
YOUR TV IS WATCHING YOU

Table of Contents

Your TV is Watching YOU!

Video Length: 19:38

Lesson Description

What if your TV isn't just showing you programs but is watching you back? This video exposes how smart TVs record what's on the screen, capture sound as well, and share that data with companies that use it to target, influence, manipulate, and profit from viewers. It challenges students to think critically about privacy, consent, and the real cost of "smart" technology.

Objectives

Students will be able to:

- describe the ways smart TVs gather information from viewers and their environments.
- illustrate how collected data can be combined to build personal or behavioral profiles.
- investigate the ethical and social implications of hidden surveillance in household technology.
- propose realistic actions people can take to limit or prevent invasive data collection.

Concepts & Key Terms

ACR (Automatic Content Recognition): technology built into many smart TVs that takes snapshots of what is on the screen to identify what viewers are watching

Algorithm: a set of computer instructions that tells a device how to process data or make decisions

Consent: permission given by a person to allow data about them to be collected, shared, or used

Data Broker: a company that collects, buys, and sells personal data from various sources to create detailed consumer profiles

Data Mining: the process of analyzing large amounts of information to find patterns or make predictions about people's behavior

Privacy Policy: a legal document that explains how a company collects, uses, and shares user data—often written in confusing language few people read

Surveillance: the close observation or monitoring of people's activities, often through technology

Targeted Advertising: ads customized for individuals based on their online activity, viewing habits, or personal data

Preview Activity

Use Think, Pair, Share to have students answer and discuss these preview questions: Have you ever noticed your devices seem to "know" what you like? How

much privacy should people expect at home when using technology? Why might companies want data about what people watch or say near their devices?

OR

Distribute copies of the K-W-L worksheet to the class. Have students fill in the K and W sections. After showing the video, have students complete the L section and answer the questions at the bottom of the worksheet.

Viewing Guide Instructions

We recommend that teachers show the video twice: first to allow students to view the video and focus on the issues presented, and second to allow them time to complete the viewing guide. After they complete the viewing guide, allow students a few minutes to work in pairs to share and verify answers.

Answers to Viewing Guide

1. snapshots
2. computer
3. data
4. worldview
5. silence

Your TV is Watching YOU!

Viewing Guide

Name _____ Date _____

Class _____Period _____ Teacher _____

Directions: As you watch the video, fill in the blanks with the correct words.

1. The smart TV is continuously capturing _____ of what the user is streaming.
2. In other words, when you connect your computer to your TV, the TV is taking snapshots of what's on your _____.
3. A 2019 study by researchers at Northeastern University and Imperial College London found that almost all TVs they tested sent _____ to Google and Netflix, even though they never connected any Netflix accounts.
4. There is a tremendous amount of value in being able to influence someone's _____ or choices.
5. Companies weaponize legislation like the CFAA to _____ research.

Take a few moments to reflect on the video and answer these questions.

1. How might targeted ads or suggested videos influence what people believe or buy?

_____

_____

_____

2. How do you feel realizing that your attention—and even your outrage—can be turned into profit for others?

_____

_____

_____

Discussion & Analysis

1. What is a smart TV?
2. What kind of information can smart TVs collect from users?
3. How do companies use the data that smart TVs gather?
4. What privacy risks come from having a smart TV in your home?
5. How does this kind of surveillance affect your sense of freedom or security?
6. Do you think users truly give consent when they click "I agree" to long privacy policies? Why or why not?
7. How can detailed viewing data be used to shape what people buy—or even what they believe?
8. If a company uses your personal data to change your behavior, is that manipulation or marketing?
9. What does it mean for elections if voters' opinions can be shaped by private data collected from their homes?
10. How does the line between persuasion and control shift when artificial intelligence personalizes content for each user?
11. Do you think people still have free will if technology constantly adjusts what they see to influence their choices? Explain.
12. If online platforms or smart devices can predict what will anger or excite people, how might that affect what content they show?
13. If smart devices help create echo chambers that confirm what users already believe, how can individuals break out of them?
14. What ethical lines are crossed when companies or governments use data to exploit fear, envy, or anger for influence?
15. How might the constant flow of targeted media affect trust—in government, in media, and even in each other?

