fulu

RESEARCH REPORT

AUTOMATIC CONTENT RECOGNITION

What Smart TVs Send

Findings from an ACR Hackathon



AUTHOR

Kevin O'Reilly

PUBLISHED

October 29, 2026

HACKATHON CO-HOSTS

Northeastern University Cybersecurity and Privacy Institute, FULU, the Ludlow Institute, and CodeDay

AT A GLANCE

Key findings

24	40+	12+	3
hours of testing, Oct. 19–20	students and coders	televisions available to test	teams' results in this report

LG	**ACR messages carried location data.** With root access, a researcher decrypted the data an LG TV sent to its ACR service, including street address, coordinates, and designated market area.
LG	**The TV fingerprinted sound, not picture.** Video with the soundtrack removed produced zero fingerprint messages; a black screen with sound produced 48.
VIZIO	**An unencrypted data stream went to an Amazon server** while the TV played its own WatchFree+ channels, and turning on Do Not Sell left data flowing to Amazon.
VIZIO	**Channel names leaked in plain text,** readable by anyone on the network path, even with Viewing Data turned off.
HISENSE	**Other devices on the home network could read back media links** stored on the TV, without a prompt or anything appearing on screen.

WHAT NEEDS TO CHANGE

Congress should give consumers a permanent right to disable or remove data-collection software from the devices they own, and allow others to provide the tools and help to do so.

INTRODUCTION

By Kevin O'Reilly · October 29, 2026

When most Americans turn on their TV, they expect to be the ones doing the watching. However, smart TV manufacturers and their advertising partners use software known as Automatic Content Recognition (ACR) to track what consumers watch from the comfort of their own couch.

Research conducted over the course of a 24-hour hackathon co-hosted by the Northeastern University Cybersecurity and Privacy Institute, FULU, the Ludlow Institute, and CodeDay adds to the growing list of concerns about ACR's impact on data privacy. The event, which took place from October 19th to 20th, brought together more than 40 students and coders who had access to more than a dozen televisions.

One participant was Atharva Keskar, a Northeastern graduate student studying machine learning. He was able to gain root access to an LG TV. That allowed him to decrypt the data the device sent to LG Ad Solutions's Alphonso ACR. It included location metadata such as address, coordinates, and designated market area.

Keskar determined that the LG's ACR fingerprinted sound rather than video to identify what was playing on the screen, as no fingerprints were sent when he played video with the soundtrack removed. That raises questions about the LG Ad Solutions privacy policy, which states that "Alphonso's ACR service can't detect…human conversation, ambient sounds, and other non-commercial audio or sounds."[1] More research on the topic is needed.

Other teams of students and researchers found that a Vizio television sent an unencrypted data stream to an Amazon server and exposed the names of the channels being watched in plain text. This information was therefore readable by anyone on the network path between the TV and the streaming service. Another team discovered a Hisense television let other devices on the same home network read back plain text media links stored on it.

While this research was limited by the length of the hackathon, it builds upon a growing body of research and concern about ACR practices. *Watching the Watchers*, a new study released by Northeastern researchers, found that opting-out of tracking did not stop Vizio and Samsung televisions from transmitting traffic consistent with ACR. Researchers were also able to gain access to the ACR server used by TVs running VIDAA OS, such as those manufactured by Hisense and Toshiba, without providing a password. In the three hours that they had access, they were able to collect more than 57 million ACR detection results from more than a million TVs running VIDAA OS around the world.[2]

57 million+

ACR detection results collected in three hours, from more than a million TVs running VIDAA OS, via an ACR server researchers reached without a password.

