy Policy[59] before using the device.

However, Amazon's Fire TV takes its obligation of providing adequate notice to consumers of its policies to a completely different level than Apple or Google, who only require consent to a handful of different policies. Amazon requires users to log in with their Amazon account and then provides notice of an exceptionally high number of policies that users must read and provide consent before use of their new streaming device.[60] In addition, Amazon requires consumers consent for using the voice assistant Alexa with two more policies: the Alexa Privacy Hub,[61] and Alexa & Alexa Device FAQs.[62]

The Roku Streaming Stick+ requires users consent to the Roku Privacy Policy,[63] Roku Account Terms,[64] and Roku Products Terms of Use.[65] The Nvidia Shield TV requires users consent to Google's Terms of Service,[66] Google Privacy Policy,[67] and the

[52] *See* Apple Privacy Policy, https://www.apple.com/legal/privacy/en-ww.

[53] *See* Apple tvOS Software License Agreement, https://www.apple.com/legal/sla/docs/tvOS14.pdf.

[54] *See* Apple One (1) Year Limited Warranty, https://www.apple.com/legal/warranty/products/accessory-warranty-english.html.

[55] *See* iCloud Terms and Conditions, https://www.apple.com/legal/internet-services/icloud/en/terms.html.

[56] *See* Apple Game Center Terms and Conditions, https://www.apple.com/legal/internet-services/itunes/gamecenter/us/terms.html.

[57] *See* Google Terms of Service, https://policies.google.com/terms?hl=en.

[58] *See* Google Play Terms of Use, https://play.google.com/about/play-terms/index.html.

[59] *See* Google Privacy Policy, https://policies.google.com/privacy?hl=en.

[60] Amazon requires users provide consent to the following twenty-five (25) policies before use of the Fire TV device: Amazon Device Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=202002080; Conditions of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000; Amazon Privacy Notice, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496; Alexa Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740; Amazon Prime Video Terms of Use, https://www.primevideo.com/help?nodeId=202095490; Amazon Prime Usage Rules, https://www.primevideo.com/help/?nodeId=G202095500; Amazon Video Third-party Software, https://www.amazon.com/gp/help/customer/display.html?nodeId=201422780; IMDB Conditions of Use, https://www.imdb.com/conditions; IMDB Privacy Notice, https://www.imdb.com/privacy; IMDB Android Legal Notice, https://www.primevideo.com/terms; Amazon Music Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201380010; Amazon Appstore for Android Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201485660; Additional Terms relating to Appstore Software, https://www.amazon.com/gp/feature.html?ie=UTF8&docId=1000797711; Amazon Coins Terms, https://www.amazon.com/gp/help/customer/display.html?nodeId=201434520; Amazon Photos Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201376540; Amazon Game Circle Terms of Use, https://www.amazon.com/gp/help/customer/display.html/?ie=UTF8&nodeId=201487670; Amazon Payments, Inc Customer Agreement, https://pay.amazon.com/help/201212430; Amazon Payments Privacy Notice, https://pay.amazon.com/help/201751600; Amazon Prime Terms, https://www.amazon.com/gp/help/customer/display.html?nodeId=G2B9L3YR7LR8J4XP; About Our Returns Policies, https://www.amazon.com/gp/help/customer/display.html/?nodeId=201819200; Audible Service Conditions of Use, https://www.audible.com/legal/conditions-of-use; Amazon Device Return FAQs, https://www.amazon.com/gp/help/customer/display.html/?ie=UTF8&nodeId=201818950; State Sales Tax Information, https://sellercentral.amazon.com/gp/help/external/G201706680?language=en_US; Amazon Silk Terms and Conditions, https://www.amazon.com/gp/help/customer/display.html?nodeId=200775270; and Amazon Fire TV Device Terms of Use, https://www.amazon.com/gp/help/customer/display.html?nodeId=201267340.

[61] *See* Alexa Privacy Hub, https://www.amazon.com/b/?node=19149155011.

[62] *See* Alexa and Alexa Device FAQs, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230.

[63] *See* Roku Privacy Policy, https://docs.roku.com/published/userprivacypolicy/en/us.

[64] *See* Roku Account Terms, https://docs.roku.com/published/usertermsandconditions/en/us.

[65] *See* Roku Products Terms of Use, https://docs.roku.com/published/deviceplayereula/en/us.

[66] *See* Google Terms of Service, https://policies.google.com/terms?hl=en.

[67] *See* Google Privacy Policy, https://policies.google.com/privacy?hl=en.

Google Play Terms of Service.[68] After users consent to Google's policies they are provided an additional notice and required to consent to the Nvidia's Terms of Use[69] and the Nvidia Privacy Policy.[70]

In total, Apple requires users consent to five policies, Google and Roku both require users consent to three policies, and Nvidia requires users consent to two policies. However, these companies policies all reference additional supplemental policies that users automatically agree to as well, which serve to inflate the number of actual words and policies that users are providing their consent when they click "I agree."

Users should not be required to provide informed consent to numerous policies that would take hours to navigate with a remote, read, and understand on a TV screen in order to use their new streaming device or service with only a single click that says "I agree." The concept that a consumer actually gives "informed consent" to use streaming apps or devices is far from reality.

Data sharing

Evaluating data sharing takes into consideration best practices of keeping personal data inside the application or smart device to help protect privacy. Any time personal data is available on the internet or on another device, the possibility of unauthorized sharing or breach is increased. Connecting social media accounts could allow children or students to share personal information with other people and with third-party companies. In addition, installing third-party apps with a smart device could allow the collection and use of personal information for a different purpose.

Table 9: Devices integrates third-party apps

Device	Third-Party Content
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	Yes
Nvidia Shield TV	Yes

[68] *See* Google Play Terms of Use, https://play.google.com/about/play-terms/index.html.
[69] *See* Nvidia Terms of Use, https://www.nvidia.com/en-us/geforce-now/terms-of-use/.
[70] *See* Nvidia Privacy Policy, https://www.nvidia.com/en-us/about-nvidia/privacy-policy/.

All of the streaming devices allow sharing a user's data and integrate with third-party subscription services or "channels" such as Netflix,[71] YouTube TV,[72] Prime Video,[73] Disney+,[74] Apple TV+,[75] HBO Max,[76] and more. In addition, all the streaming devices can integrate free ad-supported streaming services such as Tubi TV[77], Pluto TV,[78] IMDb TV,[79] and others. The Apple TV with Apple TV+ and Amazon Fire TV Cube with Prime Video are the only two streaming devices that by default integrate their own first-party original content and therefore those devices by design share less data with third-party service providers unless additional third-party subscription channels or apps are added to the software of the device by the user.

Data safety

Evaluating data safety in the context of data privacy takes into consideration best practices of using privacy protections by default and limiting potential interactions with others. It's better to start with the maximum privacy that the app or device can provide and then give users the choice to change the settings. It's also better to have people opt in to sharing rather than forcing them to opt out if they want to protect their privacy. In addition, users talking to other people through the app or device might permit personal information to be shared with strangers or be made publicly available.

Table 10: Privacy protecting default controls are enabled

Device	Default Protecting
Apple TV	Yes
Google TV	No
Amazon Fire TV	No
Roku Streaming Stick	No
Nvidia Shield TV	No

[71] Netflix, https://www.netflix.com.
[72] YouTube TV, https://tv.youtube.com/welcome.
[73] Amazon Prime Video, https://www.amazon.com/Amazon-Video/b?node=2858778011.
[74] Disney+, https://www.disneyplus.com.
[75] Apple TV+, https://www.apple.com/apple-tv-plus.
[76] HBO Max, https://www.hbomax.com.
[77] Tubi TV, https://tubitv.com.
[78] Pluto TV, https://pluto.tv/welcome.
[79] IMDB TV, https://www.imdb.com/tv.

Each of the streaming devices have different opt in or opt out default privacy settings with some incorporating privacy-by-default[80] principles by selecting the most privacy-protecting settings by default. However, default privacy settings of a streaming device are not always consistent with the default privacy settings of additional third-party apps that may be installed. The privacy settings of third-party apps should also be checked to ensure they respect your choices. The Apple TV was the only streaming device that used privacy-by-design to require opt in consent for any data sharing and set default privacy controls to the most privacy-protecting settings. Apple provided clear notice during the device set-up process of Apple's "Data and Privacy Notice" summary and link to "Learn More Privacy Notice" that links to Apple's privacy policy. The Apple TV provided notice to users to provide opt in consent to "share audio recordings" of Siri voice commands for research purposes. In addition, Apple provided notice to users to opt in to using and sharing "Location Services," and sharing TV usage data for first-party "Apple TV Analytics" and Third-Party "Developer App Analytics."

The Google TV set-up process required users authenticate with their Google Account and provided notice of additional legal terms that require agreement with Google Device Arbitration Agreement[81] and use of Google Services to "Use Location" and "Help Improve Chromecast" both of which use a checkmark to indicate consent, but are pre-checked, meaning the user must opt out of sharing data for these additional purposes. The onboarding experience following up with another notification that "Google uses activity to improve recommendations." By activity, they usually mean "your data," and by "recommendations," they usually mean ads. Within the "Privacy Settings" menu of Google TV, there are additional options for "Scanning always available for other networks" which can share WIFI SSID location information, and "Usage and Diagnostics," and "Limit Ad Tracking" which are associated with a user's cross-device Google Account privacy settings.

The Amazon Fire TV Cube set-up process is different from the Apple or Google streaming device set-up process because there is no notice of privacy settings or choices a user can make about sharing data. Only after the Amazon Fire TV Cube device has completed setup can users navigate to the "Settings" menu item, select "Preferences," then "Privacy Settings" and make privacy choices about whether to share "Device Usage Data" or whether to "Collect App Usage Data," share "Data Monitoring," or display "Interest-Based Ads" which are all enabled by default.

The Roku Streaming Stick+ set-up process did not display notice of privacy settings or choices a user can make about sharing data. Only after the Roku device has completed setup can users navigate to the "Settings" menu, and choose to opt in to the single privacy setting "Limit Ad Tracking" which is not enabled by default. This setting is worded in such a way that it may be misleading that opting in to limiting a worse practice is actually opting out of use of your data for that worse practice, which is not a principle of privacy by design.

Lastly, the Nvidia Shield TV uses the default Android TV settings and only provides privacy choices with respect to the user's Google account settings for sharing "Location Data" and "Usage & Diagnostics" data and the "Limit Ad Tracking" setting as part of the user's Google profile which are not enabled by default.

Account protection

Evaluating account protection takes into consideration best practices of using strong passwords and providing accounts for children with parental controls. Strong passwords can help prevent unauthorized access to personal information. Children younger than 13 may not understand when they are sharing personal information, so they should be required to create special accounts with more protection under the law. Lastly, parents can help children younger than 13 use a device or app with digital well-being protections in mind by using parental controls.

Table 11: Strong Passwords are Required for Accounts

Device	Strong Passwords
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	Yes
Nvidia Shield TV	Yes

[80] *See* General Data Protection Regulation (EU) 2016/679 (GDPR), Art. 25, Recital 78.

[81] *See* Google Terms, https://policies.google.com/terms?hl=en; Google Arbitration Agreement, https://support.google.com/store/answer/9427031?hl=en.

All the streaming devices include the use of company-specific user accounts that need to be created either on the device itself, or with another mobile device or computer in order to log in and use the streaming device. The Apple, Google, Amazon, Roku, and Nvidia streaming devices all recommend using strong passwords with an account in order to use the device and protect a user's personal information from unauthorized access.

Parental consent

For children age 13 or younger, a parent or guardian's verifiable consent is required before the collection, use, or disclosure of the child's personal information to an application or service.

Table 12: Child Age Gates are Used

Device	Age Appropriate User
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	Yes
Nvidia Shield TV	Yes

All of the streaming devices are intended for a general audience and require users to be older than 18 in order to create an account with the service and use the device. In addition, there is notice provided on all devices during the account creation process that users are not eligible to sign up for an account with the service if they enter a birth date or birth year that indicates they are younger than 18 years old. Also, all users during the account creation process must provide a form of payment, such as a credit card, to their account to verify that it is owned by an individual over the age of 18 and to purchase or rent media content on each streaming device.

Table 13: Parental Controls are Available

Device	Parental Controls
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	No
Nvidia Shield TV	No

Providing parental controls or settings for each streaming device is an industry best privacy-protecting practice that allows parents to provide parental consent for the collection and disclosure of personal information from their children.

Apple requires a parent to provide consent for a child account through the Family Sharing setting of their Apple ID account on another Apple device, where they can create an Apple ID for their child. A parent must first review Apple's parent privacy disclosure,[82] then enter their child's personal information, including an iCloud.com email address and a password that meets strong and complex password requirements. Parental controls for a child profile will move over to the Apple TV+ website[83] and child account users will need to request permission from their parent or guardian to download apps, rent movies, and watch content. However, content restrictions set through parental controls on the Apple TV+ website do not apply to Apple TV+ in the Apple TV app on iPhone, iPad, iPod touch, Apple TV, Mac, smart TVs, or other streaming devices.

The Google TV user experience is tied to the signed-in Google account holder's settings that apply to any service the user is logged in to with their Google account. The Google TV device has settings to add a different Google account and provides an option for parents to create separate child profiles. After a parent provides consent to create a profile for their child, Google provides notice that a child profile is tied to a parent's account and will not have a username or password associated with their profile. In addition, parents can manage their child's account to set ground rules with activity controls, screen time, content ratings, and restrictions on installing apps and devices through Google Family Link[84] and YouTube Kids.[85]

The Amazon Fire TV Cube provides settings on the device with parental controls that are restricted by a five-digit PIN. After the parental controls are enabled, additional settings can be selected such as "PIN Protect Purchases," "Viewing Restrictions" of content based on age rating, and PIN Protect App Launches and the Amazon Photos App. However, Amazon does provide its own curated kids' content

[82] *See* Apple Family Privacy Disclosure for Children, https://www.apple.com/legal/privacy/en-ww/parent-disclosure.
[83] Apple TV+, https://tv.apple.com.
[84] *See* Privacy Evaluation of Family Link, https://privacy.commonsense.org/evaluation/Google-Family-Link.
[85] *See* Privacy Evaluation of YouTube Kids, https://privacy.commonsense.org/evaluation/YouTube-Kids.

through a separate Amazon Kids+ service,[86] which has a separate terms[87] and is all-in-one subscription that gives kids access to thousands of kid-friendly books, movies, TV shows, educational apps, Audible books, and games on compatible Fire, Fire TV, Android, iOS and Kindle devices.

