

Who's Watching Whom?

Your Smart TV and Your Privacy

Douglas Povich and Allan Hide
Fairfax County Department of Cable and Consumer Services
Communications Policy & Regulation Division

Lifetime Learning Institute – Class #22SP16
March 8, 2022

Today's Agenda

1. Why smart TVs collect your personal data
2. How they do it
3. What data is collected and where does it go?
4. Is it legal?
5. How to limit or prevent data collection
6. Q&A

Why smart TVs collect your data

To give you a better experience

- Suggest programming you might like
- Provide targeted advertising
- May get coupons, discounts, rewards via phone/mail

\$\$\$

- For your TV manufacturer
- For your video service provider
- For your Internet Service Provider (ISP)

Can be seen as way to lower the cost of the TV

How smart TVs collect your data

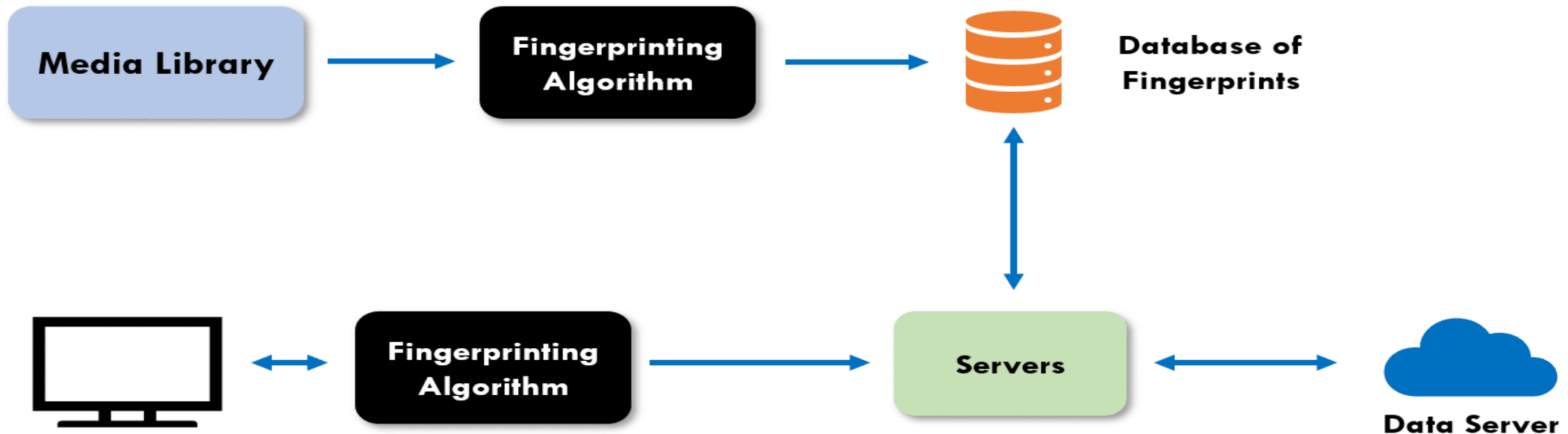
❑ Automatic Content Recognition (ACR)

- ❑ Invented by Vizio in 2009
- ❑ Takes “fingerprint” sample of pixels on your screen and sends to TV maker along with identifier for your TV
- ❑ Attempts to identify all content you watch regardless of source or type (Cable TV, over-the-air, streaming services, DVRs, ads, etc.)
- ❑ Makes TVs like Facebook in their ability to collect data
- ❑ Data not easily reviewed or deleted
- ❑ Goes by different names depending on the manufacturer

How smart TVs collect your data

❑ Automatic Content Recognition (ACR)

First, a database of fingerprints is generated using either audio or video fingerprinting.



Later, an ACR-enabled device (SmartTV for example), generates fingerprints of content that is being played which are compared with the database to recognize content.

What data is collected?

❑ Programming you watch

- ❑ On live broadcasts ACR collects & sends “fingerprint” up to every second
- ❑ Data companies use it to link what you watch with what you do on your phone, tablet & laptop (Samba TV)

❑ Your TV's Internet Protocol (IP) address

- ❑ Your home's and your devices' identity on the Internet – rough geolocation
- ❑ How the TV manufacturers/content providers link up what you watch with the rest of your life (through IP addresses of your other devices)

❑ Not all viewing data is collected

- ❑ Don't keep track of what you watch inside some streaming apps (like Netflix)

Where does your data go?

❑ To the TV manufacturer and their business partners

❑ Different manufacturers send it to different places

- ❑ Amazon, Meta (Facebook), Google (DoubleClick)
- ❑ Virtually all send it to Netflix

❑ Samba TV

- ❑ TV brands including Sony, LG, Sharp, TCL, Panasonic, Sanyo, Toshiba, Westinghouse, Hitachi, Seiki, Phillips and TiVo
- ❑ Social media brands including Amazon, Google, Twitter, Meta (Facebook) and Snapchat
- ❑ Software that communicates with other devices (TVs, phones, tablets, PCs - omniscreeen)
- ❑ Creates a “device map” of your home allowing ads to be sent to all connected devices (sends ad to phone after commercial plays on TV)
- ❑ Advertisers pay Samba TV to send the ads, not to collect the data

It is legal to collect the data?

□ Yes

- It's not Personally Identifiable Information (PII) because it's shared by a household
- But you must have given permission ("opted-in")
(And remember they have your IP address)

□ But watching TV is an activity protected under U.S. law

- 1988 Video Privacy Protection Act (passed after Robert Bork's video-rental records were published)
- 2017 Federal Trade Commission action against Vizio for deceptively tracking viewing habits
 - All TV manufacturers must require consumers to opt-in
 - All revised their privacy policies and terms of use

It is legal to collect the data?

- ❑ And there are other laws that generally protect consumer data, including:
 - ❑ Cable Communications Policy Act of 1984 protections
 - ❑ No disclosure of PII without written permission
 - ❑ A private right of action – can sue in federal court
 - ❑ Virginia Consumer Data Protection Act (CDPA) protections
 - ❑ Ability to access, correct inaccuracies, and delete personal data
 - ❑ Ability to prevent sales of data to 3rd parties
 - ❑ Exception for “targeted advertising”: businesses can use personal data to test its marketing even after opting out

How to Limit Data Collection

- ❑ Don't opt-in
 - ❑ It happens when you set up your TV for the first time
 - ❑ Opting-out requires reading the fine print and making a selection
- ❑ If you already opted-in, you may still opt-out (not easy)
- ❑ Even if you turn off ACR, your smart TV will still collect the data for the manufacturer
 - ❑ Location, which apps you open, more
- ❑ Make your "smart" TV "dumb" – disconnect it from the Internet
- ❑ Use a virtual private network (VPN)

How to Limit Data Collection (cont.)

❑ Will a Virtual Private Network (VPN) help?