Source: *Watching the Watchers*, Northeastern University

Investigations done by Gamers Nexus and Level1Techs have surfaced concerns about LG TVs' audio recording capabilities, and highlighted past statements by LG executives such as "we own the glass" and "we own the living room."[3]

Consumers, not TV makers or their advertising partners, actually own the televisions in their homes. That ownership should grant them the right to remove ACR software if they so please. Doing so, however, could violate federal law.[4] Sec. 1201 of the Digital Millennium Copyright Act,[5] a law passed in 1998 to prevent piracy at the dawn of the internet, makes it illegal to circumvent digital locks such as password protection or encryption. That is true even if the related activity does not involve copyright infringement.[6]

01

How ACR works

ACR identifies what is on a television screen by sampling it. As often as every few seconds, the TV captures a short snippet of audio or video, reduces it to a compact digital signature known as a fingerprint, and sends it to a server that compares it against a library of known shows, movies, and commercials.[7] A match tells the manufacturer, or the advertising company it works with, what the household is watching and when.

Because ACR is built into the television itself rather than into any one app, it can identify content from many sources, including antenna broadcasts, cable boxes and game consoles plugged in over HDMI, and phones mirrored to the screen. That viewing data is then used to target and measure advertising, and it can be shared with or sold to other companies.[8]

According to *Watching the Watchers*, 82% of U.S. TV households had a smart TV as of 2025. Most manufacturers claim to allow owners to turn ACR off, but the setting often doesn't use the words "automatic content recognition." LG calls it Live Plus, Vizio calls it Viewing Data, and Samsung calls it Viewing Information Services. The study found that turning the setting off fully stopped ACR traffic on only four of the seven systems where researchers identified an ACR server.[9]

82%

of U.S. TV households had a smart TV as of 2025

4 of 7

systems where turning the setting off fully stopped ACR traffic

THE ACR SETTING GOES BY A DIFFERENT NAME ON EACH BRAND	
LG	Live Plus
VIZIO	Viewing Data
SAMSUNG	Viewing Information Services

02

The hackathon teams

Participants were trained in the methods used in *Watching the Watchers*: recording all of a television's network traffic while it plays known content, then comparing what the TV sends with ACR turned on and off. This report covers the three teams whose results are summarized below.

TV TESTED	SOFTWARE	RESEARCHERS	APPROACH
LG 24LB7000PUA	webOS firmware 43.04.24	Atharva Keskar	Gained root access, decrypted ACR messages, and decoded the fingerprint format
VIZIO D32fM-K01	SmartCast firmware 3.720.91-1	Jackson Hyder, Ajin Frank, Atharva Keskar, Abhay Korti	Captured 16 sessions of traffic across apps, inputs, and privacy settings
HISENSE 32QD4SV	VIDAA OS V01.09.61Q.Q0723	Will Sergeant, Kyei Sin Nandar Tun, Gaurang Karpe	Tested the security of the TV's network services and web browser

> Each team tested a single television, and most ran each test once rather than the 30 times used in the Northeastern study. The findings below should be treated as starting points for further research.

03 / LG

What the TV sends to Alphonso

Like most manufacturers, LG encrypts the data its televisions send to Alphonso, LG's ACR subsidiary, so *Watching the Watchers* could only infer what that traffic contained from its size and timing.[10] Root access let Keskar read the messages himself. Over one baseline recording, the TV sent 289 fingerprint messages. Alongside the audio fingerprints, they carried the input source, the app or channel being watched, timestamps, device and session identifiers, and the location fields. Keskar was not able to determine where the TV got its location data or how accurate it is.

DATA IN EACH MESSAGE	WHAT IT REVEALS
Audio fingerprint	What is playing, matched against Alphonso's content library
Input source, app or channel	How the household is watching, such as HDMI, an antenna, or LG Channels
Timestamps	When and for how long
Device and session identifiers	Which TV, linked across viewing sessions
Location fields	Street address, coordinates, and designated market area

Gamers Nexus reported similar collection in its September 2026 investigation, finding that LG's ACR system gathers location, IP address, and the names of nearby Wi-Fi networks.[11]

Keskar also decoded the audio fingerprints. LG's software uses two formats: an older one built on established audio-matching techniques, and a newer one that converts each slice of sound into 63 numbers describing its frequencies. Neither can be played back as the original audio. Both are meant for matching sound against Alphonso's content library, though Keskar could not determine how that matching works on Alphonso's servers.