Discuss These Lines from the Video

Your smart TV is taking constant snapshots of everything you watch.

Even when you are using your smart TV as just a dumb screen, by connecting your laptop using an HDMI cable, it's still performing ACR.

There are audio samples being collected from that meeting, by these smart TVs.

We shouldn’t have let faceless companies and governments into our living rooms and bedrooms.

Companies use the CFAA to silence researchers who expose shady practices.

It’s almost impossible to buy a non-smart TV these days.

The whole system is murky and opaque by design, and most people have no idea what’s going on.

There is a tremendous amount of value in being able to influence someone’s worldview or choices.

Quotes for Discussion

A TV is no longer just a device for showing you content – it has become a two-way mirror allowing you to be observed in real time by a network of advertisers and data brokers. – Rowenna Fielding

Microphones and software are listening for instructions and they can capture conversations and other sounds within range. – Toby Lewis

No doubt, privacy is constantly challenged by ever advancing technology, and data is mined ubiquitously for its value, but privacy is far from dead.
– Jedidiah Bracy

A world without privacy is less imaginative, less empathetic, less innovative, less human. At Apple, that is not the world we want to live in. We believe that privacy is a fundamental human right... – Tim Cook

The goal is to keep the bewildered herd bewildered. It's unnecessary for them to trouble themselves with what's happening in the world. In fact, it's undesirable—if they see too much of reality they may set themselves to change it.
– Noam Chomsky

Recent technological advancements, involving generative AI and personality inference from consumed text, can potentially create a highly scalable 'manipulation machine' that targets individuals based on their unique vulnerabilities without requiring human input. – Sandra C. Matz, et al.

Arguing that a true democracy requires more than competitive politics; it requires an engaged and truthfully informed citizenry, which is threatened by algorithmic opacity. – Cathy O’Neil

All persons ought to endeavor to follow what is right, and not what is established.
– Aristotle

Activities

1. Have students complete the K-W-L chart in class or for homework. (Recall that the K and W sections are to be completed before watching the video and the L section after watching the video.)

2. Have students complete the political cartoon activity in class or for homework.

3. Have students complete the PMI chart in class or for homework.

4. Have students complete and submit the Exit Ticket as they leave class.

5. Students make a list of all the devices in their homes that connect to the internet, then mark which ones have cameras or microphones. They discuss how much each device might "know" about them.

6. In pairs, students review a real privacy policy from a TV or streaming company, skim it, and highlight confusing or vague language. They share what the company can actually do with user data.

7. In small groups, students sit in a circle and discuss the question: *When does persuasion become manipulation?* Each student should speak once, use evidence from the video, and respond to a peer respectfully.

8. Pose a scenario: *What if a government gained access to all smart TV data?* Groups brainstorm possible outcomes for privacy, freedom, and public trust. They present both benefits and dangers.

9. Students write a short paragraph about how they feel knowing their TV might record them and whether that would change their viewing habits.

10. Individually, students look up a real-life privacy lawsuit involving a tech company, summarize what happened, and explain how it connects to the video.

11. Students write a short opinion piece arguing either that smart technology helps or harms society, using at least one example from the video.

12. Students watch a few online ads and discuss how targeted advertising might use information collected from smart TVs.

13. Teams write and film a 30-second public service announcement warning viewers about hidden data collection and suggesting one way to protect privacy.

14. In small groups, students imagine how TV technology might look ten years from now and predict how privacy could improve—or decline—if current trends continue.

Name _____ Date _____

Class _____Period _____ Teacher _____

Quiz: Your TV is Watching YOU!

Directions: Select the answer that best completes the sentence.