The Roku Streaming Stick+ did provide parental controls to restrict content based on age rating and the creation of a PIN through the Roku website[88] after authentication. However, parental controls are available only if a user accesses the "Roku Channel" in a "logged-in" state. Parental control content restrictions apply only to viewing within the Roku Channel, and did not affect any other channels. In addition, setting a PIN does not prevent users from exiting the Roku Channel and accessing content from another channel. The PIN is only required to make purchases and add items from the Roku Channel Store.

The Nvidia Shield TV did not include parental controls or the option to create a separate child profile during the Google account creation and device set-up process. However, the device did provide the option of different users of the device with the use of an "Owner" and "Restricted Profile." The restricted profile can be used by parents to allow only certain approved apps or "channels" to be used by their kids or teens on the device in the restricted mode, which requires a four-digit PIN to leave restricted mode. However, once an app or channel is approved for use with the restricted account, the use of that third-party service is not restricted with respect to its data collection practices.

Table 14: Child Profiles are Available on Device

Device	Child Profile
Apple TV	No
Google TV	Yes
Amazon Fire TV	No
Roku Streaming Stick	No
Nvidia Shield TV	No

Parental controls give parents more control over their child's use of a streaming device which allows for the creation of a separate "profile" for their child with different content moderation filters. Parents expect a child profile to also have better privacy protecting practices that include limiting the collection of personal information to only the data required to provide the service, and the prohibition on use of a child's data for targeted advertising, marketing communications, or other tracking or advertising profile purposes.

However, even if a company provides parents with the option of creating a child profile, the company can still collect data from kids when the child uses the device for the first time after its initial set-up before a child profile has been created, or when a child is using the device outside of their restricted account. The child profiles or restricted accounts on the streaming devices we tested are primarily used for content moderation of age-appropriate content and restriction of the use of installing and using third-party apps.

Table 15: Child Profiles are Available on App

Device	Child Profile
Apple TV+	None
YouTube TV	None
Disney+	Yes
Paramount+	Yes
HBO Max	Yes
Peacock	None
Amazon Prime Video	Yes
Discovery+	None
Hulu	Yes
Netflix	Yes

Parents need to know that parental controls focus on age-appropriate content rather than data collection practices.

Disney+, Paramount+, HBO Max, Amazon Prime Video, Hulu, and Netflix all allow users to create separate profiles for personalized content recommendations and for parents to create a separate "Kids" profile for children to watch curated kid-friendly content. In addition, Paramount+ child profiles provide additional segmentation that support a "kids mode" with a choice between "Younger Kids" (TV-Y) or "Older Kids" with content ratings up to (PG)

[86] Amazon Kids+ https://www.amazon.com/kidsplus.
[87] *See* Amazon Kids+ Terms & Conditions, https://www.amazon.com/gp/help/customer/display.html?nodeId=201222340.
[88] *See* Roku Account Settings, https://my.roku.com.

Table 16: Streaming Device Child Privacy Policy

Device	Child Policy	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Apple TV	Yes	No	No	No	No	No	No
Google TV	Yes	No	No	No	Yes	Yes	Unclear
Amazon Fire TV	Yes	No	Unclear	No	Unclear	Unclear	Unclear
Roku Streaming Stick	No	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Nvidia Shield TV	No	No	Unclear	Unclear	Unclear	Unclear	Unclear

in order to better recommend age-appropriate content to younger viewers. All of the streaming services we tested provide kid—and family—directed TV shows and movies, except Discovery+.

Apple TV+, YouTube TV, and Peacock also include kids and family content directed to children under 13 years of age on their streaming platforms, but these services do not allow for the creation of separate child profiles or accounts. Apple TV+ is the only streaming service without a child profile feature that still protects children's privacy because Apple provides better privacy protecting practices for all of its users, regardless of their age.

Child privacy policy

Streaming apps and devices with kid and family directed content should minimally include child profiles or child accounts to provide a safer experience with age-appropriate content recommendations and better privacy practices that protect children's data when they are using the streaming app or device. Additional privacy protections that apply to children's data when using separate child profiles also need to be clearly communicated to parents with a separate child privacy policy that explains what stronger privacy protecting practices are in place when children are using the streaming app or device.

Apple's privacy policy says that it protects the privacy of all the users of its Apple TV streaming device and therefore the use of a separate child profile would not change Apple's already default better privacy-protecting practices that earned it a "Pass" privacy rating. In addition, Apple's Family Privacy Disclosure for Children[89] policy says personalized ad settings cannot be enabled for a child's Apple ID. Apple says a child will not receive advertising targeted to their interests from Apple's advertising platform on devices associated with a child's Apple ID. However, a child will still be able to receive non-targeted contextual advertising on those devices. In addition, the "Allow Apps to Ask to Track" setting on devices is turned off and cannot be enabled. Apps and advertisers are restricted from accessing the "Advertising Identifier" provided by an Apple device's operating system, and are also responsible for complying with Apple's guidelines prohibiting them from engaging in targeted advertising or advertising measurement, or sharing information with data brokers.

Google's use of a child profile on the streaming device allows parents to change the content recommendations to be age appropriate, and use better privacy practices that prohibit targeted advertisements to protect children's privacy. Children may still see contextual advertising based on information, like the content of the show or movie a child is viewing, the current search query, or general location such as a city or state. However, Google's Family Link[90] Disclosure for Parents of Children Under 13[91] says that third-party tracking of children using child profiles may still occur from specific third-party partners for advertising and measurement purposes, using their own third-party cookies or similar tracking technologies.

[89] *See* Apple Family Privacy Disclosure for Children, https://www.apple.com/legal/privacy/en-ww/parent-disclosure.

[90] *See* Privacy Evaluation of Family Link, https://privacy.commonsense.org/evaluation/Google-Family-Link.

[91] *See* Google Family Link Disclosure for Parents of Children under 13, https://families.google.com/familylink/privacy/notice; Privacy Notice for Google Accounts and Profiles Managed with Family Link, for Children under 13, https://families.google.com/familylink/privacy/child-policy.

Amazon's Children's Privacy Disclosure[92] policy says they will not serve any interest-based advertisements[93] to children when using child profiles or accounts. However, Amazon's privacy policy[94] and child privacy policy does not disclose whether children may still receive third-party marketing communications, or are tracked by third parties on other apps or services across the internet.

Lastly, Roku and Nvidia's privacy policies do not disclose any additional privacy protections for children and also do not not provide any separate child profile accounts on their streaming devices. Roku is the only streaming device that allows for selling data of users to third parties. In addition, Roku's privacy policy does not disclose any prohibition on selling data of children under 16 years of age.[95]

As shown in Table 17, both Apple TV+ and Google's YouTube TV have separate child privacy policies, but only Apple TV+ protects children's privacy across all indicators. Disney+ also has a separate Children's Privacy Policy[96] and related Online Tracking Technologies and Advertising[97] policy, but does not disclose whether additional privacy protections are in place for children such as prohibitions on targeted advertisements, third-party marketing communications, or tracking children across other apps or services. In addition, Disney has a California Consumer Privacy Act[98] policy, but does not disclose whether data from children under 16 years of age are excluded from sale to third parties, or whether parents can opt out of the sale of their child's data on their behalf.

Paramount+, which is owned by ViacomCBS, says in their Children's Privacy Policy[99] that they prohibit the sale of data from children under 13 years of age. In addition, their cookie policy[100] says cookies on child-directed services prohibit targeted advertisements and no third-party tracking is allowed. Paramount+ has better privacy practices for children across all indicators except one: third-party marketing. Paramount+ says they may share children's information with sponsors and other third-party partners for contests, giveaways, and sweepstakes.

HBO Max has an integrated Children's Privacy Policy[101] section in their main privacy policy[102] that says HBO may use children's information collected through "Kids Profiles" to show marketing offers, promotions, and contextual advertisements based on what the child is watching. HBO's California and CCPA Privacy Rights and Disclosures[103] section of their privacy policy says they do not sell the information of California consumers under 16 years of age. However, HBO's policy does say third parties may use cookies or similar technologies to understand and personalize a child's online experience within the service for advertising and the content a child is watching and on other apps and services across the internet.

Peacock, which is owned by NBCUniversal, has a separate Children's Privacy Policy[104] that also says children may receive third-party marketing communications for contests and sweepstakes. However, the policy does not disclose any prohibitions on the sale of children's data to third parties or prohibitions on the use of children's data for targeted advertisements or third-party tracking.

Discovery+ says in its privacy policy[105] that it is directed to adults and not intended for children under the age of 13. Therefore, it is expected that Discovery+ would not provide a separate child privacy policy or disclose any additional privacy protections for children. However, Discovery+ has content that would likely appeal to children and especially

[92] *See* Amazon's Children's Privacy Disclosure, https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560.

[93] *See* Amazon-Interest-Based Ads, https://www.amazon.com/b/?&node=5160028011.

[94] *See* Amazon Privacy Notice, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496.

[95] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code §§1798.115(a)(1)-(3), 1798.115(c)(1), 1798.120(c), 1798.135(a)(2)(A)-(B), 1798.140(t)(1).

[96] *See* The Walt Disney Company, Children's Privacy Policy, https://privacy.thewaltdisneycompany.com/en/for-parents/childrens-online-privacy-policy.

[97] *See* The Walt Disney Company, Online Tracking Technologies and Advertising, https://privacy.thewaltdisneycompany.com/en/privacy-controls/online-tracking-and-advertising/

[98] *See* The Walt Disney Company, California Consumer Privacy Act (CCPA), https://privacy.thewaltdisneycompany.com/en/dnsmi.

[99] *See* ViacomCBS, Children's Privacy Policy, https://www.viacomcbsprivacy.com/en/childrens.

[100] *See* ViacomCBS, Cookie Policy, https://www.viacomcbsprivacy.com/en/cookies.

[101] HBO Max, Children's Privacy Policy, https://www.hbomax.com/privacy/en-us#otnotice-section-960b6cd7-87f8-4f59-9225-b4da79e1aad2.

[102] HBO Max Privacy Policy, https://www.hbomax.com/privacy.

[103] HBO Max, California and CCPA Privacy Rights and Disclosures, https://www.hbomax.com/privacy/app#page11381-band50811.

[104] *See* NBCUniversal, Children's Privacy Policy, https://www.nbcuniversal.com/privacy/Children.

[105] *See* Discovery, Privacy Notice, https://corporate.discovery.com/privacy-policy.

Table 17: Streaming App Child Privacy Policy

App	Child Policy	Sell Data	Third-Party Marketing	Targeted Ads	Third-Party Tracking	Track Users	Ad Profile
Apple TV+	Yes	No	No	No	No	No	No
YouTube TV	Yes	No	No	No	Yes	Yes	Unclear
Disney+	Yes	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Paramount+	Yes	No	Yes	No	No	No	No
HBO Max	Yes	No	Yes	No	Unclear	Unclear	Unclear
Peacock	Yes	Unclear	Yes	Unclear	Unclear	Unclear	Unclear
Amazon Prime Video	Yes	No	Unclear	No	Unclear	Unclear	Unclear
Discovery+	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Hulu	No	Unclear	Unclear	Unclear	Unclear	Unclear	Unclear
Netflix	No	No	Unclear	Unclear	Unclear	Unclear	Unclear

students in K–12 classrooms with its Animal Planet content with documentaries customized to helping children learn about the natural world and Discovery's annual "Shark Week" event that is used by educators across the country to encourage students to learn more about marine biology. As such educators and parents should carefully consider the implications of using content platforms not intended for children because there are no additional privacy protections put in place.

Similarly, Hulu's privacy policy[106] and Netflix's privacy policy[107] say the services are intended only for adults, and children under 13 years of age are not permitted to register with the services. These streaming services say they are not intended to be used by children without the involvement and approval of a parent or guardian.

However, Hulu and Netflix both provide kid—and family targeted—TV shows and movie content to children and provide parents with the ability to create separate child profiles, with the expectation children would use and interact with the service to view kid-friendly content. Hulu and Netflix do not provide a separate child privacy policy or disclose any additional privacy protections for children. Therefore, Hulu and Netflix need to put in place stronger privacy practices with separate child privacy policies to better protect children and use their existing child profile account features to allow parents to enable stronger privacy protections for children.

Adequate privacy protections for children typically require a separate child profile and child privacy policy that clarifies different data collection and use practices are in place for child accounts. However, none of the streaming apps and devices provided a separate child profile with stronger privacy practices for children across all evaluation criteria. Although Apple allows the creation of child accounts with Family Accounts, and Google allows the creation of child accounts through Family Link, all streaming apps and devices need a separate child profile which have stronger privacy-protecting data collection and use practices for children already in place.

Parental controls, PINs, or restricted child accounts are not sufficient to protect a child's data unless additional privacy protections are put in place.

Advertisements, marketing, and tracking

Responsible advertising practices limit the use of personal information for any third-party marketing, targeted advertising, tracking, or profiling purposes.

[106] *See* Hulu Privacy Policy, https://www.hulu.com/privacy.
[107] *See* Netflix, Privacy Statement, https://help.netflix.com/legal/privacy.