- ❑ What is a VPN? It is software that can be installed onto your computer or other electronic device. VPNs make your online activity private (hide your true IP address). If you've sent your bank details to anyone online or use public WiFi networks (coffee shop, airport), you're at risk of exposing your personal information to hackers.
- ❑ Requires contract with VPN hosting provider (e.g., NordVPN or ExpressVPN etc.). How does one set a VPN up?
- ❑ Creates an encrypted connection between you and Internet (encrypted to the VPN server)
 - Uses highly elaborate ciphers and encryption protocols (including secure tunnels which data travels through)
- ❑ Hides your browsing history (your Internet Service Provider (ISP) cannot see what you are looking at) VPN providers claim that **they do not log your usage** (Therefore if required/asked by the Government, the VPN should not have any of your usage data available. Can select your VPN server geo-location anywhere in the World)
 - Useful if on holiday in Italy and want to continue to see your Netflix shows that you pay for back home. Change your VPN server location to the USA*
 - Also, may be useful to change your VPN server location to access programming from other parts of the World, say, in a politically sensitive area (note may also be illegal and dangerous to use VPNs in some countries). Not illegal to use a VPN in the USA!

* Fairfax County is against conducting any activity that is not legal in the USA or VPN location country.

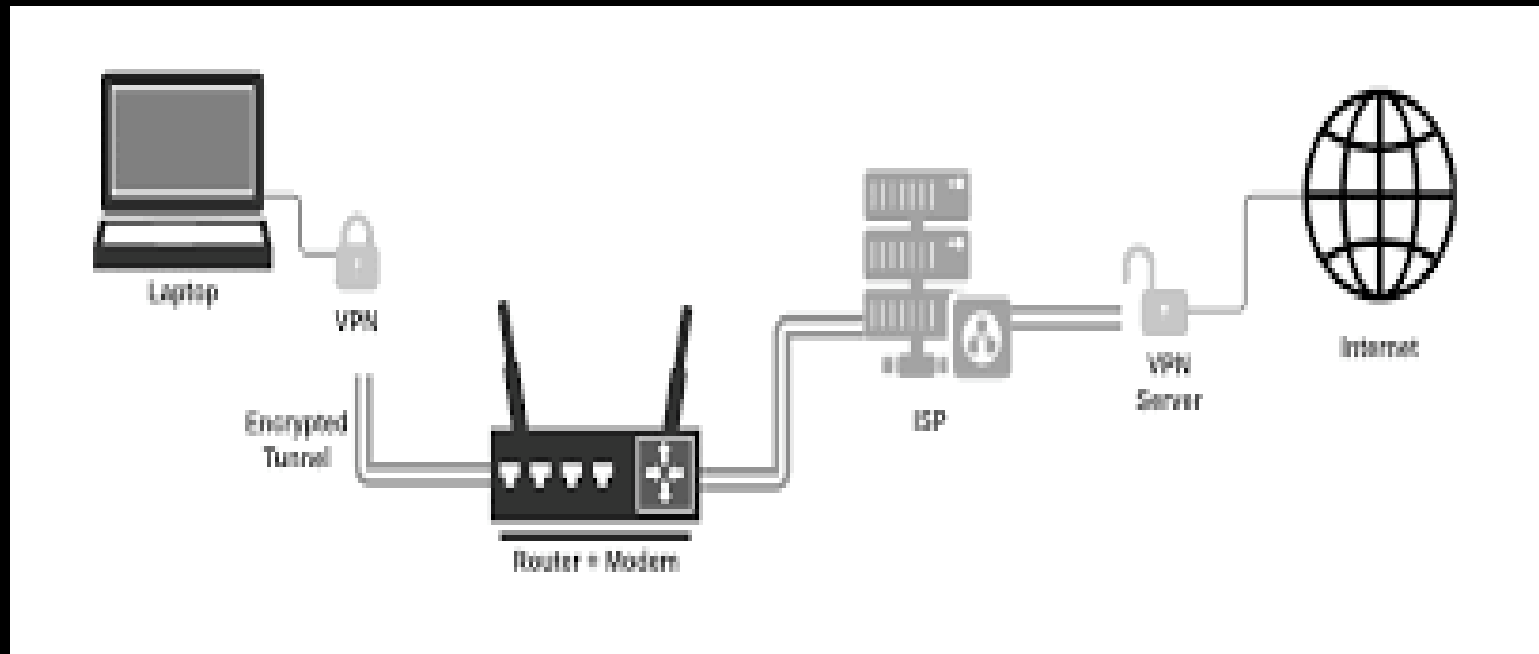
How to Limit Data Collection (cont.)

❑ Will a Virtual Private Network (VPN) help?

- ❑ May be used by some (illegally) to access “pirate” sites and see content for free that normally one would have to purchase*
- ❑ **Smart TVs:** VPNS must be compatible with your Smart TV (easiest to get VPN protection by using apps available on your Amazon Firestick or apps available on Android TVs (using Google Play Store). VPN apps not available on Roku. Smart TVs may be able to achieve partial VPN capability by altering location (DNS settings in conjunction with a VPN provider). Also, If you have the VPN installed on your home router then your Smart TV will also have VPN protection.
 - Stops Internet Service Provider seeing what you are looking at (will/may not get targeted ads for example).
 - Can view programming, say in another Country that you can't access from the USA *(unblocking regional geo-location) e.g., Netflix*, Hulu*
- ❑ VPNs can also be installed on other devices in your home (computer, iPhone etc.). Or you could get blanket coverage for all by installing VPN on your router (including guests visiting) by setting up the VPN on your router (if VPN compatible). If not VPN compatible can add a "slave" router for VPN. Setting up via router is more complex.

* Fairfax County is against conducting any activity that is not legal in the USA or VPN location country.

How do VPNs work?



When you use the Internet you have an **IP (Internet Protocol)** address. A VPN protects you by putting a VPN server (a dedicated computer with VPN software running on it), with a *different* IP address, between you and the website you want to access. Others can't 'see' *your* IP address as it's hidden behind the VPN server's address. It effectively makes you anonymous on the web.

How to Limit Data Collection (cont.)

□ On your Smart TV

- **Interest-based advertising** - aims to show you relevant ads based on the level of interest your household show in products. It will use your TV's unique advertising ID and Internet protocol ID address to provide to third parties
- **Viewing Information services** - what sort of programs you watch. i.e., the networks, channels, websites visited, and programs viewed – and the amount of time spent viewing them
- **Voice navigation services** - if your TV's remote has a microphone that connects to Bixby, Alexa or Google Assistant it can connect to other devices; it will record and analyze what you say

Examples: TVs and Media Devices - How to Opt-out

Samsung TV

- Go to "settings."
- Then go to "support."
- Scroll to "terms and policy."
- Navigate to "viewing information services."
- Uncheck the part that says, "I agree," which will stop it from monitoring what you're watching.
- Then navigate to "interest-based advertisements service privacy notice" and turn it off. This prevents targeted ads.