1. The term *Automatic Content Recognition* means a TV can _____.
   A. record live broadcasts
   B. measure internet speed
   C. block streaming services
   D. identify what appears on its screen

2. Even when used as a monitor, a smart TV can still _____.
   A. protect user passwords
   B. run without electricity
   C. collect data through ACR
   D. stop malware

3. Some researchers face legal threats under the CFAA because they _____.
   A. create harmful viruses
   B. design new smart TVs
   C. expose how companies collect data
   D. sell personal information

4. The video suggests that privacy settings are often _____.
   A. updated by the government
   B. hidden and confusing
   C. controlled by advertisers
   D. clear and easy to find

5. The main idea of the video is that smart TVs _____.
   A. stop unwanted advertising
   B. cannot connect to the internet
   C. are safer than computers
   D. watch users to collect data for profit

Answer Key:

1. D
2. C
3. C
4. B
5. D

Name _____ Date _____

Class _____ Period _____ Teacher _____

Your TV is Watching YOU!

Political Cartoon Activity

Directions: Use the political cartoon to answer the questions.

What does the phrase *"The Profit of Division"* suggest about the relationship between emotion, media, and money? _____

_____

_____

_____

_____

_____

_____

Who are the people around the table supposed to represent? _____

_____

_____

_____

How do data and algorithms make it easier to identify which emotions will "sell" best? _____

_____

_____

How can individuals recognize when their emotions are being manipulated for profit or power? _____

_____

_____

_____

How do you feel knowing that the shows, ads, or videos you watch might be designed to influence your emotions or opinions? _____

_____

_____

_____

Name _____ Date _____

Class _____ Period _____ Teacher _____

Your TV is Watching YOU!

PMI Chart

P = Plus: What might be some positive effects of smart TVs collecting data?
M = Minus: What might be some negative effects of smart TVs collecting data?
I = Interesting: What is interesting or surprising about smart TVs collecting data?

+ Plusses +	- Minuses -	I

How might targeted ads or suggested videos influence what people believe or buy? _____

_____

_____

_____

What could happen if people stopped caring about privacy or assumed surveillance was normal? _____

_____

_____

_____

Name _____ Date _____

Class _____ Period _____ Teacher _____

Your TV is Watching YOU!

K-W-L Chart

Directions: Complete the **K** and **W** sections prior to watching the video. After you have seen the video, complete the **L** section and answer the questions below the K-W-L chart.

K	W	L
What I know about smart TVs collecting data from viewers…	What I want to know about smart TVs collecting data from viewers…	What I've learned about smart TVs collecting data from viewers…

Should TV companies be allowed to collect this data? Why or why not? _____

_____

_____

_____

How can detailed viewing data be used to shape what people buy—or even what they believe? _____

_____

_____

_____

_____

Exit Ticket

Name

Admit One

If technology can watch, listen, and learn from everything we do, how can we stay truly free in a connected world?

Admit One

EXIT TICKET

Name

Admit One

If technology can watch, listen, and learn from everything we do, how can we stay truly free in a connected world?

Admit One

EXIT TICKET

Name

Admit One

If technology can watch, listen, and learn from everything we do, how can we stay truly free in a connected world?

Admit One

EXIT TICKET

Transcript

Naomi Brockwell
Your smart TV is taking constant snapshots of everything you watch. Wait, what? Isn't watching TV meant to be a private activity from the comfort of your own home? Not anymore.

Do you think that the things that we're watching on our smart TVs are private, just between us and our television?

Yash Vekaria
Definitely not.

Naomi Brockwell
In this video, we're going to take a look at what smart TVs are actually doing behind the glass. We'll break down how they collect your most sensitive data. We'll explore how that data is used to profile and manipulate you. And finally, we'll go over some ways to protect yourself. Basically, in internet age, smart TV watches you. Let's get started by understanding what smart TVs are and how they operate. They're basically just modern TVs. It's almost impossible to get a non-smart TV these days.

YouTube/Washington Post
Most new TVs connect to the internet to stream shows and movies on demand.

Naomi Brockwell
They come preloaded with apps for watching content, things like Amazon Prime Video, YouTube, Hulu, cable provider apps, and fast channels.

YouTube/Washington Post
They're also quietly sending out reports about everything you watch.

Naomi Brockwell
Quietly being the keyword.