Table 18: Marketing messages are sent

Device	Marketing Messages	Method
Apple TV	No	None
Google TV	Yes	Opt-in
Amazon Fire TV	Yes	Opt-in
Roku Streaming Stick	Yes	Opt-out
Nvidia Shield TV	Yes	Opt-in

The Apple TV registration process did not provide notice of any marketing communications that may be sent to the user and Apple did not send any first-party or third-party marketing communications to the user's Apple ID email address after setup of the Apple TV. During the Google TV registration process users are provided opt in consent to sign up for Google's "Stay in the Know" marketing communications. After the Google TV setup is complete the user receives a service notification email from Google titled, "Welcome to Chromecast with Google TV" which provides additional notice of opt in consent to explore third-party apps for use with the Google TV and sign-up for Google's "Stay in the Know" marketing communications about new Google hardware products, and related features, services, and offers.

The Amazon Fire TV registration process sent a first-party marketing communication after set-up was complete titled "Welcome to the Fire TV Family" which encouraged the user to learn more about their new device and purchase colorful remote covers.[108] However, Amazon did not send any third-party marketing communications to the user's Amazon account email address after setup of the Fire TV device.

The Roku Streaming Stick+ registration process did not provide opt in notice and consent of marketing communications. Instead Roku sends both first-party (Roku) and third-party (Channels) marketing communications that are opt out. Roku sent an initial email communication titled, ``Roku! Let's get started'' which includes third-party content labeled "Free channels to check out" that will add those third-party services into the user's Roku streaming software. Roku follows up with a second marketing communication a day later titled "Meet your new home for free and premium TV" which encourages the user to "Add a premium subscription on the Roku Channel and enjoy all your favorites in one place." Roku continues to send marketing communications every other day reminding subscribers to use their Roku device and sign up for more third-party channels. Roku's marketing emails include subjects such as "You've got 3 months of Apple TV+ for free*. Just for Roku customers," and to explore new third-party app categories. Roku does include an unsubscribe feature at the bottom of every marketing communication.

The Nvidia Shield TV registration process includes notice of Google's policies and opt in consent to "Get the Most out of Google Assistant" marketing communications. In addition, Nvidia prominently displays notice of opt in consent to "Join Shield Rewards!" which offers free third-party content trial subscriptions with third-party email marketing promotions. The choices to join Shield Rewards may be confusing: Users need to choose to have a direct relationship with Google or Nvidia. The choices are as follows: Not Now (Default), Use my Google Account, Use a Different Email, Don't Show Me Again, and View Privacy Policy.

Table 19: Advertising is displayed

Device	Displayed Ads	Content
Apple TV	First-party	Apple TV+
Google TV	Third-party	Special Offers
Amazon Fire TV	First-party	Prime Video
Roku Streaming Stick	Third-party	Special Offers
Nvidia Shield TV	First-party	Nvidia Games

Advertising may be displayed within each third-party "channel" or subscription service, regardless of the device used. For example, viewing content in the "Netflix" channel or "Prime Video" channel on any streaming device may display first-party video advertisements for TV shows and movies and other media content from that provider. Table 19 only looks at advertising displayed by the device itself, irrespective of any third-party apps or channels which display their own advertising for third-party content that are used interchangeably.

The Apple TV displayed no advertisements during the device set-up process, but did show first-party Apple TV+ previews for Apple original TV shows and movies available on Apple TV+ while

[108] *See* Made for Amazon Remote Cover Case, for Alexa Voice Remote - Candy Red, https://www.amazon.com/Amazon-Mission-Cables-All-new-controls/dp/B07JCJP2N5.

using the device. The Google TV displayed no advertisements during the device set-up process, but did show third-party subscription content previews for TV shows and movies available on Peacock, Apple TV+, HBO Max, and Tubi TV while using the device.

The Amazon Fire TV Cube displayed no advertisements during the device set-up process, but did show first-party Prime Video previews for free and pay-per-view Amazon original TV shows and movies available on Prime Video while using the device. In addition, the Fire TV also displays third-party subscription content previews for TV shows and movies available on other channels.

The Roku Streaming Stick+ displays third-party advertisements for "Add More Channels" during the device set-up process and another advertisement to join "Free Trials" of third-party subscription services, such as Showtime, StarZ, Paramount+, AMC+, and many more. The user is required to scroll past all the available third-party subscriptions to the very bottom of the screen to continue with the set-up process. After the device set-up process is complete, the Roku displays first-party vertical banner advertisements for Roku products while using the device to "Buy Another Roku Device" and a full-screen video advertisement to sign up for Roku's premium "Roku Express Service."

The Nvidia Shield TV displayed no advertisements during the device set-up process, but does show first-party featured games from Nvidia Games, which is part of Nvidia's GeForce Now subscription service. In addition, the device displays a "App Spotlight" banner advertisement at the bottom of the home screen that says it is featured by Google Play.

Our observational analysis and classification of advertising and tracking domains that were sent and received by each streaming device is displayed in Table 20. We indicate whether any primary domains are classified as trackers, based on the open source Tracker Radar project from DuckDuckGo.[109] The Track Radar tool is not a block list, but is a data set of the most common third-party domains on the web with information about their behavior, classification, and ownership. Each observed domain in our security testing is classified by Tracker Radar into the following advertising and tracking categories that are relevant to streaming apps and devices: **AP**: Action Pixels; **AF**: Ad Fraud; **AMT**: Ad Motivated Tracking; **AD**: Advertising; **AM**: Audience; Measurement; **SN**: Social Networking; and **TPAM**: Third-Party Analytics Marketing.[110] Additional information about the classification of each domain for each streaming app or device is available in the Appendix.

It is also important to understand that the presence of trackers in each classification only looks at unique primary domains and not their subdomains which could have multiple requests and used for a potentially non-tracking purpose. Also, presumed first-party requests from the streaming app or device are not counted as a third-party domain tracker in our analysis. Therefore, any first-party domain requests that are owned by their respective company are excluded—even if Tracker Radar would have classified the domains as trackers if observed in other companies' products.

Observing first- or third-party trackers is an important step in validating a product's privacy practices, but it is also an ephemeral process that is constantly changing. Tracking the trackers is simply a snapshot in time based on the most up-to-date knowledge we have of each particular tracker's past behavior.

In addition, a domain may not be counted as a tracker in our analysis because Tracker Radar has not yet collected information about that particular domain or subdomain with DuckDuckGo's Tracker Radar Collector.[111] Moreover, Tracker Radar is a data set of the most common third-party domains on the web which was not necessarily designed to apply to known tracking domains from streaming mobile applications and devices. However, our analysis still indicates that streaming apps and devices that use trackers should be more carefully scrutinized by parents and educators before use, and their privacy policies carefully read to better understand their privacy practices. Lastly, our observational results of trackers are simply a snapshot of behavior we observed from a streaming app or device on a specific date and time in our particular network environment, which could change based on different testing configurations or real world use.

[109] DuckDuckGo Tracker Radar, https://github.com/duckduckgo/tracker-radar.

[110] DuckDuckGo Tracker Radar, Categories, https://github.com/duckduckgo/tracker-radar/blob/main/docs/CATEGORIES.md.

[111] DuckDuckGo Tracker Radar Detector, https://github.com/duckduckgo/tracker-radar-collector.

Table 20: Tracking behavior based on domain or primary domain contacted
Abbreviated columns are as follows: (**AP**) Action Pixels, (**AF**) Ad Fraud, (**AMT**) Ad Motivated Tracking, (**AD**) Advertising, (**AM**) Audience Management, (**SN**) Social Network, (**TPAM**) Third-Party Analytics Marketing. For further explanation, see appendix Tracking Categories.

Device	AP	AF	AMT	AD	AM	SN	TPAM
Apple TV	No	No	No	No	No	No	No
Google TV	No	No	Yes	Yes	No	No	No
Amazon Fire TV	No	No	No	No	No	No	No
Roku Streaming Stick	No	No	Yes	Yes	No	No	No
Nvidia Shield TV	Yes	Yes	Yes	Yes	Yes	Yes	Yes

The Apple TV sent and received requests from Apple related cloud services and third-party domains, but did not send or receive any presumed third-party advertising or tracking domain requests.[112] This better privacy-protective observational behavior is expected from a product with a highly transparent privacy policy that received a high overall score and "Pass" privacy rating. These better practices also align with our privacy evaluation criteria that require products not engage in third-party tracking of users. However, the Google TV sent and received requests to both third-party advertising and tracking domains, such as DoubleClick, that could be used for tracking or profiling for advertising purposes.[113]

The Amazon Fire TV Cube primarily sent and received network requests during testing to Amazon-related cloud services and also included first-party advertising and tracking domains, such as Amazon's Adsystem and AWS analytics, which are not counted in this analysis, but are used for third-party advertising and tracking purposes on other sites and services.[114] The Roku Streaming Stick+ also sent and received requests to known third-party advertising domains such as the advertising service DoubleClick, that could be used for tracking or profiling purposes.[115]

The Nvidia Shield TV sent and received data to both third-party advertising and tracking domains, such as Google Syndication and Facebook, even though no Facebook account login was displayed or used during testing, which means a user's data could be used by third parties for tracking or profiling purposes.[116]

Additionally, our observation of domain requests indicated many streaming devices used unencrypted requests to send and receive data for the purpose of displaying cover artwork for TV shows and movies from third-party content providers, to collect data analytics, and to display advertisements from third-party ad networks; all could potentially expose streaming device users to a Man-in-the-Middle (MiTM) attack.[117] Encrypting all data sent and received between the streaming device and the internet is an industry standard best practice which prevents the interception of unencrypted traffic and its modification by an attacker who could include malicious or nefarious content. This potential harm is especially acute for child users of streaming devices who are using restricted profiles and viewing content that is specifically moderated to be age appropriate. Without reasonable security practices in place that include industry standard encryption of the content and cover artwork sent and received by the streaming device, there is an increased risk of the possible interception or injection of harmful or offensive images into a child's viewing experience.

In Table 21 as part of our limited observational testing of the streaming apps and devices we found all apps and devices sent and received data from presumed third-party domains—except Apple TV+, which did not send or receive any third-party domain requests as indicated by NA. For third-party advertising and tracking domains, Apple TV+, YouTube TV, HBO Max, Amazon Prime Video, and Netflix all had better observational privacy practices of no known presumed third-party tracker domains classified by Tracker Radar. However, both Amazon Prime Video and YouTube TV did have presumed first-party domains that were classified as trackers

[112] *See* Appendix, Apple TV.
[113] *See* Appendix, Google TV.
[114] *See* Appendix, Amazon Fire TV Cube.
[115] *See* Appendix, Roku Streaming Stick+.
[116] *See* Appendix, Nvidia Shield TV.

[117] Internet Society, Fact Sheet: Man-in-the-Middle Attacks, https://www.internetsociety.org/wp-content/uploads/2020/03/Man-in-the-Middle-Fact-Sheet.pdf.

Table 21: Tracking behavior based on domain or primary domain contacted
Abbreviated columns are as follows: (**AP**) Action Pixels, (**AF**) Ad Fraud, (**AMT**) Ad Motivated Tracking, (**AD**) Advertising, (**AM**) Audience Management, (**SN**) Social Network, (**TPAM**) Third-Party Analytics Marketing. For further explanation, see appendix Tracking Categories.

App	AP	AF	AMT	AD	AM	SN	TPAM
Apple TV+	NA	NA	NA	NA	NA	NA	NA
YouTube TV	No	No	No	No	No	No	No
Disney+	No	No	Yes	Yes	Yes	No	Yes
Paramount+	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HBO Max	No	No	No	No	No	No	No
Peacock	No	No	Yes	Yes	Yes	No	Yes
Amazon Prime Video	No	No	No	No	No	No	No
Discovery+	No	No	Yes	Yes	Yes	No	Yes
Hulu	Yes	Yes	Yes	Yes	Yes	No	Yes
Netflix	No	No	No	No	No	No	No

which were not counted as part of our analysis because they were owned by their respective first-party company, but they would have been considered third-party trackers if observed in other products. Therefore, there is an inherent bias against classifying third-party trackers for large companies who own and control the full product lifecycle from hardware to hosting infrastructure, content creation, and delivery through cloud software services. Smaller companies who create only a mobile application or hardware as a value-added retailer need to rely heavily on third party companies to integrate third-party content and cloud services which would therefore result in observation of more third-party advertising and tracking technologies.

Tracking behavior provides valuable insight into how streaming services share data, but reading the privacy policies is also required to complete the whole picture of how a product can still use or share a user's data.

Paramount+, Peacock, and Hulu all had worse observational privacy practices because they had the most unique presumed third-party tracking domain requests, such as Facebook,[118] Google Doubleclick,[119] and Scorecard research.[120] Our observations indicate these streaming apps are sharing a user's data with the greatest number of known third-party advertising and tracking companies. If a streaming app or device only sends and receives data to their own first-party primary domains, then we are unable to observe what the streaming app and device actually does with the personal information they collect after they have received it. However, just because we only observed a streaming app or device communicating with first-party primary domains does not mean that the app or device does not either communicate directly or indirectly with third parties through another method that was not observed during testing.

For streaming apps and devices with parental controls and child profiles, we also analyzed the domain requests sent and received without parental controls or child profiles enabled, and also after parental controls or child profiles had been enabled and were in use on each app or device. As expected, because parental controls are primarily used to restrict age-inappropriate content and not to limit data collection from child profiles, we did not observe any significant change in the unique domain requests sent and received by the streaming apps or devices with or without parental controls or child profiles in use.

[118] *See* Facebook, https://www.facebook.com.

[119] *See* Google Marketing Platform, https://marketingplatform.google.com/about/enterprise.

[120] Scorecard Research, https://www.scorecardresearch.com/home.aspx.

Software updates

Evaluating software updates takes into consideration best practices of keeping a smart device secure with up-to-date software patches and settings. When a company improves its app or device, better privacy and security should be part of the package and should be automatically updated or easy to update.

Table 22: Software Updates are Automatically Installed

Device	Updates Automatic
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	Yes
Nvidia Shield TV	Yes

All streaming devices provided firmware updates, either during or after the set-up process was complete. However, parents and educators should also keep in mind that all smart devices may not continue to provide software updates past the product's warranty. And if smart devices do not receive regular security updates and patches, there could be an increased risk to a child's or student's personal information.