Roku

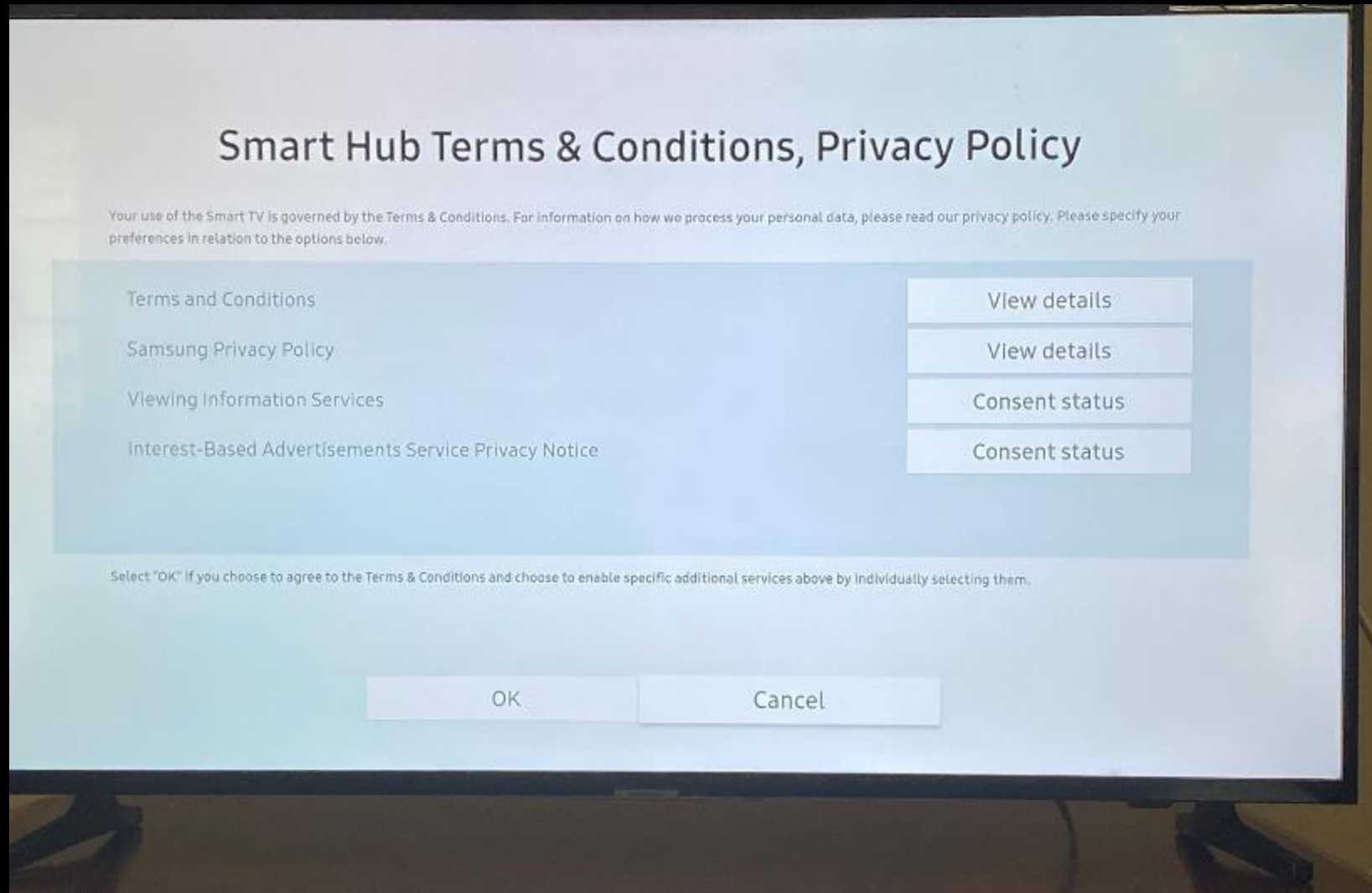
- Go to "settings" on the home screen.
- Go to "privacy."
- Then click on "advertising" and then check "limit ad-tracking."
- Go back to the previous screen and select "smart TV experience."
- Uncheck "use information for TV inputs," which disables the smart TV's ACR technology.

Amazon Fire TV

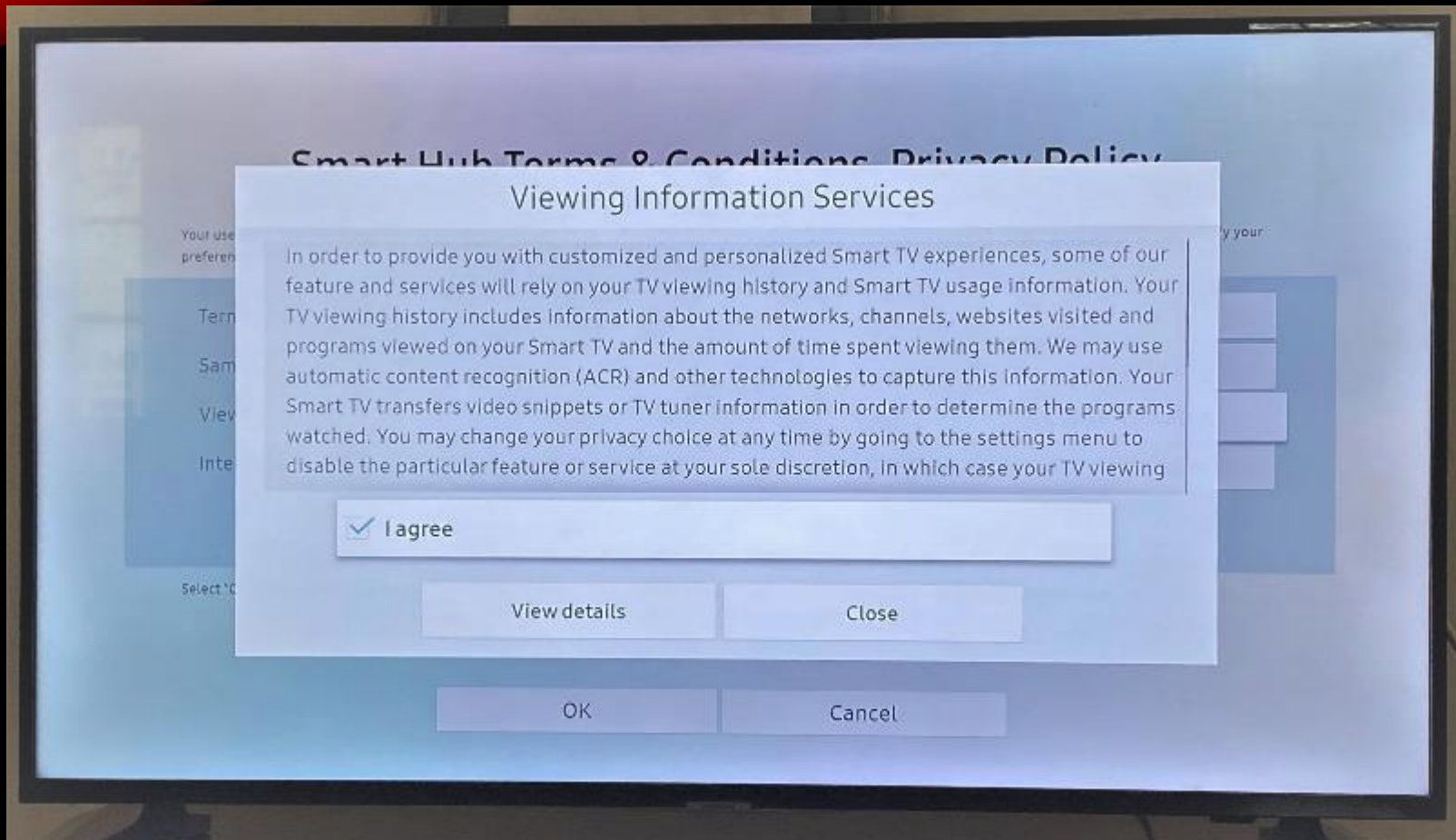
- Go to "settings."
- Go to "preferences"
- Then "privacy settings."
- Under "privacy settings," turn off "device usage data," which prevents using your data for personal marketing purposes.
- Also disable "collect app and over the air usage" and "interest-based ads."