Yash Vekaria

If you ask a random user, “Do you know that your smart TV is doing this?” They will likely not know about it.

Naomi Brockwell
Yash Vekaria is a researcher who worked on a paper about how bad smart TVs really are for privacy.

Yash Vekaria
Our study focuses on two major players in the market, one being LG and one being Samsung. While we were investigating this, we stuck upon something which is known as ACR, which stands for automatic content recognition.

Naomi Brockwell
It's a technology built deeply into the OS of modern TVs. How it works is basically:

Yash Vekaria
The smart TV is continuously capturing snapshots of what where the user is streaming. Now, these snapshots could be audio snapshots or video snapshots, or it could be both.

Naomi Brockwell
And by doing this, the TV manufacturer is able to recognize whatever is playing.

YouTube/Washington Post
ACR data allows them to know which household is watching a particular program so that they can target ads to impressionable audiences.

Yash Vekaria
You will be astonished by the number of snapshots they collect every second.

Naomi Brockwell
How many snapshots are they collecting?

Yash Vekaria
LG openly mentioned that this frequency is 10 milliseconds for them.

Naomi Brockwell
Every 10 milliseconds, a snapshot is being taken.

Yash Vekaria
Yeah.

Naomi Brockwell
This is crazy. That's 100 snapshots every second.

Yash Vekaria
And for Samsung, it is 500 milliseconds.

Naomi Brockwell
These snapshots are batched together to form something called a content fingerprint, which is sent to the TV manufacturer's servers.

Yash Vekaria
The smart TV manufacturers maintain their own database of these content fingerprints. The server can identify what show is exactly being watched by the user based on the match. So, if the content fingerprint of an NFL show matches, then the server can infer that the user is watching NFL at this moment. What if you're watching something you don't want others to know about? It is a big privacy concern for the users.

Naomi Brockwell
But it gets worse. It's not just shows that the TV is taking snapshots of.

Yash Vekaria
Even when you're using smart TV as just a dumb screen by connecting your laptop using an HDMI cable, they are still performing ACR.

Naomi Brockwell
In other words, when you connect your computer to your TV, the TV is taking snapshots of what's on your computer. The implications of that are pretty wild.

Yash Vekaria
Let's suppose you're browsing through an email on your laptop and just projecting it on a bigger screen just to view it in a better manner. That information is still being captured and sent to the ACR servers.

Naomi Brockwell

So let's say you and I are having a Zoom meeting for our corporation, and we're thinking, well, there are 20 people on this call. Let's put it on a big monitor. There are audio samples being collected from that meeting by these smart TVs.

Yash Vekaria
Yeah, exactly.

Naomi Brockwell
These are private activities that aren't meant to be shared. Same with doing your banking, logging into accounts, or simply browsing through personal photos on a larger screen. Why are our televisions taking snapshots? Now, currently, the way ACR works is the recordings themselves aren't not necessarily sent to the TV manufacturer, just the content fingerprint. But your TV itself is still collecting these snapshots. As we know, modern AI can instantly identify what's in any photo, right down to the most subtle details. This technology just keeps getting better, too.

It's going to get easier and easier to recognize everything.

Naomi Brockwell
According to Tobi Lewis, global head of threat analysis at Darktrace, ACR could be used in conjunction with data from facial recognition built to the TV's cameras, sentiment analysis, speech to text, and content analysis, all put together to build an in-depth picture of an individual user.

We should presume that that's the direction we're headed in, moving away from fingerprint-powered ACR and into an era of instant, AI-powered content recognition, where every subtle detail of what's on your screen will be tagged and analyzed.

An ACR is just one tool currently used to spy on us. There are all kinds of other ways that these companies collect our data, like collecting IP addresses or through data sharing agreements.

A 2019 study by researchers at Northeastern University and Imperial College London found that almost all TVs they tested sent data to Google and Netflix, even though they never connected any Netflix accounts. A 2017 lawsuit against Vizio revealed that the company was sharing the detailed viewing histories of 11 million users with data brokers. Unfortunately, there are countless ways that all this data can be weaponized. Let's start with simple viewing habits.