His muting tests were clear-cut. In trials of roughly three minutes each, normal playback produced 43 and 42 fingerprint messages, video with the sound removed produced none, and a black screen with the soundtrack playing produced 48. *Watching the Watchers* reached the same conclusion from outside the TV, measuring a 97.3% drop in LG's ACR traffic when sound was removed and no drop when the picture went black.[12]

TEST (LG, ABOUT 3 MINUTES EACH)	FINGERPRINT MESSAGES SENT
Normal picture and sound	43
Picture with sound removed	0
Black screen with sound	48
Normal picture and sound, repeated	42

The opt-out did work on this TV. With Live Plus turned on, the TV sent 215 fingerprint messages in each of two roughly 10-minute tests. With it off, the fingerprint uploads he was monitoring stopped, and uploads resumed as soon as the setting was switched back on. That matches the Northeastern study, which found LG's opt-out fully effective.[13] Gamers Nexus reported that opted-out LG TVs still check in occasionally, such as when the set is turned on.[14]

Questions about the microphone remain open. The audio that ACR sampled contained the program's soundtrack, but Keskar could not tell whether that source ever drew on the TV's microphone, and he did not test the TV in standby mode.

Keskar found a security weakness in the rooted TV as well. The ACR uploader accepted his proxy's certificate and sent audio fingerprints through it, even though Keskar hadn't installed the proxy's certificate authority on the TV. He also found that the uploader code he copied from the TV had certificate and hostname verification disabled. If unmodified LG TVs behave the same way, anyone able to intercept a TV's traffic could read its fingerprints and location data. That has not yet been tested on a TV without root access.

04 / VIZIO

An unencrypted data stream tied to WatchFree+

The Vizio team found an unencrypted stream of data that appeared only while the TV played WatchFree+, Vizio's free, ad-supported streaming service. With Viewing Data (Vizio's name for ACR) turned on, the TV sent a small packet to an Amazon server roughly every three-quarters of a second while Fox News or CNN played on WatchFree+. The stream did not appear when the TV sat idle, when the same Fox News feed came in over HDMI or through YouTube, or when the Sesame Street app was open. It stopped when Viewing Data was turned off. The team believes the stream carries fingerprints but was not able to decode it.

WHAT WAS PLAYING (VIEWING DATA ON)	UNENCRYPTED DATA STREAM	INSCAPE CHECK-IN
Fox News on WatchFree+, Oct. 19	YES 800 packets in 10 minutes	YES
CNN on WatchFree+, Oct. 19	YES 800 packets in 10 minutes	YES
Fox News over HDMI	NO	NO
Fox News on YouTube	NO	Not reported
Sesame Street app	NO	YES
TV idle	NO	Not reported
Fox News on WatchFree+, Oct. 20	NO	NO

The stream was also hard to pin down. Partway through one session, it switched to a new server about a second after the TV finished checking in with Inscape, Vizio's ACR company. The TV never looked up either server by name, which suggests that blocklists that filter traffic by domain name would not catch it. On the second day of testing, Fox News on WatchFree+ produced no stream at all, even though video was playing, which suggests Vizio's ACR activity varies from session to session.

Vizio's privacy settings had mixed results. With Do Not Sell turned on, the TV did not check in with Inscape during the test. The team cautioned that Inscape checks in only every few minutes, so its absence from a single 10-minute run could be a matter of timing. Either way, the TV kept sending the same amount of data to

Amazon Kinesis, about 85 KB per run. *Watching the Watchers* identified that Kinesis server as the destination most consistent with Vizio's ACR, and found that turning off Viewing Data had no effect on its traffic.[15] The hackathon result suggests Do Not Sell doesn't stop it either, though the team ran the comparison only once.