Example: Samsung Smart TV- How to Opt-out

Go to menu/privacy policy/terms:

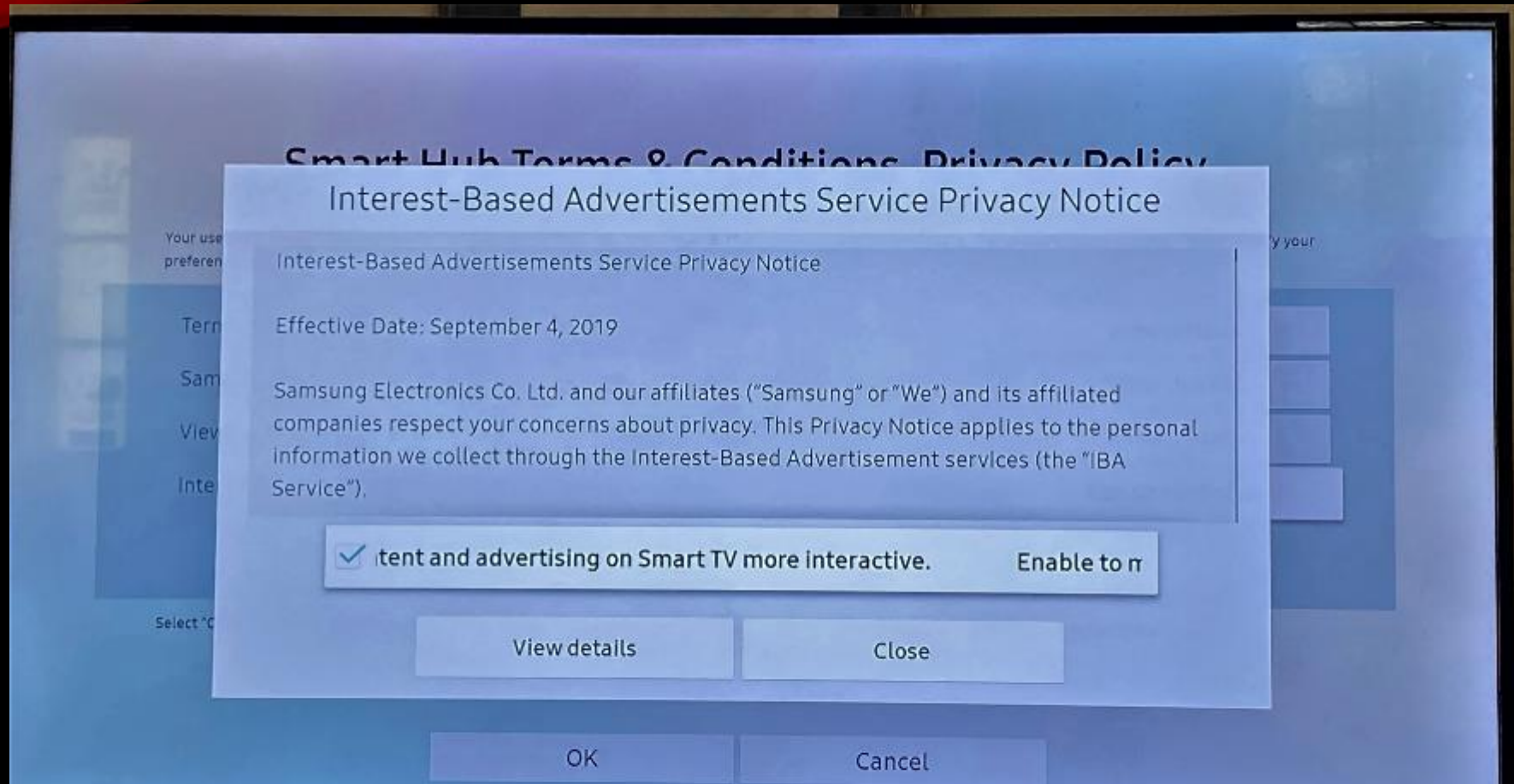


Example: Samsung Smart TV- How to Opt-out



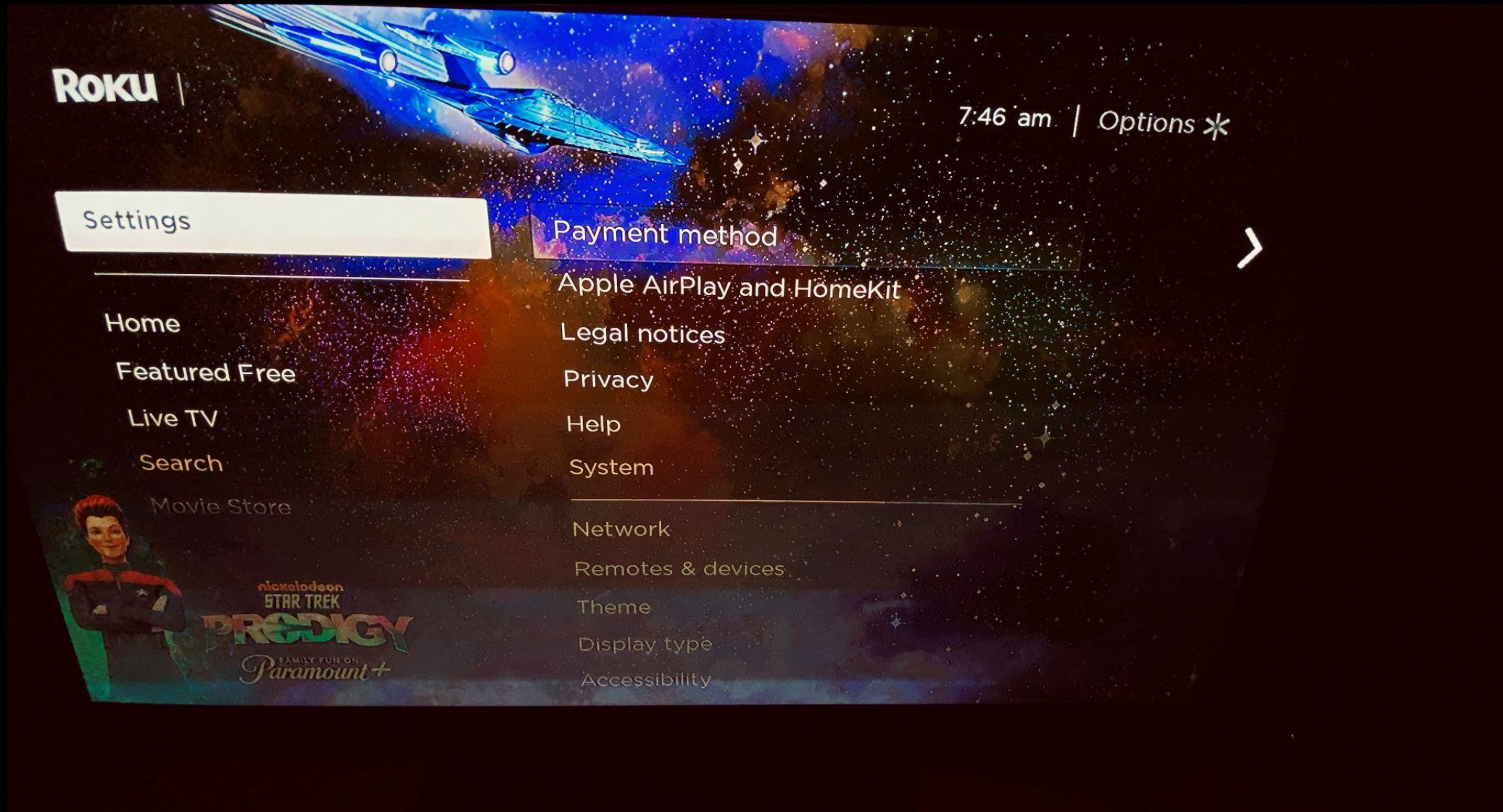
Viewing Information Service: Uncheck the part that says "I agree," which will stop it from monitoring what you're watching