Yash Vekaria
For example, you're interested in sports. Mostly, you watch sports shows from 9:00 to 12:00, but in the afternoon, you watch something else. Let's say you watch fashion shows.

Naomi Brockwell
These habits are tracked and analyzed by TV manufacturers, and over a period of time—

Yash Vekaria
They can develop a holistic profile of the user to understand what are their viewing patterns, what are their behavioral traits, what are they interested in, what are they not interested in.

Naomi Brockwell
The most obvious use is to sell this data to streaming platforms, stores, or companies who can sell you things.

Yash Vekaria
This is just one dimension of the data. What is your viewing habits? But when other data brokers, based on your same identifiers, let's suppose your name and email address or IP address, have other information about you, let's say, what did you buy? Which all hotels did you book? Where all did you travel to? When they collect all this information, it becomes a complete profile about you, whereas they know more better than you. What decision would you make at this point?

Naomi Brockwell
A known goal of this industry is cross-device tracking. The real data gold is when they link your smart TV usage with your phone, laptop, home automation or IoT devices, browsing habits, social media activity, car, wearables, transaction history, the list goes on. The Vizio lawsuit revealed that the company worked with other companies to combine data sets so that viewing habits be paired with information like a viewer's sex, age, income, marital status, and more.

YouTube/Washington Post
Using ACR and voter databases, campaigns can know which shows persuadable voters watch most, even when the programs have nothing to do with politics.

Naomi Brockwell

Aggregating these databases to build incredibly detailed psychological profiles about us is a trillion-dollar industry because the more someone knows about us, the easier it is to manipulate what we think, how we vote, even whom we trust. There is a tremendous amount of value in being able to influence someone's worldview or choices.

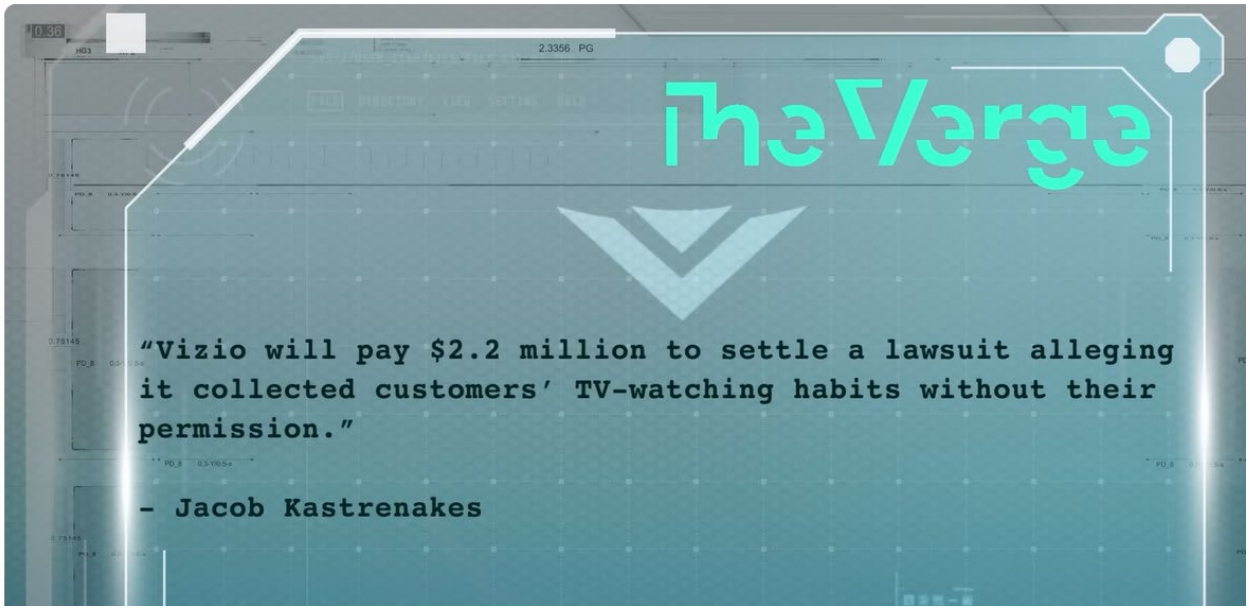
Yash Vekaria
It'll be able to be super creepy and super personalized in terms of the experience that they'll be targeting at you.