Table 23: Software Update Transmissions are Secure

Device	Updates Secure
Apple TV	Yes
Google TV	Yes
Amazon Fire TV	Yes
Roku Streaming Stick	No
Nvidia Shield TV	Yes

Software updates should always be transferred securely to the device with encryption to ensure malware or other harmful software is not unintentionally installed on the device, which could compromise the privacy of all users' personal information collected from the device and companion applications.

The Apple, Google, Amazon, and Nvidia devices were all observed downloading firmware and software updates with encryption to the devices. However, the Roku Streaming Stick+ was observed sending a large amount of nonencrypted data[121] during the firmware update process. During the update process, all devices displayed a notice that the software update was being verified. It is possible that the Roku software update download was verified on the device before installation to ensure the updates were not corrupted or contain malware, but this is not a security best practice to send firmware updates over the internet without reasonable security protections.

Security testing methodology

To begin, Common Sense conducted a hands-on basic security assessment of the 10 most critical security practices around the collection of information from a smart device and from a companion mobile application with the internet, and the transmission of information between the device and the app. These 10 critical questions are organized into five categories which were derived from the Consumer Reports "Digital Standard" testing criteria.[122] In addition to a basic security assessment of the 10 most critical security practices of a smart device, the Common Sense Privacy program created a full, 80-point inspection of the security practices of a smart device and mobile application.[123]

Security framework

The following five "Smart Tech" evaluation concern categories comprise 10 basic security questions. These security questions illustrate the diverse security-related issues needed to complete a basic security assessment of smart tech devices:

Data sharing. Evaluating data sharing takes into consideration best practices of keeping personal data inside the application or smart device to help protect privacy. Connecting social media accounts could allow people to share personal information with other people and with third-party companies. In addition, installing third-party apps with a smart

[121] The Roku Streaming Stick+ downloaded firmware over port 80 from the domain http://firmware.roku.com.

[122] *See* Consumer Reports, The Digital Standard, https://www.thedigitalstandard.org.

[123] *See* Common Sense Privacy Program, Full Security Assessment Questions, https://privacy.commonsense.org/resource/full-security-assessment-questions.

device could allow the collection and use of personal information for a different purpose. Criteria for Data Sharing include sharing with: 1) social media accounts and 2) the third-party app store.

Data safety. Evaluating data safety takes into consideration best practices of using privacy protections by default and limiting potential interactions with others. It's better to start with the maximum privacy that the app or device can provide, and then give users the choice to change the settings.[124] In addition, users talking to other people through the app or device might permit sharing personal information with strangers. Criteria for Data Safety include: 3) providing privacy-protecting controls and 4) limiting social interactions.

Account protection. Evaluating account protection takes into consideration best practices of using strong passwords and providing accounts for children with parental controls. Strong passwords can help prevent unwanted access to personal information. Children younger than 13 may not understand when they are sharing personal information, so they should be required to create special accounts with more protection under the law.[125] Lastly, parents can help children under the age of 13 use a device or app with digital well-being protections in mind by using parental controls. Criteria for Account protection include: 5) requiring a strong password, 6) displaying an age gate, and 7) providing parental controls and optional child profile.

Device security. Evaluating device security takes into consideration best practices of securing personal information against unwanted use that is shared between the mobile device, smart tech, and the internet. Keeping personal information encrypted,[126] or masked,[127] helps to protect information while it is transmitted.[128] In addition, advertising and tracking requests from the device or app could contain personal information about the user, including what they're doing with the device or app. Criteria for Device Security include: 8) securing data and 9) ads and tracking requests.

Software updates. Evaluating software updates takes into consideration best practices of keeping a device secure with up-to-date software patches and settings. When a company improves its app or device, better privacy and security should be part of the package and should be automatically updated or easy to update. Criteria for Software Updates include: 10) updates available.

Security testing

To perform basic information security testing we created a "blank slate" testing environment that monitored only the data sent and received between a smart device, its companion mobile application, and the internet.[129] This included purchasing and setting up networking hardware equipment to monitor network traffic in order to create a specific type of testing environment. Also, iOS[130] and Android[131] mobile devices were used for testing and each was factory reset without any personal information loaded onto the device in order to test only a single companion mobile application at a time. Additionally, software was installed on our local computer for network packet analysis.[132]

There are several different types of information security testing that could be used to monitor network traffic and determine security vulnerabilities of smart devices. Some methods make extensive use of an intercepting software proxy to observe, and in some cases modify, encrypted network requests generated by the application.[133] There are also mobile application frameworks that can be used with Android mobile devices or jailbroken[134] iOS

[124] *See* General Data Protection Regulation (EU) 2016/679 (GDPR) (generally, provides for data subjects to opt in); *See also* California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.140 (generally, provides for data subjects to opt out).

[125] COPPA, 16 C.F.R. Part 312.

[126] Encryption is the process of converting information or data into a code, to prevent unauthorized access.

[127] Data masking is the process of hiding original data with modified content, used to protect data.

[128] De-encryption is the conversion of encrypted data into its original form. Reidentification is the practice of matching anonymous data with publicly available data or auxiliary data in order to discover the individual to which the data belongs. While encryption or anonymization are not perfect, these measures provide some security over allowing unencrypted data to pass over public channels (i.e. passed from product to product via internet protocols).

[129] *See* Ren, Jingjing, Dubois, Daniel J., Choffnes, David, Mandalari, Anna M., Kolcun, Roman, Haddadi, Hamed, *Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach*, IMC '19: Proceedings of the Internet Measurement Conference, Oct. 2019, pp. 267–279, https://doi.org/10.1145/3355369.3355577.

[130] iOS is a mobile operating system created and developed by Apple Inc. for iPhone.

[131] Android is an open-source operating system used for smartphones and tablets.

[132] *See* OWASP Zed Attack Proxy (ZAP), https://www.zaproxy.org/.

[133] Intercepting proxies are tools used to analyze the normal session created between a client and server.

[134] Jailbreaking refers to the process of removing all restrictions imposed on an iOS device.

devices to gain root administrator level access[135] to the mobile operating system in order to observe network requests from a mobile application to the internet. However, these advanced approaches are still limited for the purposes of our basic security testing because they can observe 1) decrypted network traffic between the mobile application and the internet, and 2) decrypted network traffic between the smart streaming device and the mobile device, but they cannot decrypt and observe data sent from the smart device directly to the internet.

When researching which method to use for our basic information security testing we considered how difficult it would be for nontechnical educators and students to reproduce our network testing environment for their own educational and testing purposes.[136] Therefore, we designed our method of basic information security testing to be used as part of a project-based collaborative development experience for both teachers and secondary students to increase their experience with and knowledge of hands-on software and hardware tools and how to test the privacy and security of a mobile application, online service, or smart device. Through the unifying theme of learning about smart technology, teachers and students could work together to learn various technologies (focusing on their individual interests and use of the technology). They could also use this process to consider how to protect their privacy and gauge the security of their data while engaging with everyday smart technologies, like streaming devices.

We believe the following testing process that uses a hardware-based network environment testing approach with the preconfigured open-source data analysis software Security Onion is the easiest method to set up and start security testing smart devices quickly with educators and students.[137] Security Onion software provides an out-of-the-box solution that is easy to install on a computer and provides extensive documentation for educators and students to learn how to perform basic security analysis.[138]

In addition, Security Onion software also provides the flexibility for more advanced security testing for students if desired. Security Onion can also be installed in a virtual machine, which allows students and researchers without access to the devices to reproduce the testing results and investigate the findings themselves by importing the original pcap (packet capture of network traffic) data used for testing.

Overall the goal of designing the testing environment was to get educators and students to start testing the privacy and security of smart devices with minimal effort and a small learning curve. Therefore, we believe the following network testing environment relies more on basic hands-on networking and operating system installation skills, rather than extensive computer science knowledge of open-source software tools and Unix administration processes[139] often used by security professionals to configure information security testing environments.

Network testing environment

The diagram below illustrates the basic network topography environment used for testing all five streaming devices. However, it is important to note that every network hardware configuration is different and may require different devices to connect to the internet, such as a DSL[140] or cable modem, router, or gateway, that may need to be configured to allow the network switch in our diagram below to connect to the internet.

The following list describes the components required for the testing environment:

The internet. The basic information security testing environment requires that all devices be connected to the internet in order to make and receive network requests that can be captured and analyzed by the Security Onion server. This type of security testing environment attempts to recreate as closely as possible the real-world interaction, data collection, and use of streaming devices and companion mobile applications running on a smartphone.[141]

Network switch. The switch in our testing environment can be a low-cost device that is used to connect a wireless access point[142] to the internet and

[135] Root administrator access provides all privileges to the operating system of an Android mobile device.

[136] While some of the audience for our research may be a CTO or IT professionals, we also seek to inform school district administrators and classroom teachers who may have no technical background.

[137] Security Onion, https://securityonion.net/.

[138] *See* Security Onion Documentation, https://securityonion.readthedocs.io/en/latest/.

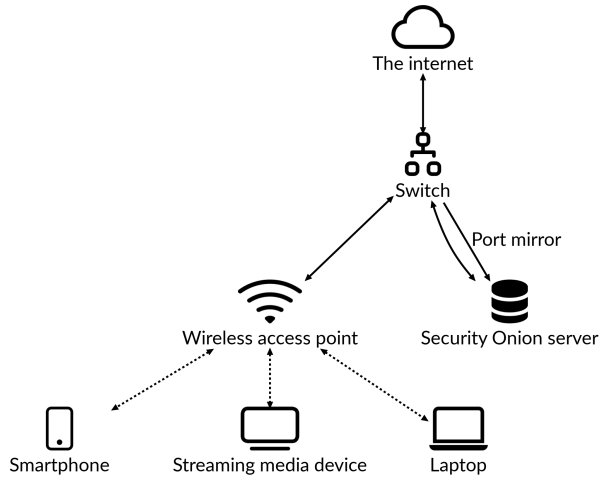
[139] Unix is an operating system which supports multi-tasking and multi-user functionality.

[140] A digital subscriber line (DSL) is a device used to connect a computer or router to a telephone line which provides connection to the internet.

[141] iOS or Android varieties.

[142] A network switch is a networking hardware device that connects other devices on a computer network by using packet

Figure 1: Image of network testing environment structure.



also connect a Security Onion server for monitoring all network packets received by the wireless access point. In order to monitor all the network packets that are sent and received from the streaming device to the internet, our testing environment used a switch with port mirroring.[143]

Security Onion server. Security Onion is a free and open-source Linux distribution for intrusion detection, enterprise security monitoring, and log management.[144] The software is available in a downloadable image that can be used to create a bootable USB device that allows users to quickly install the network monitoring server on a personal computer that meets the sufficient hardware requirements. The Security Onion server captures network traffic[145] from the wireless access point on the mirrored port of the network switch for security analysis.

Wireless access point. The wireless access point in our testing environment can be a low-cost device to connect wireless devices for basic information security testing to the network switch and the internet. This network configuration allows for the network switch to mirror all network packets[146] from the wireless access point that uses Wi-Fi to another port on the network switch for packet capture and analysis by the connected Security Onion server.[147]

Streaming device. Each streaming device used for testing was wirelessly connected to the wireless access point only one at a time to ensure data captured originated from a specific device because the network switch will mirror all network traffic from the streaming device to another port on the network switch for the Security Onion server to capture for analysis of that specific smart device.

Smartphone. A low-cost Android or iOS smartphone can be used in the testing environment with the mobile application used to control the streaming device installed. The mobile device was "factory reset" before use, meaning that the operating system had been reinstalled and no other applications were installed on the device to avoid inadvertent data collection during our basic information security testing. The mobile device was wirelessly connected to the wireless access point and the network switch mirrored all network traffic from the mobile application on the smartphone to another port on the network switch for the Security Onion server to capture for analysis.

Laptop. A low-cost laptop in our testing environment was used to connect to the wireless access point and access the basic information security testing tools on the Security Onion Server through a web browser or over a SSH terminal session.[148]

Process overview

The basic information security testing process was designed into three modules to analyze several different security-related data points with Security Onion to determine the security practices of the smart device and companion mobile application.

1) *What type of network requests are being sent and received from the streaming device and the mobile application?* This module illustrates what type of secure or unsecure requests are sent from the smart device to the internet and requests received between the smart device and

switching technology to receive and forward data from the source device to the destination device.

[143] Port mirroring is used on a network switch to send a copy of all network packets received on a designated switch port to a network monitoring connection on another switch port. This is commonly used for network devices that require monitoring or network traffic such as an intrusion detection system (IDS).

[144] Security Onion, https://securityonion.net/.

[145] Network traffic is the data set for this testing methodology. It is the flow of data from inside the product to the outside world.

[146] A packet is a unit of data that is routed between an origin and a destination on the internet or any other packet-switched network.

[147] *See* Security Onion Documentation, https://securityonion.readthedocs.io/en/latest/.

[148] Secure Shell (SSH) is a cryptographic network protocol for operating network services securely through terminal emulation software.

mobile application. This analysis provides users with more information about whether reasonable security practices, such as encryption, are used to protect personal data while in transit from its source to its destination.

2) *What destinations are network requests sent to?* This module illustrates what third-party companies send and receive data from a smart device and mobile application. Intuitively, most smart devices and mobile applications communicate primarily with the manufacturer's online web services, but often third-party advertising or tracking services can be seen sending or receiving data from the smart device or mobile application.

3) *How much data is shared with the company or third parties?* This module illustrates the total amount of bytes sent from the smart device or mobile application to the company's servers or third parties. This analysis provides users with more information about when data is collected and how much data is actually collected.

This three-step modular process is helpful to illuminate who the smart device and mobile application are talking to (the company or third-party servers), but is limited because it does not show the content of the data that is actually being sent between the parties because it is likely encrypted.