TRAFFIC DURING BACK-TO-BACK SESAME STREET SESSIONS	DO NOT SELL OFF	DO NOT SELL ON
Inscape (Vizio's ACR company)	2 check-ins, about 5 KB sent	None
Amazon Kinesis	5 connections, 85.2 KB sent	5 connections, 86.5 KB sent

Even with Viewing Data turned off, WatchFree+ revealed what was on screen. Channel names such as "foxnewsnow" and "cnnus" appeared in plain text in the web addresses the TV looked up from Amagi, the company that delivers WatchFree+ streams. Anyone on the network path, including an internet provider, could read them. The Northeastern study first documented this leak and found that no setting turns it off.[16]

The hackathon team found no ACR activity when content came in over HDMI, matching the study's results for Vizio.[17]

05 / HISENSE

Media links and tracking IDs left open

The Hisense team tested the security of a TV running VIDAA OS, the same operating system whose ACR data *Watching the Watchers* found traveling unencrypted.[18]

Phones and laptops on a home network can send media to the TV to play. When they do, the TV displays a prompt asking the owner to agree or disagree, and in the team's tests, that prompt worked as intended. However, the TV saves the link it was sent before it asks, and any other device on the network can read that link back without a prompt or anything appearing on screen. Using synthetic data, the team placed an access code in a link, retrieved it from a second device, and used the code to download the protected file. That download worked only because the team's own media server accepted anyone who presented the code. Nonetheless, the team pointed to the risk this poses when consumer TVs end up in sensitive settings, such as a hospital using one as a replacement display, where a link could carry a patient ID.

The team also found that web pages running in the TV's built-in browser, including a frame loaded from a separate origin, could read the TV's device ID and advertising ID.[19] Advertisers use those identifiers to follow viewers across apps and ads.[20] The Northeastern study similarly found VIDAA attaching a permanent device ID, which owners cannot reset, to every ACR message.[21]

The TV also appeared to be running outdated software. After a firmware update, it still used a web browser based on Chromium 111 and an AirPlay component older than the version Apple lists as fixing known flaws.[22] Hisense would need to confirm whether those fixes were applied separately.

06

Hackathon findings compared with prior research

FINDING	TV	RELATION TO PRIOR RESEARCH
ACR messages contain fingerprints, viewing details, IDs and location fields	LG	**Extends**: Northeastern study inferred from encrypted traffic; Gamers Nexus reported location collection
Fingerprints depend on sound, not picture	LG	**Confirms** study (97.3% traffic drop without sound)
Live Plus opt-out stopped the monitored fingerprint uploads	LG	**Confirms** study; Gamers Nexus saw some check-ins after opt-out
Uploader accepted an untrusted certificate	LG	NEW rooted device only
Unencrypted suspected fingerprint stream on WatchFree+ only	VIZIO	NEW
Do Not Sell left Kinesis traffic unchanged	VIZIO	**Confirms** study
Channel names leak through Amagi lookups with tracking off	VIZIO	**Confirms** study
HDMI not fingerprinted	VIZIO	**Confirms** study
Stored media links readable by other devices	HISENSE	NEW
Device and ad IDs readable by web content	HISENSE	**Parallels** study's VIDAA ID exposure

07

What needs to change

The hackathon results, *Watching the Watchers*, and the Gamers Nexus investigation all point in the same direction: consumers have good reason to be concerned about what their televisions collect and who can see it. In just 24 hours, students found location data in LG's ACR messages, an unencrypted data stream on Vizio's own channels, a Do Not Sell setting that left data flowing to Amazon, and channel names visible to anyone on the network path.

The tools consumers have today are not enough to protect them. ACR settings go by a different name on most brands, and on Samsung and Vizio televisions, turning them off did not stop traffic consistent with ACR.[23] No setting stops Vizio's channel names from leaking. Blocklists may miss servers that a TV reaches without looking them up by name. Disconnecting a TV from the internet works, but it also disables the apps and features people paid for.