Naomi Brockwell
Targeted messages, videos, or content can radically shift opinions, sow division, or incite unrest. Entire government departments all over the world already specialize in this.

Unfortunately, once our data is sold onward, it's out of the manufacturer's control, so there's no way for us to know who has access to it. As David Shoffness, an associate professor in the Calgary College of Computer Sciences, said, “We are increasingly letting these devices in our homes, and we have almost no insight into the data they're collecting who they're sharing that data with and what the privacy implications are.”

So the ways this data could be weaponized are limitless. And indeed, the concept of consent becomes murky when one agreement with a TV maker cascades into countless third parties you've never heard of getting your information. The whole system is murky and opaque by design, and most people have no idea what's going on.

We already mentioned that Vizio was sued for collecting and sharing personal data, but the important part of this case was that they were doing it without ever telling the user or getting their consent.



By the time anyone looked into what was going on, Vizio had already made unknown amounts of money from that data, and the penalty was little more than a slap on the wrist and a mandate to tell users going forward.

By then, the damage was done. This surveillance had already been normalized, and companies were deep into our living rooms and bedrooms. After the lawsuit, Vizio and other smart TV manufacturers kept doing the same thing. The only real change was the addition of vague, buried disclosures hidden in their terms of service.

Yash Vekaria
When you set up a TV, you have to agree to hundreds of different things, and no one really reads these privacy policies or terms on services.

Naomi Brockwell
They're meant to inform users, but are written more as liability insurance and leave users in the dark about what's actually going on.

If they were to explain it to the users in simple terms and say, Hey, you are agreeing to share that information with countless third parties who will profile you on it. I think that most people would say, wait, no, I don't want all my personal viewing habits to be monitored and tracked.

But instead, Smart TV privacy settings are often hard to find, and the terminology is unclear. If you dive into countless submenus, you'll find terms like Live Plus and Viewing Information Services. These terms both refer to ACR, actually. Not that anyone would know. If we're not being told what's actually going on inside the tech that we use, how are we meant to make better choices? Well, researchers, like

those that we spoke to, try to break into this tech themselves to see if they can understand it all. But there are two huge obstacles to this. The first is technical.

Yash Vekaria
There was no public repository for jail-breaking into Samsung, so it just tells me that their safeguards have become more stronger to prevent this kind of thing from happening.

Naomi Brockwell
Companies use a lot of proprietary algorithms and technical barriers that make it near impossible for people to actually reverse engineer their systems.

As a result:

Yash Vekaria
We could not look at the raw data.

Naomi Brockwell
So Yash and his team had to take a lot of guesses about how the surveillance in these smart TVs worked.

Yash Vekaria
If they had ACR in the domain name, we identified them to be servers related to ACR technology. However, this is just a lower bound because we don't know if they're using some other domains for the same purposes. Let's say, samsungads.com.

Naomi Brockwell
It really is a testament to how opaque these systems are, the fact that you have to infer so much.

The second obstacle that researchers face when trying to investigate surveillance, and it's a huge one, is legal. Companies weaponize legislation like the CFAA to silence research. The CFAA stands for the Computer Fraud and Abuse Act. Its intention is to try to protect companies and government entities from bad people, breaking in and exploiting vulnerabilities.

But the thing is, the CFAA doesn't actually have intent written into the law, so it doesn't tell the difference between someone who scrutinizes code in order to do

harm to a business and someone who researches code in order to inform users about how the tech works and whether or not it's spying on them. Companies use the CFAA to silence researchers who expose shady practices and to deter others from doing similar investigations. As a result, researchers are often too scared to publish their findings, not because they've done anything wrong, but because they fear being sued by powerful companies under vague and outdated laws.