Security Onion software. After the network testing environment is deployed successfully and the streaming device, mobile device, and laptops can access the internet through the wireless access point, then users need to install Security Onion on a personal computer or laptop attached to the network switch. After installation of the Security Onion server, users can use their laptops to connect to the Security Onion server and begin the information testing modules that teach basic security monitoring skills. It includes preconfigured network security testing software applications and utilities, such as Elasticsearch, Logstash, Kibana, Snort, Suricata, Zeek, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security analysis tools.[149]

Testing limitations. However, there are limitations with this basic information testing approach. First, our testing results are simply a snapshot of behavior we observed from a smart device and mobile application on a specific date and time in our particular network environment, which could change based on different testing configurations or real-world use.[150] In addition, firmware updates to the smart device and software updates to the companion mobile application could also change expected observational behavior from what was observed during our testing period.[151]

Second, our testing can only see what data is transferred from one device or server to another, but not subsequent data processing or sharing with third parties.[152] For example, a smart device or mobile app may only send and receive data to one destination server address, such as Amazon's web services, before forwarding the data packets off to other third-party domains to be processed elsewhere. Users will be unable to observe what the first-party company (e.g., Amazon Web Services in this example) actually does with the personal information it collects after it has received it. Therefore, we believe reading the privacy policies of these smart devices is also a critically important part of evaluating the privacy and security of a streaming device.

In addition to observing the smart device's data collection and sharing practices, it is important to know how each company promises it will process personal data after it has been collected. Combining some knowledge of actual data flows, as we have done in this testing, with the legal obligations described in the privacy policies puts more of the crucial puzzle pieces on the table. Putting them together into a coherent whole, however, requires more work.

[149] *See* Elasticsearch, https://www.elastic.co/; Logstash, https://www.elastic.co/logstash; Kibana, https://www.elastic.co/kibana; Snort, https://www.snort.org/; Suricata, https://suricata-ids.org/; Zeek, https://zeek.org/; Wazuh, https://wazuh.com/; Squil, https://bammv.github.io/sguil/index.html; Squert, https://github.com/int13h/squert; CyberChef, https://gchq.github.io/CyberChef/; NetworkMiner, https://www.netresec.com/index.ashx?page=NetworkMiner.

[150] Our observational testing was conducted from single use observation for each app or device from January 2021 to June 2021

[151] Firmware is data that is stored on a hardware device that provides instructions on how that device should operate. Firmware updates are one of the weak points in IoT security, particularly where the devices are either not updated at all and considered disposable once the initial software has become outdated, or require the user to locate and perform manual updates. In contrast to firmware updates and their security limitations, software updates may be effectuated automatically from the server, without user input, or, with user input but with the click of a button.

[152] The term "third parties" is somewhat misleading in the sense that it implies only one entity might receive the data, in a single transaction. In actuality, data brokers and other initial recipients of the data often forward and resell this information over multiple transactions, combine data with other data for use and sale, and store data for future use and sale.

Advanced techniques. Currently, the basic information security testing modules are designed to only analyze the source and destination of network traffic requests to determine where data is sent and received. Educators and students interested in privacy and security research are not expected to use packet analysis to review the actual content of the data transferred between devices, apps, and the internet because the network packets are likely encrypted with TLS encryption,[153] which would require more advanced security monitoring techniques beyond the scope of our basic testing environment. However, Security Onion is extremely flexible and allows for more advanced monitoring techniques such as the use of a separate "forward node" and installation of third-party software proxies that can be used to decrypt TLS-encrypted data sent and received from the mobile application and the internet.[154]

A user would need to introduce another Security Onion server as a forward node or stand-alone server that runs a proxy that could decrypt, inspect, and re-encrypt TLS traffic before forwarding it to the Security Onion "master server" and then the internet. Also, students could learn to relay mirrored network traffic to a network interface on a computer with Security Onion and use network analysis tools with the use of digital certificates to decrypt network traffic.[155]

As discussed, this is an advanced man-in-the-middle security analysis technique that is outside the scope of our basic information testing approach, but could provide more insight for advanced students about what data is actually being sent and received by the companion mobile application on a mobile device, but not from the streaming device because a trusted digital security certificate cannot be installed on the smart device itself.[156] As discussed, this advanced technique is considered out of scope for the basic information security testing because data from smart devices cannot be easily decrypted, and mobile applications that send and receive encrypted data often put in place advanced mechanisms to prevent the interception or decryption of encrypted data with pinned digital certificates on the smart device, or runtime malware detection code in the mobile application to prevent circumvention of encryption.

Therefore, the results presented in this paper on the privacy and security practices of the top five streaming devices and top 10 streaming apps did not attempt to decrypt any encrypted network traffic in order to examine the content of what data was actually sent and received by the streaming devices or companion mobile application. This research only examined the source and destination of where data was sent and received. We encourage additional research and experimentation based on these results, including analyzing content transmitted or received as well as identifying if additional third parties are implicated.

What should parents and educators do?

Parents and educators have several options when deciding whether to use streaming media apps and devices. Some may be thinking about which streaming app they should subscribe to, or which streaming device to purchase, and others may have already made up their mind to subscribe to one or more services, but aren't sure which one is best for privacy. Some may want to know how to change their app's privacy settings to best protect their children or students. Parents and educators may also want to know how to exercise their data rights and tell companies not to sell their data.

Below are some suggestions for managing this process to better protect child and student users:

- **Check the privacy settings**. All streaming apps have some settings inside that allow varying degrees of data collection features to be turned on or off. If it's not necessary to collect viewing data or analytics data on how the app is used, then these extra features can be turned off to minimize the amount of sensitive information collected.
- **Check Common Sense Media**. Streaming content may not be age appropriate, but our media reviews can help take away the guesswork.[157]
- **Encourage supervision**. Children and students should use streaming apps only when an adult

[153] Transport Layer Security ("TLS") is a cryptographic protocol designed to provide communications security over a computer network.

[154] *See* Security Onion Documentation, supra note 65.

[155] Digital certificates are an electronic document used to prove the ownership of a public key.

[156] A public key certificate, also known as a digital security certificate is an electronic file used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner, and the digital signature of an entity that has verified the certificate's contents.

[157] Common Sense Media, https://www.commonsensemedia.org.

is present to supervise use and limit use of streaming apps based on age-appropriate screen-time recommendations.

- **Check which apps or subscriptions are installed**. Remove unwanted third-party streaming apps or TV subscriptions to limit information collection.
- **Ask companies not to sell your data**. Use free online resources, like donotsell.org,[158] to request that companies not sell your personal data for profit.
- **Make your preferences known to companies and legislators**. Many parents have taken (or wanted to take) steps to limit data collection—recent research indicates about half of those surveyed think they have, and half want to but don't know how.[159] This is the jumping-off point for action. The next step is to empower parents and educators so that they know how to exercise their privacy protecting options. Legislators can support this practice by mandating features allowing parental controls, and when that doesn't fully protect kids, allowing the information to be deleted from devices and databases.
- **Make informed decisions about which apps to use**. This report is a snapshot of streaming apps and devices right now. Business practices change rapidly as companies think creatively about how to gather, process, and sell data. In deciding whether to purchase subscriptions or use streaming apps, consider the impact on children that use the service and the amount of screen time. Factor into your decision the cost of the service, purchases that may be made with the app, and the potential use of your personal information by the company and other third-party companies the app might share your data with over time.

What should streaming apps and devices do?

There are several industry best privacy practices that streaming app and device companies can adopt to differentiate themselves from their competitors and earn their consumers' trust as a product that respects their privacy and the privacy of their children.

[158] CCPA: Do Not Sell My Information, http://donotsell.org.

[159] Common Sense, Privacy user research, studies to understand parents' privacy-related knowledge and concerns (2019).

The following privacy practices are used in our evaluation process to determine whether a product receives a "Pass" or "Warning" rating for unclear or worse practices. These practices are also the most important factors for consumers, parents, and educators when choosing a better privacy-protecting product for themselves or their children or students.

A company should disclose in their privacy policy all of the following best practices:

- **No selling data**. A user's personal information should not be sold or rented to third parties. If a user's personal information is sold to third parties, then there is an increased risk that the personal information could be used in ways that were not intended at the time at which the user provided their personal information to the company, resulting in unintended harm. Two-thirds of the streaming apps and devices we tested disclosed in their privacy policies that they sell users' data. Only Apple, Google, Amazon, Netflix, and Nvidia disclosed they do not sell their user's data for profit to third parties.
- **No third-party marketing communications**. A user's personal information should not be shared with third parties for marketing purposes. A streaming app or device that requires a user to be contacted by third-party companies for their own revenue generating purposes increases the risk of exposure to inappropriate messages and influences that may exploit a user's preferences and vulnerabilities. Third parties who try to influence a user's purchasing behavior for other goods and services may cause unintended harm. Only Apple and Google disclosed they do not send users third-party marketing communications by default.
- **No displaying targeted advertising**. Targeting users with personalized advertising on the streaming service based on their personal information or viewing habits should not be displayed in the product or elsewhere on the internet. A user's personal information provided to a streaming app or device should not be used to exploit that user's specific knowledge, traits, and viewing behaviors to influence their desire to purchase goods and services. Only Apple disclosed they do not display targeted advertisements on their service to all users. However, Google, HBO, and Amazon disclosed in their additional child privacy policies that they do not display targeted advertisements to children.

- **No third-party tracking**. A streaming app or device should not permit third-party advertising services or tracking technologies to collect any information from a user while using the service. A user's personal and viewing information provided to a streaming app or device should not be also used by a third party to persistently track that user's behavioral actions on the app or device to influence what content they see in the product and elsewhere online. Third-party tracking can influence a user's decision-making processes without their knowledge, which may cause unintended harm. Only Apple disclosed they do not engage in third-party tracking of all users.
- **No tracking across apps**. A user's personal information should not be tracked and used to target them with advertisements on other third-party websites or services. A user's personal information provided to a streaming app or device should not be used by a third party to persistently track that user's behavioral actions over time and across the internet on other apps and services. Only Apple disclosed they do not engage in tracking any user over time across other third-party apps and services.
- **No data profiling**. A company should not allow third parties to use a user's data to create a profile, engage in data enhancement or social advertising, or target advertising based on that profile. Automated decision-making, including the creation of data profiles for tracking or advertising purposes, can lead to an increased risk of harmful outcomes that may disproportionately and significantly affect children or students. Only Apple disclosed they do not engage in profiling all users for the purpose of advertising or tracking users over time.
- **Protect use by students in K–12**. Streaming apps and devices should provide more information about how they protect student data privacy when used in K–12 schools and districts. Streaming companies that don't talk about how they protect student data privacy and also have content directed to children, or would appeal to children, need to clarify and discuss how they protect children and students.

Children and data privacy

When it comes to their children and students, parents and educators value the ability to understand and control what personal information is collected from apps they use. And if so, does the user know how to control what information is collected and whether their child's or students' personal data is being used to deliver personalized or targeted ads? Streaming apps and devices can request access to a user's mobile device location, play age-appropriate or age-inappropriate media, and subscribe to different third-party app content providers through channels. Parents and educators may also feel like they don't have the ability to make a meaningful choice when it comes to privacy because the TV shows, movies, or educational content they need is only available on a single streaming platform.

- **The facts**: Streaming apps and devices may be treated as trusted services, but they can collect a significant amount of behavioral viewing data and personal information to influence your behavior to get you to watch one more episode and consume more content.
- **The feelings**: Parents and educators may have feelings about streaming apps and devices always collecting data from their children and students while they are watching to create a personalized profile—basically noting every show that has been watched or not watched. This is often referred to as the "creepiness" factor and could include collecting behavioral data without express permission, or using the data for purposes other than what the app was initially used for. For example, a person might watch a show on a streaming service and get an email or advertisement elsewhere selling them merchandise related to the show.
- **The future**: Beyond what is currently collected and how it is used, streaming apps may store behavioral data indefinitely. At some point, companies may use the data in ways that no one has yet imagined, such as changing default interactions on other unrelated apps and services based on what types of content that was already watched. In addition, data brokers could also combine behavioral data in the future with data collected from other apps and services in order to reidentify presumed anonymous or deidentified data. In order to better protect children, the streaming media industry needs to develop alternative monetization methodologies for distributing content in a more privacy-protecting manner; additionally streaming app developers should incorporate privacy-by-design principles.

APPENDIX

Traffic analysis methodology

During the operation of each device or app, traffic was captured and later analyzed. Due to the majority of, but not all, traffic being transmitted over secure communication channels we only have aggregate domain level information and therefore do not have insight into particular resources accessed. Each application's traffic was only observed using the lowest price point there may be observable differences in traffic based on pay plan that we did not make an effort to observe. As such, any of the following analysis should be interpreted with some caution.

Our analysis is intended to indicate the possibility that the respective tracking behavior could be happening based on the device or app accessing resources on a particular domain known to have exhibited tracking behavior. For all domains captured, we first made a best effort to determine if the traffic was presumably from the first party or third party. We then ran two sets of analysis to categorize the potential for tracking related behavior based on the domains contacted for each app or device. If a domain is indicated as potentially engaging in a tracking behavior, it should be interpreted to mean that caution is warranted with respect to tracking concerns. In addition, the observed traffic does not necessarily mean that the respective tracking behavior was necessarily engaged in.

For each domain we observed, we also indicate the "Matching Domain" indicating which Tracker Radar domain file was used to provide the tracking categories. We only considered domains in the U.S. directory for Tracker Radar. If a domain indicates "NA" that means we did not have a corresponding Tracker Radar domain file to classify the domain traffic. Some of these unknown domains are expected as the process to obtain the Tracker Radar data is from a web browser—a context notably different than the apps or devices that we tested. As such, there may not have been opportunities to observe traffic as seen when using an app or device as opposed to a web browser.

We used a git checkout of the tracker-radar project with git tag `2021.03' corresponding to a git hash 3580393035dd1d7e8daf6172b63afbaceeec9036.