Example: Samsung Smart TV- How to Opt-out

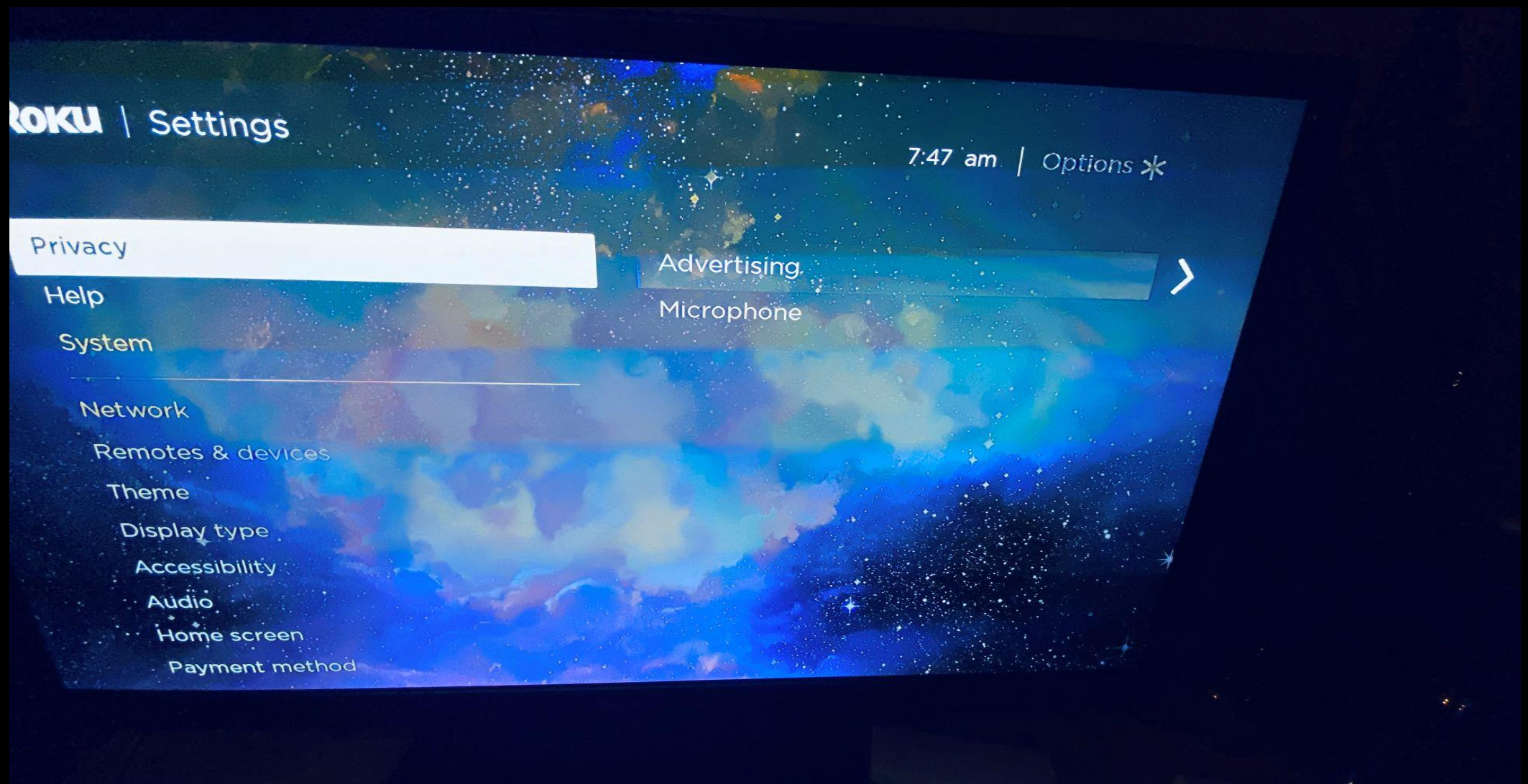


Interest Based Advertisements: aims to show you relevant ads based on the level of interest your household show in products. It will use your TV's unique advertising ID and Internet protocol ID address to provide to third parties