The most reliable option would be to remove ACR software altogether. The U.S. Copyright Office currently grants an exemption to Sec. 1201 that lets owners jailbreak smart TVs so they can run lawfully obtained apps, but does not seem to allow for the removal of software.[24] FULU has submitted a petition to the Copyright Office to change that in the course of its 2027 rulemaking.[25] However, that exemption has to be renewed every three years,[26] it is unlikely to cover removing ACR built into a TV's operating system, and the law still prohibits distributing the tools most owners would need to do it.[27]

RECOMMENDATION

Congress should give consumers a permanent right to disable or remove data-collection software from the devices they own, and allow others to provide the tools and help to do so. Lawmakers and regulators should also require TV makers to honor opt-outs, encrypt viewing data, and clearly disclose every source of content that ACR monitors.

Hackathon findings come from the teams' presentations, "Watching Vizio," "Inside LG ACR," and "The TV Asked Before Playing. It Had Already Shared the URL."

REFERENCES

Notes

1 LG Ad Solutions, "Site Privacy Policy," https://lgads.tv/site-privacy-policy/.

2 Ilgar Mammadov, Het Rutul Joshi, Daniel J. Dubois, and David Choffnes, *Watching the Watchers: Privacy Analysis of U.S. Smart TV Automatic Content Recognition* (Proceedings on Privacy Enhancing Technologies, 2027), https://watchingthewatchers.github.io/watchingthewatchers/paper.pdf. The study was partially funded by the Ludlow Institute, a co-host of the hackathon.

3 Gamers Nexus, "216,000,000 Spy TVs," YouTube, September 2026, https://www.youtube.com/watch?v=6IFVTcM28KA.

4 Freeman Law, "Digital Millennium Copyright Act: Key Provisions Explained," https://freemanlaw.com/digital-millennium-copyright-act-key-provisions-explained/.

5 U.S. Copyright Office, "Section 1201 Study: Notice and Request for Public Comment," 80 Fed. Reg. 81369 (December 29, 2015), https://copyright.gov/fedreg/2015/80fr81369.pdf.

6 Electronic Frontier Foundation, "Unintended Consequences: Three Years under the DMCA," 2002, https://w2.eff.org/IP/DMCA/20020503_dmca_consequences.html.

7 Mammadov et al., *Watching the Watchers*.

8 Mammadov et al., *Watching the Watchers*.

9 Mammadov et al., *Watching the Watchers*.

10 Mammadov et al., *Watching the Watchers*.

11 Gamers Nexus, "216,000,000 Spy TVs."

12 Mammadov et al., *Watching the Watchers*.

13 Mammadov et al., *Watching the Watchers*.

14 Gamers Nexus, "216,000,000 Spy TVs."

15 Mammadov et al., *Watching the Watchers*.

16 Mammadov et al., *Watching the Watchers*.

17 Mammadov et al., *Watching the Watchers*.

18 Mammadov et al., *Watching the Watchers*.

19 Note: The team ran this test with its own local pages and with the TV's privacy consent set to "Accept All"; it did not test public websites, stricter privacy settings, or whether the IDs persist across restarts.

20 Princeton Center for Information Technology Policy, "Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices," September 18, 2019, https://blog.citp.princeton.edu/2019/09/18/watching-you-watch-the-tracking-ecosystem-of-over-the-top-tv-streaming-devices.

21 Mammadov et al., *Watching the Watchers*.

22 Apple, "About the security content of AirPlay audio SDK 2.7.1, AirPlay video SDK 3.6.0.126, and CarPlay Communication Plug-in R18.1 Updates," https://support.apple.com/en-us/122403.

23 Mammadov et al., *Watching the Watchers*.

24 U.S. Copyright Office, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," October 28, 2024, https://www.govinfo.gov/content/pkg/FR-2024-10-28/pdf/2024-24563.pdf.

25 U.S. Copyright Office, "Exemptions To Permit Circumvention of Access Controls on Copyrighted Works," (October 28, 2026), https://www.federalregister.gov/documents/2026/10/28/2026-21939/exemptions-to-permit-circumvention-of-access-controls-on-copyrighted-works

26 U.S. Copyright Office, "Section 1201 Study."

27 Electronic Frontier Foundation, "Unintended Consequences"; see also U.S. Copyright Office, "Section 1201 Study."