Tracking categories

For the purposes of our analysis we only considered Tracker Radar categories[160] that could pose a privacy risk, especially because it is unlikely that a user of a streaming app or device would know any tracking was happening. As such, we have excluded the "Social–Comment" and "Social–Share" Tracker Radar categories in our analysis as it is likely the user would see the respective interfaces or social share buttons making it more explicit that data is being shared or transmitted that could be used to track behavior. It should also be noted that we considered "Obscure Ownership," "Session Replay," and "Unknown High Risk Behavior" but at least for the traffic that we were able to observe no streaming devices or apps contacted domains triggering any of those Tracker Radar categories. Several other innocuous categories were also excluded. The categories we included in our analysis are as follows:

- Action Pixels (**AP**): This tracker may be collecting user specific events in a first-party or third-party environment.
- Ad Fraud (**AF**): The tracker is intended to help prevent ad fraud (either on behalf of the publisher or the network). These can come from a network (like Google) or ad middleware (software designed to identify bots and not show them ads).
- Ad Motivated Tracking (**AMT**): The tracking that takes place is related to advertising. This could include targeting users, header bidding, ad beacons, demographic collection, preventing ad fraud, etc.
- Advertising (**AD**): The purpose of this tracker is related to advertising.
- Audience Measurement (**AM**): Similar to analytics, but may focus on deeper demographics, behavior sets, and specific actions.
- Social Network (**SN**): The domain is owned by a major social network.
- Third-Party Analytics Marketing (**TPAM**): Related to third-party analytics systems for marketing, usually marketing attribution or funnel management.

[160] DuckDuckGo Tracker Radar, Categories, https://github.com/duckduckgo/tracker-radar/blob/main/docs/CATEGORIES.md.

App traffic analysis

Amazon Prime

Table 24: Amazon Prime presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
s3-iad-ww.cf.videorolls.row.aiv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
api.us-east-1.aiv-delivery.net	NA	NA	NA	NA	NA	NA	NA	NA
cf-timedtext.aux.pv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
doh6p23r7m48u.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
dp-gw-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
msh.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
atv-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
device-metrics-us-2.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
images-na.ssl-images-amazon.com	ssl-images-amazon.com	No	No	No	No	No	No	No
m.media-amazon.com	media-amazon.com	No	No	No	No	No	No	No
s3-iad-2.cf.dash.row.aiv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
pop-iad-2.cf.dash.row.aiv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
dmqdd6hw24ucf.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
cf-trickplay.aux.pv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
ecx.images-amazon.com	images-amazon.com	No	No	No	No	No	No	No
Total:	0	0	0	4	0	0	0	4

Table 25: Amazon Prime presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
homecloudcastsdk-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
www.hulu.com	hulu.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Apple TV+

Table 26: Apple TV+ presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
p69-fmfmobile.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
is1-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is3-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is5-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No

is2-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
s.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
uts-api.itunes.apple.com	apple.com	No	No	No	No	No	No	No
play-edge.itunes.apple.com	apple.com	No	No	No	No	No	No	No
play.itunes.apple.com	apple.com	No	No	No	No	No	No	No
vod-ap3-aoc.tv.apple.com	apple.com	No	No	No	No	No	No	No
cma2.itunes.apple.com	apple.com	No	No	No	No	No	No	No
xp.apple.com	apple.com	No	No	No	No	No	No	No
np-edge.itunes.apple.com	apple.com	No	No	No	No	No	No	No
init.itunes.apple.com	apple.com	No	No	No	No	No	No	No
pd.itunes.apple.com	apple.com	No	No	No	No	No	No	No
iphone-ld.apple.com	apple.com	No	No	No	No	No	No	No
daf.xp.apple.com	apple.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

We did not observe any presumed third-party traffic for Apple TV+.

Discovery+

Table 27: Discovery+ presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
us1-prod-images.disco-api.com	disco-api.com	No	No	No	No	No	No	No
avatars-prod.disco-api.com	disco-api.com	No	No	No	No	No	No	No
us1-prod.disco-api.com	disco-api.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 28: Discovery+ presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
firebase-settings.crashlytics.com	NA	NA	NA	NA	NA	NA	NA	NA
passwordsleakcheck-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
api.getblueshift.com	getblueshift.com	No	No	No	No	No	No	No
4unal8ngvngjm07lj2q2umlc4.litix.io	litix.io	No	No	No	No	No	No	No
api.arkoselabs.com	arkoselabs.com	No	No	No	No	No	No	No
content-ause2-ur-discovery1.uplynk.com	uplynk.com	No	No	No	No	No	No	No

client-api.arkoselabs.com	arkoselabs.com	No	No	No	No	No	No	No
x-default-stgec.uplynk.com	uplynk.com	No	No	No	No	No	No	No
2ecd5.v.fwmrm.net	fwmrm.net	No	No	Yes	Yes	No	No	Yes
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
cdn.branch.io	branch.io	No	No	No	Yes	Yes	No	Yes
api2.branch.io	branch.io	No	No	No	Yes	Yes	No	Yes
mobile-collector.newrelic.com	newrelic.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
bsftassets.s3-us-west-2.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
Total:	0	0	0	1	3	2	0	3

Disney+

Table 29: Disney+ presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
vod-cmc-na-west-2.media.dssott.com	NA	NA	NA	NA	NA	NA	NA	NA
search-api-disney.svcs.dssott.com	NA	NA	NA	NA	NA	NA	NA	NA
global.edge.bamgrid.com	NA	NA	NA	NA	NA	NA	NA	NA
sanalytics.disneyplus.com	NA	NA	NA	NA	NA	NA	NA	NA
vod-ftc-na-west-2.media.dssott.com	NA	NA	NA	NA	NA	NA	NA	NA
appconfigs.disney-plus.net	NA	NA	NA	NA	NA	NA	NA	NA
bam-sdk-configs.bamgrid.com	NA	NA	NA	NA	NA	NA	NA	NA
content.global.edge.bamgrid.com	NA	NA	NA	NA	NA	NA	NA	NA
disney.playback.edge.bamgrid.com	NA	NA	NA	NA	NA	NA	NA	NA
vod-akc-na-west-2.media.dssott.com	NA	NA	NA	NA	NA	NA	NA	NA
Total:	0	0	0	0	0	0	0	0

Table 30: Disney+ presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
growth-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
7ba3f64df98de730df38846b54ecfbdf7f61f80f.cws.conviva.com	conviva.com	No	No	No	No	No	No	No
sdk.iad-03.braze.com	braze.com	No	No	No	No	No	No	No

www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
disney.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
assets.adobedtm.com	adobedtm.com	No	No	Yes	No	Yes	No	Yes
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
mtalk.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
Total:	0	0	0	2	1	1	0	2

Hulu

Table 31: Hulu presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
ads-e-darwin.hulustream.com	NA	NA	NA	NA	NA	NA	NA	NA
manifest-dp.hulustream.com	NA	NA	NA	NA	NA	NA	NA	NA
discover.hulu.com	hulu.com	No	No	No	No	No	No	No
ib.hulu.com	hulu.com	No	No	No	No	No	No	No
img2.hulu.com	hulu.com	No	No	No	No	No	No	No
engage.hulu.com	hulu.com	No	No	No	No	No	No	No
img4.hulu.com	hulu.com	No	No	No	No	No	No	No
play.hulu.com	hulu.com	No	No	No	No	No	No	No
vortex.hulu.com	hulu.com	No	No	No	No	No	No	No
home.hulu.com	hulu.com	No	No	No	No	No	No	No
ariel.hulu.com	hulu.com	No	No	No	No	No	No	No
auth.hulu.com	hulu.com	No	No	No	No	No	No	No
emu.hulu.com	hulu.com	No	No	No	No	No	No	No
img1.hulu.com	hulu.com	No	No	No	No	No	No	No
img3.hulu.com	hulu.com	No	No	No	No	No	No	No
views.hulu.com	hulu.com	No	No	No	No	No	No	No
www.hulu.com	hulu.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 32: Hulu presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
firebase-settings.crashlytics.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
update.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA

launches.appsflyer.com	appsflyer.com	No	No	No	No	No	No	No
cws-hulu.conviva.com	conviva.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
firebaseremoteconfig.googleapis.com	firebaseremoteconfig.googleapis.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
collect.tealiumiq.com	tealiumiq.com	Yes	No	Yes	Yes	Yes	No	Yes
secure-dcr.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
cdn-gl.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
wqc89bfta2l4f0st2vn6tk00kx82b1617987040.uaid.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
z.moatads.com	moatads.com	Yes	Yes	Yes	Yes	Yes	No	Yes
assetshuluimcom-a.akamaihd.net	akamaihd.net	No	No	No	No	No	No	No
accounts.youtube.com	youtube.com	No	No	Yes	No	No	No	No
tags.tiqcdn.com	tiqcdn.com	No	No	Yes	Yes	Yes	No	Yes
accounts.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
clients4.google.com	google.com	No	No	No	No	No	No	No
accounts.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
Total:	0	5	1	8	7	6	0	6

Netflix

Table 33: Netflix presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
ipv4-c067-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
android-h2.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c051-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c069-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
android-appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
android.prod.cloud.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
Total:	0	0	0	0	0	0	0	0

Table 34: Netflix presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
homecloudcastsdk-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
sessions.bugsnag.com	bugsnag.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Paramount+

Table 35: Paramount+ presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
wwwimage-us.pplusstatic.com	NA	NA	NA	NA	NA	NA	NA	NA
thumbnails.cbsig.net	NA	NA	NA	NA	NA	NA	NA	NA
www.paramountplus.com	NA	NA	NA	NA	NA	NA	NA	NA
sparrow.paramountplus.com	NA	NA	NA	NA	NA	NA	NA	NA
saa.cbsi.com	cbsi.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 36: Paramount+ presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
cbsi.live.ott.irdeto.com	NA	NA	NA	NA	NA	NA	NA	NA
chromesyncpasswords-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
geller-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
passwordsleakcheck-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
safebrowsing.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
update.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
i-amlg-prod.appspot.com	i-amlg-prod.appspot.com	No	No	No	No	No	No	No
control.kochava.com	kochava.com	No	No	No	No	No	No	No
87a6b28bc7823e67a5bb2a0a6728c702afcae78d.cws.conviva.com	conviva.com	No	No	No	No	No	No	No
kvinit-prod.api.kochava.com	kochava.com	No	No	No	No	No	No	No
ceres.iad-03.braze.com	braze.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
r1---sn-qxoedn7k.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No

r2---sn-q4flrn7r.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r2---sn-q4fl6nsy.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
link.theplatform.com	theplatform.com	No	No	No	No	No	No	No
api2.branch.io	branch.io	No	No	No	Yes	Yes	No	Yes
cdn.branch.io	branch.io	No	No	No	Yes	Yes	No	Yes
imasdk.googleapis.com	imasdk.googleapis.com	No	No	No	No	No	No	No
mobile-collector.newrelic.com	newrelic.com	No	No	No	No	No	No	No
tv.rlcdn.com	rlcdn.com	No	Yes	Yes	Yes	No	No	Yes
sb.scorecardresearch.com	scorecardresearch.com	No	No	No	No	Yes	No	No
qixhcdih3kiwsarl8bp20oo4hqhz5161 8437043.uaid.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
secure-dcr.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
sdk.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
secure-gg.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
yw14dzy9uqrrixbmofkza1awgmbm91 618437501.uaid.imrworldwide.com	imrworldwide.com	Yes	No	Yes	Yes	Yes	No	Yes
dpm.demdex.net	demdex.net	No	No	Yes	Yes	No	No	Yes
storage.googleapis.com	storage.googleapis.com	No	No	No	No	No	No	No
cbsinteractive.hb.omtrdc.net	omtrdc.net	No	No	Yes	Yes	Yes	No	Yes
accounts.youtube.com	youtube.com	No	No	Yes	No	No	No	No
www.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.google-analytics.com	google-analytics.com	No	No	No	Yes	Yes	No	Yes
pagead2.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
pubads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
ad.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
accounts.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
clients4.google.com	google.com	No	No	No	No	No	No	No
accounts.google.com	google.com	No	No	No	No	No	No	No
dai.google.com	google.com	No	No	No	No	No	No	No
mtalk.google.com	google.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
redirector.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r1---sn-qxo7rn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-qxoedn7d.gvt1.com	gvt1.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
Total:	0	6	2	14	16	11	1	11

HBO Max

Table 37: HBO Max presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
artist.api.cdn.hbo.com	hbo.com	No	No	No	No	No	No	No
gateway.api.hbo.com	hbo.com	No	No	No	No	No	No	No
comet.api.hbo.com	hbo.com	No	No	No	No	No	No	No
oauth-us.api.hbo.com	hbo.com	No	No	No	No	No	No	No
oauth.api.hbo.com	hbo.com	No	No	No	No	No	No	No
telegraph.api.hbo.com	hbo.com	No	No	No	No	No	No	No
sessions-us.api.hbo.com	hbo.com	No	No	No	No	No	No	No
sessions.api.hbo.com	hbo.com	No	No	No	No	No	No	No
cmaf.cf.us.hbomaxcdn.com	NA	NA	NA	NA	NA	NA	NA	NA
Total:	0	0	0	0	0	0	0	0

Table 38: HBO Max presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
hercules.iad.appboy.com	appboy.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
storage.googleapis.com	storage.googleapis.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Peacock