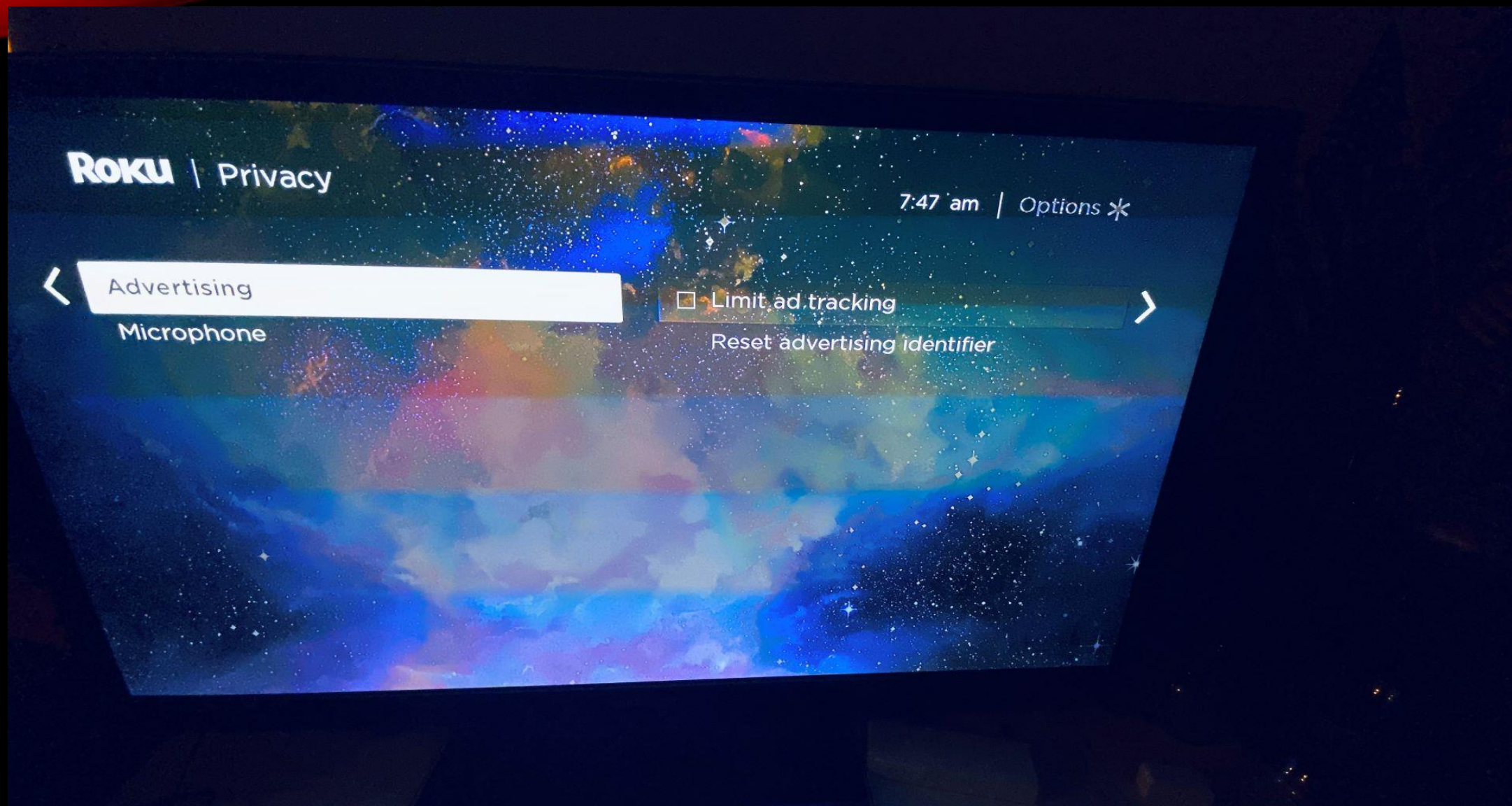
Example: Roku Box or TV- How to Opt-out



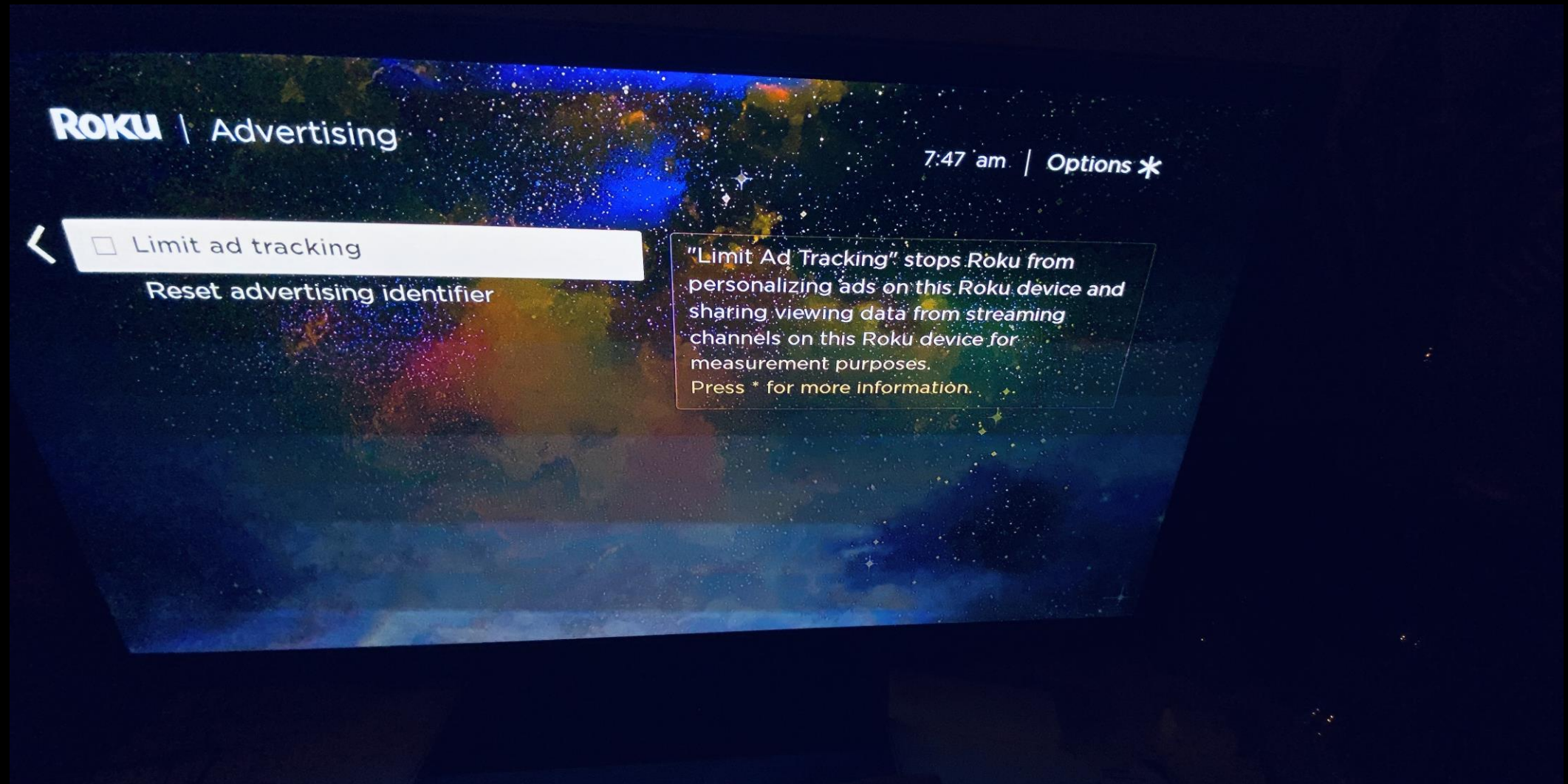
Example: Roku Box or TV- How to Opt-out



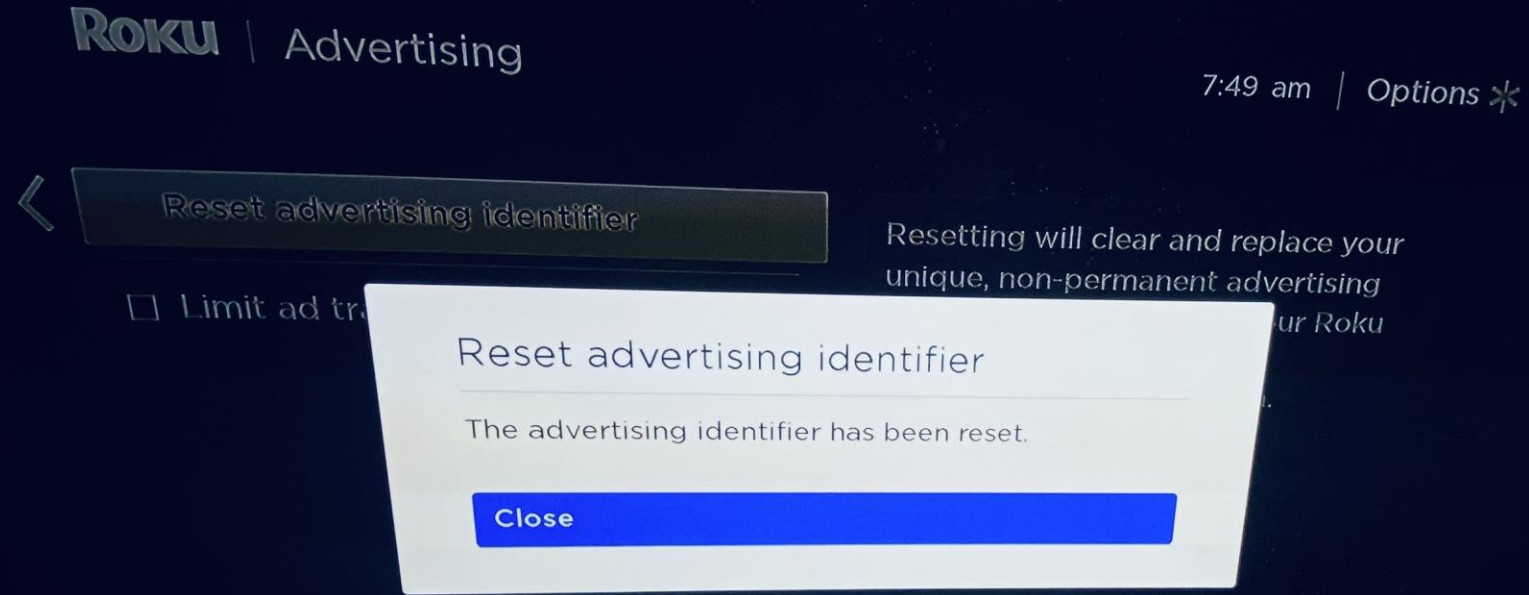
Example: Roku Box or TV - How to Opt-out