They're arbitrarily going after security engineers who are trying to reverse engineer this code. But really, it's by analyzing this code that we understand what these companies are actually doing. It's not fair that they're creating this safe moat around themselves and putting up all these barriers so that consumers never really understand what's going on.

Yash Vekaria
They are kind of protecting themselves, but it is really hurting privacy research that goes into figuring out these things and what exactly these companies are doing and how are they tracking the users.

Naomi Brockwell
We need more researchers looking into this stuff, and we as consumers, need to be allowed to educate ourselves about what's actually going on. The CFAA really needs to change.

So what can we actually do to better protect our privacy if we want to watch TV? First, don't connect your smart TV to the internet. Keep the WiFi on the TV off, and instead watch TV by connecting a laptop or some other device that you trust more.

Yash Vekaria
If you disconnect the smart TV from internet, there will be no ACR traffic, so they will not be able to send any of this information to their servers. But still, this is an OS-integrated mechanism, so they will still be collecting that information.

Naomi Brockwell
It's possible that if you ever connect to the internet in the future, that data might all be sent out in bulk. But presuming that you never connect to the internet again and only use your TV as a dumb monitor through your laptop:

Yash Vekaria
Even if they are collecting the information that never leaves your device.

Naomi Brockwell
Next, you can comb through your settings to find all the different toggles on your device that need to be switched off in order to opt out. Good luck.

Yash Vekaria
By opt out, I mean opt out of everything related to advertising and tracking or anything related to AI.

Naomi Brockwell
This can be a difficult task and likely requires you going to many hidden submenus to find all the settings.

Yash Vekaria
Opting out of all of those things will block all the traffic going to the ACR servers.

Naomi Brockwell
The TV may still collect this data, but it won't be sent off. If you trust that the TV is doing what it says it's doing, and if you can be sure that you didn't miss any settings.

Another solution is you can try to find a device that isn't smart. This is not easy. It's almost impossible to buy a non-smart TV these days. I recently scoured the internet, finally found one and ordered it, and when it arrived, it was a smart TV, and I wrote to complain that none of this connectivity was in the specs, and the seller told me that they didn't have my model in stock, so they upgraded me. I didn't consider adding spyware to my TV an upgrade. You might also consider buying a projector instead of a TV. There are still a few dumb projectors in existence, but even they're getting rare. Or you can look for a dumb monitor, but they only go up to a certain size, and it's nowhere near the average consumer television size these days.

Yash Vekaria
We hope dumb TVs are brought back to the market instead of smart TVs.

Naomi Brockwell
Please. Next, we can be vocal that we value privacy and ask hard questions when we buy electronics.

Yash Vekaria
When you go and buy some device in the market, privacy is not really a factor that people consider. And that's, I think, partly because of lack of awareness.

Naomi Brockwell
So we need to spread the word about what's going on and push companies to make better devices, hold them to higher standards, and tell them that privacy is important to us.

Even just getting this conversation started really goes a long way to moving the needle.

Finally, we can fight back against the CFAA and make sure that researchers are protected.

It's just so important that people with the technical skills are using their talents to really dive into this stuff. I think it helps empower everyone.

One thing that we're doing at the Ludlow Institute is trying to support more researchers with these kinds of investigations. If you are a privacy researcher who likes to reverse engineer things and you're interested in uncovering hidden surveillance in everyday tech, please reach out and apply for a grant, or let us amplify your work.

We want to help educate as many as many people as possible about what's going on.

In summary, smart TVs are a privacy nightmare. As soon as you switch them on, they're gathering and sharing data about what you're doing, including taking continuous snapshots of everything you watch. Out of all the IoT devices, smart TVs are the chattiest, contacting not only the TV maker's servers, but also all kinds of advertisers, analytics companies, and cloud service providers. This data can end up in anyone's hands, including government records. We shouldn't have let faceless companies and governments into our living rooms and bedrooms, and we have a long way to go with improving the situation. But it starts with awareness. It's time to blow the lid off the pervasive surveillance in our lives. We may have gotten to a bad place, but let's make better choices going forward and start spreading the word.