Table 39: Peacock presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
ovp.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
imageservice.disco.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
atom.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
g005-sf-us-cmaf-prd-ak.cdn.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
atlantis.disco.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
ctl.stream.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
g002-vod-us-cmaf-prd-ak-a331.cdn.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
g005-sf-us-cmaf-prd-ak-a196.cdn.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA

g005-sf-us-cmaf-prd-ak-a247.cdn.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
init.clients.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
rango.id.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
config.clients.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
cybertron.id.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
g002-vod-us-cmaf-prd-ak.cdn.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
mobile.clients.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
persona.id.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
recs.disco.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
throttled.ovp.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
www.peacocktv.com	NA	NA	NA	NA	NA	NA	NA	NA
video-ads-module.ad-tech.nbcuni.com	nbcuni.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 40: Peacock presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playatoms-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
chromesyncpasswords-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
android-appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
android-h2.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
android.prod.cloud.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
beacons.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
firebase-settings.crashlytics.com	NA	NA	NA	NA	NA	NA	NA	NA
growth-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
notifications-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
passwordsleakcheck-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
secure.insightexpressai.com	insightexpressai.com	No	No	Yes	Yes	Yes	No	No
47e224be59415ec068b94bca857581bd7dde7fb6.cws.conviva.com	conviva.com	No	No	No	No	No	No	No
control.kochava.com	kochava.com	No	No	No	No	No	No	No
kvinit-prod.api.kochava.com	kochava.com	No	No	No	No	No	No	No

sdk.iad-03.braze.com	braze.com	No	No	No	No	No	No	No
29773.v.fwmrm.net	fwmrm.net	No	No	Yes	Yes	No	No	Yes
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
mssl.fwmrm.net	fwmrm.net	No	No	Yes	Yes	No	No	Yes
mobile-collector.newrelic.com	newrelic.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
natives dks.mparticle.com	mparticle.com	No	No	No	No	No	No	No
identity.mparticle.com	mparticle.com	No	No	No	No	No	No	No
config2.mparticle.com	mparticle.com	No	No	No	No	No	No	No
sb.scorecardresearch.com	scorecardresearch.com	No	No	No	No	Yes	No	No
nbcstreaming.hb.omtrdc.net	omtrdc.net	No	No	Yes	Yes	Yes	No	Yes
assets.adobedtm.com	adobedtm.com	No	No	Yes	No	Yes	No	Yes
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
Total:	0	0	0	6	5	4	0	4

YouTube TV

Table 41: YouTube TV presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
r2---sn-qxoedne7.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r1---sn-qxoedne7.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r3---sn-qxoedn7k.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r4---sn-qxoedn7z.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r1---sn-qxo7rn7l.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r5---sn-qxoedne7.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r4---sn-qxoedne7.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r4---sn-qxoedn7k.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r2---sn-qxoedn7z.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r5---sn-qxoedn7d.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r6---sn-qxoedn7z.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
redirector.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r2---sn-qxo7rn7l.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r2---sn-qxoedn7e.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No

r5---sn-qxo7rn7l.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r5---sn-qxoedn7k.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r6---sn-qxoedn7e.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r4---sn-qxoedn7e.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r6---sn-qxoedn7d.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
manifest.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r5---sn-qxoedn7e.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
yt3.ggpht.com	ggpht.com	No	No	No	No	No	No	No
www.googleadservices.com	googleadservices.com	No	No	Yes	Yes	No	No	No
www.googletagmanager.com	googletagmanager.com	No	No	Yes	Yes	Yes	No	Yes
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
Total:	0	0	0	2	2	1	0	1

Table 42: YouTube TV presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
mobile-collector.newrelic.com	newrelic.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Device traffic analysis

Amazon Fire TV Cube

Table 43: Amazon Fire TV Cube presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
andr-59e19706d5-cbc62794911ff31b-e1b148d80a9aa0d4ca-2610165.na.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
d1s31zyz7dcc2d.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
api.us-east-1.aiv-delivery.net	NA	NA	NA	NA	NA	NA	NA	NA
andr-28-aftr-620019910.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
d14j89z87mkhwa.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
d21m0ezw6fosyw.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
aftv-28-amazon-aftr-3242.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
aftv-28-amazon-aftr-3242.na.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA

andr-28-aftr-0.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
andr-59e19706d5-cbc62794911ff31b-e1b148d80a9aa0d4ca-2610165.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
d3a510xmpll7o6.cloudfront.net	NA	NA	NA	NA	NA	NA	NA	NA
ters.us-east-1.aiv-delivery.net	NA	NA	NA	NA	NA	NA	NA	NA
wl.amazon-dss.com	NA	NA	NA	NA	NA	NA	NA	NA
mobileanalytics.us-east-1.amazonaws.com	mobileanalytics.us-east-1.amazonaws.com	No	No	No	No	No	No	No
cognito-identity.us-east-1.amazonaws.com	cognito-identity.us-east-1.amazonaws.com	No	No	No	No	No	No	No
prod-iad.notification.mayday-screen-sharing.cs.a2z.com	a2z.com	No	No	No	No	No	No	No
kinesis.us-east-1.amazonaws.com	kinesis.us-east-1.amazonaws.com	No	No	No	No	No	No	No
ktpx.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
msh.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
mas-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
unagi-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
api.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
device-metrics-us.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
arcus-uswest.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
atv-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
dp-gw-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
aviary.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
fls-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
dp-discovery-na-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
idc-service-oz.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
aca-livecards-service.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
cortana-gateway.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
ags-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
appstore-tv-prod-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
dcape-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
devicemessaging.us-east-1.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
dna.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
prime.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
alexa.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
firs-ta-g7g.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
device-messaging-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
det-ta-g7g.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
dps-proxy.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes

ftvr-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
cs-ext.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
digprjsurvey.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
firetvdeviceprofilemanagementservice-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
mads.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
mas-sdk.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
na.account.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
paifas.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
remoteconfig-na.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
todo-ta-g7g.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
softwareupdates.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
www.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
images-na.ssl-images-amazon.com	ssl-images-amazon.com	No	No	No	No	No	No	No
i8xcss1sc8.execute-api.us-west-2.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
cdws.us-east-1.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
drive.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
device-artifacts-v2.s3.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
kraken-measurements.s3-external-1.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
m.media-amazon.com	media-amazon.com	No	No	No	No	No	No	No
content-na.drive.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
screensaver-sponsored-content-assets.s3.us-east-2.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
pinpoint.us-east-1.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
s3-iad-2.cf.dash.row.aiv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
pop-iad-2.cf.dash.row.aiv-cdn.net	NA	NA	NA	NA	NA	NA	NA	NA
fireoscaptiveportal.com	NA	NA	NA	NA	NA	NA	NA	NA
ecx.images-amazon.com	images-amazon.com	No	No	No	No	No	No	No
g-ecx.images-amazon.com	images-amazon.com	No	No	No	No	No	No	No
spectrum.s3.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
aax-us-east.amazon-adsystem.com	amazon-adsystem.com	No	No	Yes	Yes	No	No	No
Total:	0	0	0	39	1	0	0	38

Table 44: Amazon Fire TV Cube presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
subtitles.cdn-ec.viddler.com	NA	NA	NA	NA	NA	NA	NA	NA
ichnaea.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
api-global.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
nrdp.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c021-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c043-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c069-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c037-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-590-586.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
h1-scm.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
h2-scm.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
preapp.prod.partner.netflix.net	NA	NA	NA	NA	NA	NA	NA	NA
thumbs.cdn-ec.viddler.com	NA	NA	NA	NA	NA	NA	NA	NA
secure.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c012-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
push.prod.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
uiboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
www.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.nflxext.com	nflxext.com	No	No	No	No	No	No	No
codex.nflxext.com	nflxext.com	No	No	No	No	No	No	No
sessions.bugsnag.com	bugsnag.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
amazonadsi-a.akamaihd.net	akamaihd.net	No	No	No	No	No	No	No
a261avoddashs3ww-a.akamaihd.net	akamaihd.net	No	No	No	No	No	No	No
avodmp4s3ww-a.akamaihd.net	akamaihd.net	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Apple TV

Table 45: Apple TV presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
setup.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
p69-escrowproxy.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
edge-039.usden.icloud-content.com	NA	NA	NA	NA	NA	NA	NA	NA
metrics.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
keyvalueservice.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
p69-availability.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
p69-fmipmobile.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
p69-keyvalueservice.icloud.com	NA	NA	NA	NA	NA	NA	NA	NA
is3-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is2-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is1-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is4-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
s.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
is5-ssl.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
apps.mzstatic.com	mzstatic.com	No	No	No	No	No	No	No
gspe21-ssl.ls.apple.com	apple.com	No	No	No	No	No	No	No
uts-api.itunes.apple.com	apple.com	No	No	No	No	No	No	No
init.itunes.apple.com	apple.com	No	No	No	No	No	No	No
xp.apple.com	apple.com	No	No	No	No	No	No	No
bag.itunes.apple.com	apple.com	No	No	No	No	No	No	No
itunes.apple.com	apple.com	No	No	No	No	No	No	No
p3-buy.itunes.apple.com	apple.com	No	No	No	No	No	No	No
gsa.apple.com	apple.com	No	No	No	No	No	No	No
mesu.apple.com	apple.com	No	No	No	No	No	No	No
play.itunes.apple.com	apple.com	No	No	No	No	No	No	No
vod-ak-aoc.tv.apple.com	apple.com	No	No	No	No	No	No	No
identity.ess.apple.com	apple.com	No	No	No	No	No	No	No
api-edge.apps.apple.com	apple.com	No	No	No	No	No	No	No
buy.itunes.apple.com	apple.com	No	No	No	No	No	No	No
play-edge.itunes.apple.com	apple.com	No	No	No	No	No	No	No
hls.itunes.apple.com	apple.com	No	No	No	No	No	No	No
gdmf.apple.com	apple.com	No	No	No	No	No	No	No
guzzoni.apple.com	apple.com	No	No	No	No	No	No	No
pancake.apple.com	apple.com	No	No	No	No	No	No	No
profile.ess.apple.com	apple.com	No	No	No	No	No	No	No
vod-ap2-aoc.tv.apple.com	apple.com	No	No	No	No	No	No	No

amp-api.apps.apple.com	apple.com	No	No	No	No	No	No	No
aidc.apple.com	apple.com	No	No	No	No	No	No	No
cl3.apple.com	apple.com	No	No	No	No	No	No	No
sylvan.apple.com	apple.com	No	No	No	No	No	No	No
configuration.apple.com	apple.com	No	No	No	No	No	No	No
client-api.itunes.apple.com	apple.com	No	No	No	No	No	No	No
ld-4.itunes.apple.com	apple.com	No	No	No	No	No	No	No
pd.itunes.apple.com	apple.com	No	No	No	No	No	No	No
albert.apple.com	apple.com	No	No	No	No	No	No	No
vod-ap1-aoc.tv.apple.com	apple.com	No	No	No	No	No	No	No
api.apps.apple.com	apple.com	No	No	No	No	No	No	No
gsas.apple.com	apple.com	No	No	No	No	No	No	No
cma2.itunes.apple.com	apple.com	No	No	No	No	No	No	No
gspe35-ssl.ls.apple.com	apple.com	No	No	No	No	No	No	No
configuration.ls.apple.com	apple.com	No	No	No	No	No	No	No
daf.xp.apple.com	apple.com	No	No	No	No	No	No	No
gspe1-ssl.ls.apple.com	apple.com	No	No	No	No	No	No	No
np-edge.itunes.apple.com	apple.com	No	No	No	No	No	No	No
upp.itunes.apple.com	apple.com	No	No	No	No	No	No	No
valid.apple.com	apple.com	No	No	No	No	No	No	No
sf-api-token-service.itunes.apple.com	apple.com	No	No	No	No	No	No	No
cl2.apple.com	apple.com	No	No	No	No	No	No	No
cma.itunes.apple.com	apple.com	No	No	No	No	No	No	No
courier.push.apple.com	apple.com	No	No	No	No	No	No	No
bookkeeper.itunes.apple.com	apple.com	No	No	No	No	No	No	No
gs-loc.apple.com	apple.com	No	No	No	No	No	No	No
homesharing.itunes.apple.com	apple.com	No	No	No	No	No	No	No
init.push.apple.com	apple.com	No	No	No	No	No	No	No
gsp64-ssl.ls.apple.com	apple.com	No	No	No	No	No	No	No
humb.apple.com	apple.com	No	No	No	No	No	No	No
iphonesubmissions.apple.com	apple.com	No	No	No	No	No	No	No
init.gc.apple.com	apple.com	No	No	No	No	No	No	No
iosapps.itunes.apple.com	apple.com	No	No	No	No	No	No	No
radio.itunes.apple.com	apple.com	No	No	No	No	No	No	No
profile.gc.apple.com	apple.com	No	No	No	No	No	No	No
sp.itunes.apple.com	apple.com	No	No	No	No	No	No	No
static.gc.apple.com	apple.com	No	No	No	No	No	No	No
sandbox.itunes.apple.com	apple.com	No	No	No	No	No	No	No
lcdn-locator.apple.com	apple.com	No	No	No	No	No	No	No
updates-http.cdn-apple.com	cdn-apple.com	No	No	No	No	No	No	No

ocsp.apple.com	apple.com	No	No	No	No	No	No	No
captive.apple.com	apple.com	No	No	No	No	No	No	No
init-p01md.apple.com	apple.com	No	No	No	No	No	No	No
static.ess.apple.com	apple.com	No	No	No	No	No	No	No
init.ess.apple.com	apple.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 46: Apple TV presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
ipv4-c011-den001-dev-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c073-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ios.prod.http1.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c049-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c074-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c072-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
ichnaea-web.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
www.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.nflxext.com	nflxext.com	No	No	No	No	No	No	No
webvtt-s.nflxext.com	nflxext.com	No	No	No	No	No	No	No
appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ocsp.digicert.com	digicert.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Google TV