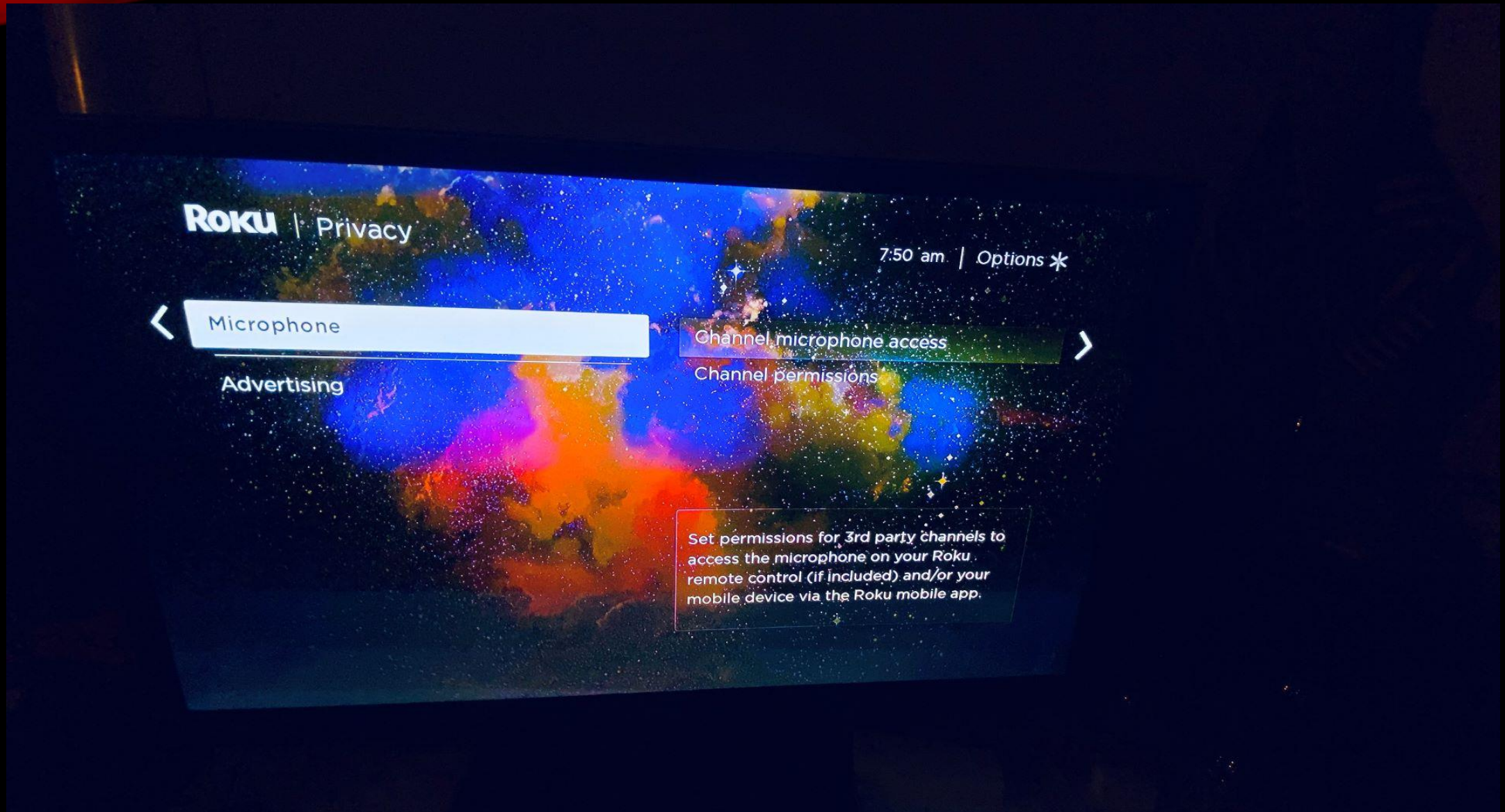
Example: Roku Box or TV- How to Opt-out



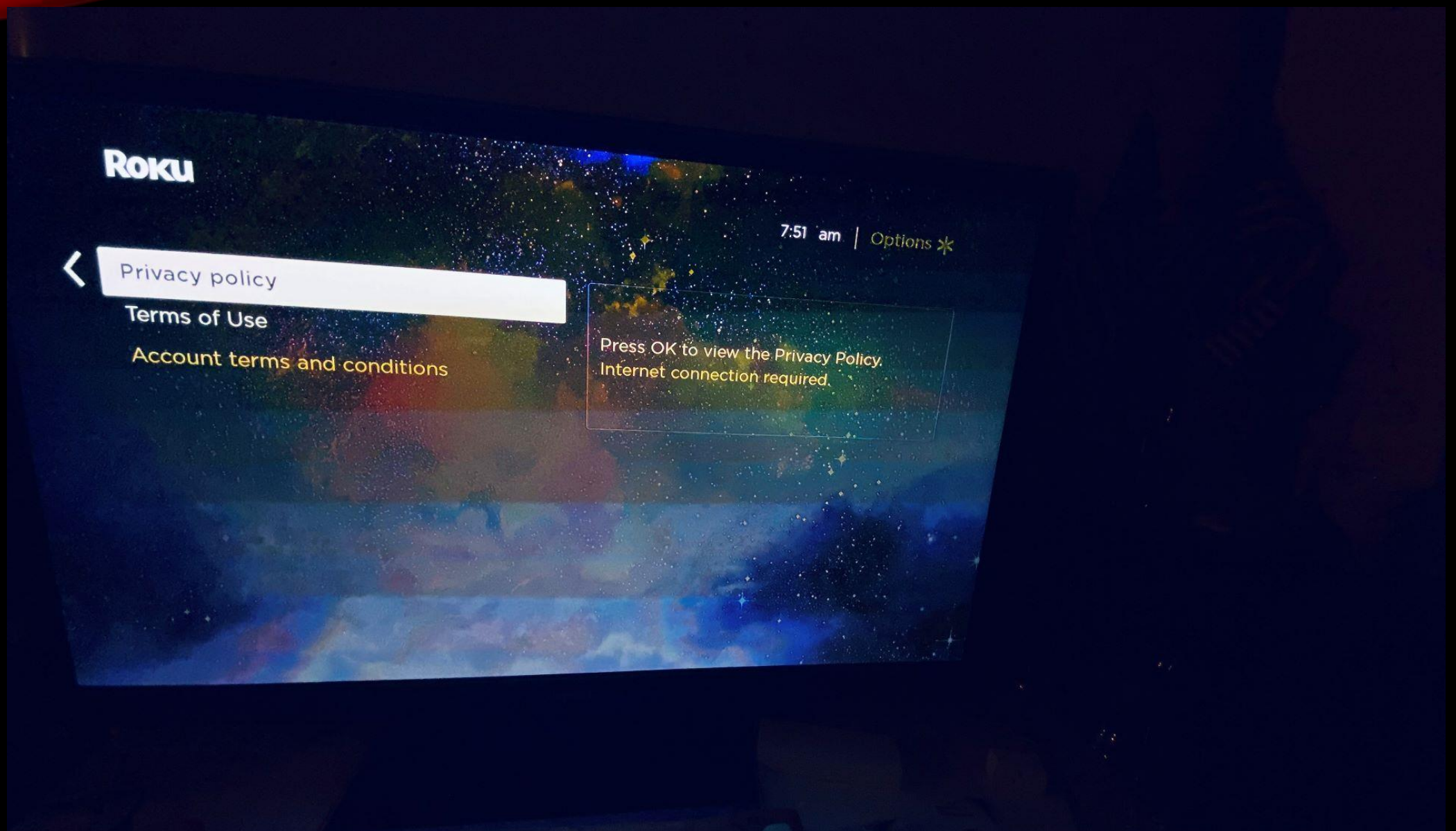
Example: Roku Box or TV- How to Opt-out



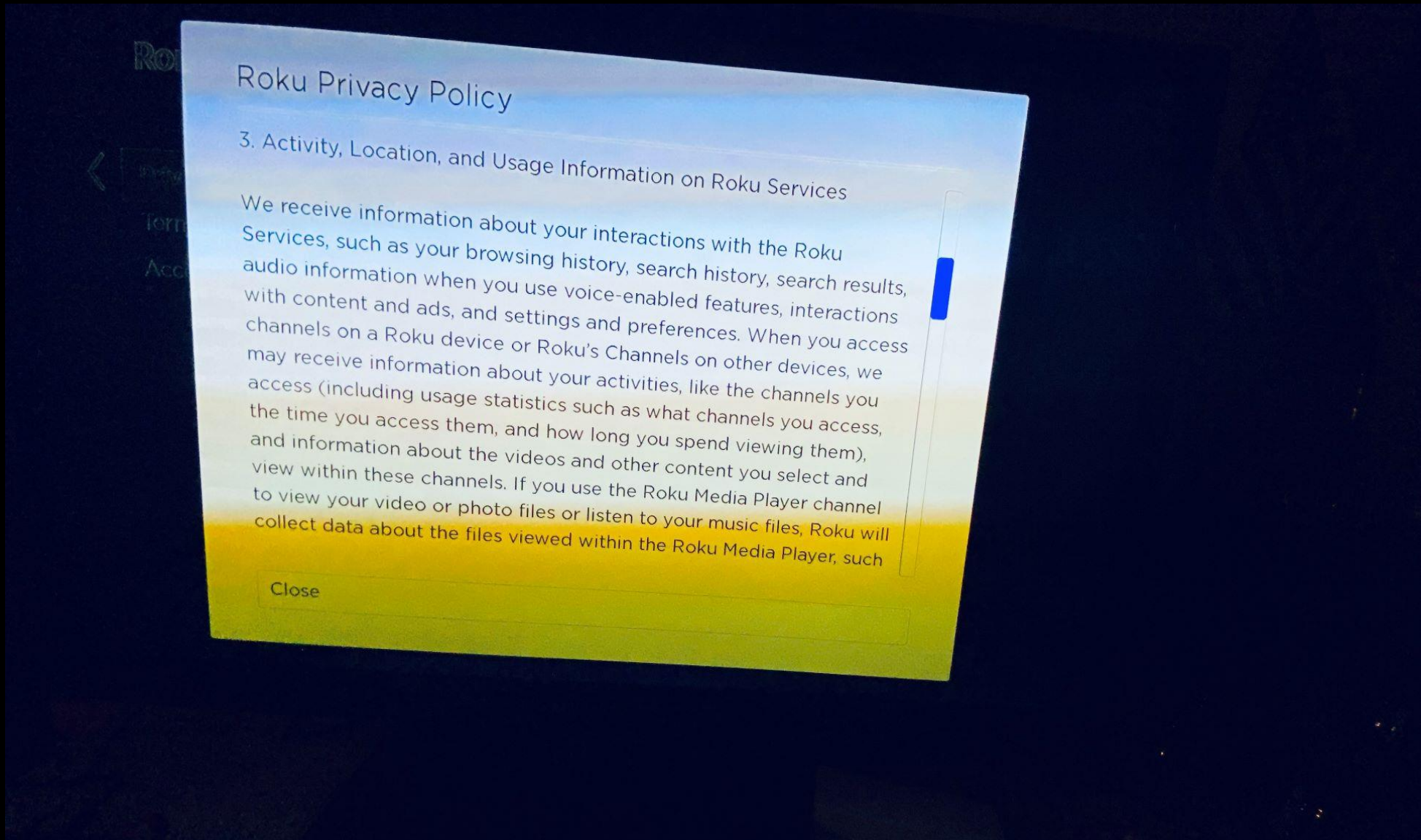
Example: Roku Box or TV- How to Opt-out



Example: Roku Box or TV- How to Opt-out



Example: Roku Box or TV- How to Opt-out



Roku Privacy Policy

3. Activity, Location, and Usage Information on Roku Services

We receive information about your interactions with the Roku Services, such as your browsing history, search history, search results, audio information when you use voice-enabled features, interactions with content and ads, and settings and preferences. When you access channels on a Roku device or Roku's Channels on other devices, we may receive information about your activities, like the channels you access (including usage statistics such as what channels you access, the time you access them, and how long you spend viewing them), and information about the videos and other content you select and view within these channels. If you use the Roku Media Player channel to view your video or photo files or listen to your music files, Roku will collect data about the files viewed within the Roku Media Player, such

Close

Example: Today Show video demo of opting out on different devices

<https://youtu.be/jpIQp1Z4LYg>

Recap

1. **Why smart TVs collect your personal data** - Viewing experience, targeted ads, \$\$\$
2. **How they do it** – Automatic Content Recognition (ACR)
3. **What data is collected and where does it go?** Viewing habits, IP address; Goes to business partners, Samba TV, other data companies
4. **Is it legal?** Yes; it's not PII, but it requires opting-in; legal recourse
5. **How to limit or prevent data collection** – Read the fine print, don't opt in, if opted-in then opt-out; make your TV dumb; consider using a VPN

Questions & Answers

Douglas Povich and Allan Hide

Fairfax County Department of Cable & Consumer Services
Communications Policy & Regulation Division
703-324-5902

Douglas.Povich@fairfaxcounty.gov

Allan.Hide@fairfaxcounty.gov

www.fairfaxcounty.gov