Table 47: Google TV presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
android.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
embeddedassistant.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
zerostateproxy-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
fcm.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playatoms-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
androidtvlauncherxfe-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA

androidtvsetupwraithfe-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
auditrecording-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playmoviesdfe-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
footprints-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
androidtvcustomization-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
chromesyncpasswords-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
powerful-gizmo-526.appspot.com	NA	NA	NA	NA	NA	NA	NA	NA
androidtvchannels-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
app.goo.gl	NA	NA	NA	NA	NA	NA	NA	NA
beacons.gcp.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
clientservices.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
device-provisioning.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
fir-auth-gms.firebaseapp.com	NA	NA	NA	NA	NA	NA	NA	NA
firebaseperusertopics-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
g.co	NA	NA	NA	NA	NA	NA	NA	NA
geomobileservices-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
googlehomefoyer-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
homecloudirdb-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
iid.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
mdh-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
near.by	NA	NA	NA	NA	NA	NA	NA	NA
notifications-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
pai.googlezip.net	NA	NA	NA	NA	NA	NA	NA	NA
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
redirector.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
r5---sn-q4flrnes.googlevideo.com	googlevideo.com	No	No	No	No	No	No	No
imasdk.googleapis.com	imasdk.googleapis.com	No	No	No	No	No	No	No
r2---sn-q4fl6ney.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4flrn7y.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r1---sn-q4flrnee.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4fl6n7d.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4fl6nle.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4fl6nlr.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4flrnle.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r3---sn-q4f7sn7l.gvt1.com	gvt1.com	No	No	No	No	No	No	No

r3---sn-q4fl6nly.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4flrnez.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r3---sn-q4fl6ns7.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r3---sn-q4fl6nlr.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r3---sn-qxoedn7e.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r4---sn-q4fl6ne7.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r4---sn-q4f7sn76.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r4---sn-q4fl6ner.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r4---sn-q4fl6nly.gvt1.com	gvt1.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
lh3.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
play-lh.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
ccp-lh.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
lh3-dz.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
fonts.googleapis.com	fonts.googleapis.com	No	No	No	No	No	No	No
encrypted-tbn2.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn3.gstatic.com	gstatic.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
fonts.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn0.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn1.gstatic.com	gstatic.com	No	No	No	No	No	No	No
pagead2.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
ade.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
clients5.google.com	google.com	No	No	No	No	No	No	No
android-safebrowsing.google.com	google.com	No	No	No	No	No	No	No
history.google.com	google.com	No	No	No	No	No	No	No
enterprise.google.com	google.com	No	No	No	No	No	No	No
clients4.google.com	google.com	No	No	No	No	No	No	No
dl.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
accounts.google.com	google.com	No	No	No	No	No	No	No
clients3.google.com	google.com	No	No	No	No	No	No	No
play.google.com	google.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
mtalk.google.com	google.com	No	No	No	No	No	No	No
alt2-mtalk.google.com	google.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No

connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
Total:	0	0	0	2	2	0	0	0

Table 48: Google TV presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
nrdp.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ichnaea.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
api-global.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c042-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c078-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
push.prod.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
secure.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
uiboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
app.primevideo.com	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-590-586.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
play.hbomax.com	NA	NA	NA	NA	NA	NA	NA	NA
play.hbonow.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.nflxext.com	nflxext.com	No	No	No	No	No	No	No
sessions.bugsnag.com	bugsnag.com	No	No	No	No	No	No	No
codex.nflxext.com	nflxext.com	No	No	No	No	No	No	No
hbomax.onelink.me	onelink.me	No	No	No	No	No	No	No
hbonow.onelink.me	onelink.me	No	No	No	No	No	No	No
nrdp52-appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
googleads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
pubads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
Total:	0	0	0	2	2	0	0	0

Nvidia Shield TV

Table 49: Nvidia Shield TV presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
img.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
prod.northstar.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
layouts.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
prod.cloudmatchbeta.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
gfnpc.api.entitlement-prod.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA

rconfig.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
services.tegrazone.com	NA	NA	NA	NA	NA	NA	NA	NA
static.nvidiagrid.net	NA	NA	NA	NA	NA	NA	NA	NA
ota.nvidia.com	nvidia.com	No	No	No	No	No	No	No
images.nvidia.com	nvidia.com	No	No	No	No	No	No	No
mobileupdate.nvidia.com	nvidia.com	No	No	No	No	No	No	No
ls.dtrace.nvidia.com	nvidia.com	No	No	No	No	No	No	No
ota-downloads.nvidia.com	nvidia.com	No	No	No	No	No	No	No
events.gfe.nvidia.com	nvidia.com	No	No	No	No	No	No	No
Total:	0	0	0	0	0	0	0	0

Table 50: Nvidia Shield TV presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
play.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
nrdp.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
api-global.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
ichnaea.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-590-586.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
secure.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
mclients.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
preapp.prod.partner.netflix.net	NA	NA	NA	NA	NA	NA	NA	NA
app-measurement.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c069-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
settings.crashlytics.com	NA	NA	NA	NA	NA	NA	NA	NA
uiboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
geomobileservices-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playatoms-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
plex.tv	NA	NA	NA	NA	NA	NA	NA	NA
androidtvchannels-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
antv-28-nvidia-shieldandroidtv-505003009.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
atv-a1kaxig6vxsg8y-nvidia-sif-shieldandroidtv-nvidiasifleasekeys.api.amazonvideo.com	NA	NA	NA	NA	NA	NA	NA	NA
chromesyncpasswords-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
footprints-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
apicache.vudu.com	NA	NA	NA	NA	NA	NA	NA	NA

app.primevideo.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.androidtv.com	NA	NA	NA	NA	NA	NA	NA	NA
auditrecording-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
beacons.gcp.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
beacons4.gvt2.com	NA	NA	NA	NA	NA	NA	NA	NA
clientservices.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c021-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
mdh-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
people-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
playmoviesdfe-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
powerful-gizmo-526.appspot.com	NA	NA	NA	NA	NA	NA	NA	NA
push.prod.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
voledevice-pa.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
www.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
youtubei.googleapis.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.nflxext.com	nflxext.com	No	No	No	No	No	No	No
codex.nflxext.com	nflxext.com	No	No	No	No	No	No	No
watch.amazon.co.jp	amazon.co.jp	No	No	No	No	No	No	No
watch.amazon.co.uk	amazon.co.uk	No	No	No	No	No	No	No
watch.amazon.de	amazon.de	No	No	No	No	No	No	No
sessions.bugsnag.com	bugsnag.com	No	No	No	No	No	No	No
www.googleapis.com	www.googleapis.com	No	No	No	No	No	No	No
device-metrics-us-2.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
watch.amazon.com	amazon.com	No	No	Yes	No	No	No	Yes
r2---sn-q4flrner.gvt1.com	gvt1.com	No	No	No	No	No	No	No
r2---sn-q4flrnes.gvt1.com	gvt1.com	No	No	No	No	No	No	No
firebaseinstallations.googleapis.com	firebaseinstallations.googleapis.com	No	No	No	No	No	No	No
2ctcysy2xi.execute-api.us-west-1.amazonaws.com	amazonaws.com	No	No	No	No	No	No	No
ajax.googleapis.com	ajax.googleapis.com	No	No	No	No	No	No	No
lh3.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
ccp-lh.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
play-lh.googleusercontent.com	googleusercontent.com	No	No	No	No	No	No	No
yt3.ggpht.com	ggpht.com	No	No	No	No	No	No	No
i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
fonts.googleapis.com	fonts.googleapis.com	No	No	No	No	No	No	No
nvidia.tt.omtrdc.net	omtrdc.net	No	No	Yes	Yes	Yes	No	Yes
mboxedge35.tt.omtrdc.net	omtrdc.net	No	No	Yes	Yes	Yes	No	Yes
graph.facebook.com	facebook.com	Yes	Yes	Yes	Yes	Yes	Yes	No

ssl.gstatic.com	gstatic.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn0.gstatic.com	gstatic.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
fonts.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn1.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn3.gstatic.com	gstatic.com	No	No	No	No	No	No	No
encrypted-tbn2.gstatic.com	gstatic.com	No	No	No	No	No	No	No
pagead2.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
alt5-mtalk.google.com	google.com	No	No	No	No	No	No	No
clients4.google.com	google.com	No	No	No	No	No	No	No
history.google.com	google.com	No	No	No	No	No	No	No
www.google.com	google.com	No	No	No	No	No	No	No
mtalk.google.com	google.com	No	No	No	No	No	No	No
clients3.google.com	google.com	No	No	No	No	No	No	No
accounts.google.com	google.com	No	No	No	No	No	No	No
play.google.com	google.com	No	No	No	No	No	No	No
policies.google.com	google.com	No	No	No	No	No	No	No
android-safebrowsing.google.com	google.com	No	No	No	No	No	No	No
alt2-mtalk.google.com	google.com	No	No	No	No	No	No	No
android.clients.google.com	google.com	No	No	No	No	No	No	No
images2.vudu.com	NA	NA	NA	NA	NA	NA	NA	NA
nrdp52-appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
i.ytimg.com	ytimg.com	No	No	No	No	No	No	No
www.gstatic.com	gstatic.com	No	No	No	No	No	No	No
connectivitycheck.gstatic.com	gstatic.com	No	No	No	No	No	No	No
Total:	0	1	1	6	4	3	1	4

Roku Smart Streaming Stick+

Table 51: Roku Smart Streaming Stick+ presumed first-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
scribe.logs.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
image.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
channels.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
display.ravm.tv	NA	NA	NA	NA	NA	NA	NA	NA
amarillo.sb.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
images.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
api.rokutime.com	NA	NA	NA	NA	NA	NA	NA	NA

cooper.logs.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
api.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
api2.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
tis.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
configsvc.cs.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
content.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
track.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
amoeba-plus.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
plugins.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
ravm.tv	NA	NA	NA	NA	NA	NA	NA	NA	NA
amarillo.sw.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
cloudservices.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
component-cdn.cs.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
ls.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
samples.voice.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
search.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
us.cts-delivery.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
vod.delivery.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
api.rpay.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
bookmarks.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
cts-delivery.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
customer-feedbacks.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
identity.ads.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
keysvc.cs.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
lat-services.api.data.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
lingua.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
navigation.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
optimus.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
p.ads.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
predictive-text.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
retail-prod.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
rights-manager.sr.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
roku-device-activate.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
tts.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
voice5.cti.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
wwwimg.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
cigars.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
channels.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
captive.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA
firmware.roku.com	NA	NA	NA	NA	NA	NA	NA	NA	NA

amoeba2.web.roku.com	NA	NA	NA	NA	NA	NA	NA	NA
Total:	0	0	0	0	0	0	0	0

Table 52: Roku Smart Streaming Stick+ presumed third-party domains contacted

Domain	Matching Domain	AP	AF	AMT	AD	AM	SN	TPAM
occ-0-586-590.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
nrdp.prod.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ichnaea.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
api-global.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
push.prod.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c037-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
ipv4-c072-den001-ix.1.oca.nflxvideo.net	NA	NA	NA	NA	NA	NA	NA	NA
secure.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
cfp4573tkkhwnes5xpcxs-usw2.r.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
oca-api.eu-west-1.origin.prodaa.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
oca-api.us-west-2.origin.prodaa.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
anycast.ftl.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
oca-api.us-east-1.origin.prodaa.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
uiboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
occ-0-590-586.1.nflxso.net	NA	NA	NA	NA	NA	NA	NA	NA
pr.service.expressplay.com	NA	NA	NA	NA	NA	NA	NA	NA
assets.nflxext.com	nflxext.com	No	No	No	No	No	No	No
codex.nflxext.com	nflxext.com	No	No	No	No	No	No	No
link.theplatform.com	theplatform.com	No	No	No	No	No	No	No
tpc.googlesyndication.com	googlesyndication.com	No	No	Yes	Yes	No	No	No
securepubads.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
adclick.g.doubleclick.net	doubleclick.net	No	No	Yes	Yes	No	No	No
index.ehub.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
nrdp50-appboot.netflix.com	NA	NA	NA	NA	NA	NA	NA	NA
Total:	0	0	0	3	3	0	0	0

"Do not sell" links

Apps

Two-thirds of the streaming apps and devices we tested disclosed in their privacy policies that they sell users' data to third parties. The following links provide users with the ability to provide opt out consent to the streaming services they use to stop them from selling their data to third-party companies.

- **Apple TV+**: The policies state they do not sell personal information.
- **YouTube TV**: The policies state they do not sell personal information.
- **Disney+**: https://privacyportal-de.onetrust.com/webform/64f077b5-2f93-429f-a005-c0206ec0738e/0a4f1f0b-7130-421f-971d-ef578c0bce6d
- **Paramount+**: https://www.viacomcbsprivacy.com/dns
- **HBO Max**: https://www.warnermediaprivacy.com/do-not-sell/request/
- **Peacock**: https://privacyportal.onetrust.com/webform/17e5cb00-ad90-47f5-a58d-77597d9d2c16/612ec9ee-1248-4528-965f-47143d2ec631
- **Amazon Prime Video**: The policies state they do not sell personal information.
- **Discovery+**: https://privacyportal-cdn.onetrust.com/dsarwebform/50417659-aa29-4f7f-b59d-f6e887deed53/59ad2e6e-03b5-44a2-8f89-b5aed0acc924.html
- **Hulu**: https://privacyportal-hulu-cdn.onetrust.com/dsarwebform/dbf35915-9140-401d-a543-cf08b05ae9f6/draft/0787e831-4706-4541-822e-cefa2e7ea2a7.html
- **Netflix**: The policies state they do not sell personal information.

Devices

- **Apple**: The policies state they do not sell personal information.
- **Google**: The policies state they do not sell personal information.
- **Amazon**: The policies state they do not sell personal information.
- **Roku**: https://privacy.roku.com/ccpa#!
- **Nvidia**: The policies state they do not sell personal information.

OUR OFFICES

San Francisco Headquarters
8th Street, Suite C150
San Francisco, CA 94103

New York Office
2160 Broadway, 4th Floor
New York, NY 10024

Washington, D.C. Office
2200 Pennsylvania Avenue NW, 4th Floor East
Washington, D.C. 20037

Los Angeles Office
1100 Glendon Avenue, 17th Floor
Los Angeles, CA 90024

Arizona Office
201 E. Camelback Road, Suite 403B,
Phoenix, AZ 85016

London Office
Exmouth House, 3/11 Pine Street,
Farringdon, London EC1R 0JH,
United Kingdom

common sense®

www.commonsense.org

© 2021 Common Sense Media. This work is licensed under a Creative Commons Attribution 4.0 International Public License Common Sense, associated names, associated trademarks, and logos are trademarks of Common Sense Media, a 501(c)(3) nonprofit organization, FEIN 41-2024986.

Cover image: © 2021 iStockphoto LP.