UNCUT-NEWS
INDEPENDENT ANALYSES AND INFORMATION ON GEOPOLITICS, ECONOMICS, HEALTH, TECHNOLOGY

Big Brother is built directly into the screen

- October 13, 2025

Even in standby mode, TVs continue to signal for service. Here's what you can do about it.

By Christina Maas

When European regulators began looking behind the sleek black bezels of modern televisions, they didn't expect to discover a small surveillance operation quietly humming away in the background.

But that's exactly what they found: TVs that behaved less like passive screens and more like digital snitches – with a direct line to an international network of data traders, software providers, streaming services and anyone else willing to pay for a piece of your living room.

It turns out the only thing that's really "off" about your smart TV is the assumption that turning it off does anything.

The investigation

The investigation was launched as part of the GDPR joint project by data protection authorities from the Netherlands, Hungary, Italy and Liechtenstein.

They selected the three best-selling smart TVs on the European market. Less a product test, more a covert operation.

They recorded raw network traffic under normal conditions: during setup, while idle, after 24 hours of being turned off, and during regular use.

The result: Your TV is surprisingly busy for a set that's supposed to only show "Bake Off" repeats.

During installation, over 96% of outgoing data on one model went directly to the operating system vendor.
Another device sent a third of its initial traffic to streaming services. The manufacturers—whose names appear on the box—barely appeared in the data stream.

Third-party domains were listening before the remote control even came out of the plastic wrap.

And it doesn't stop there. Not even when you turn off the TV.

“We found it interesting that even when the device is turned off, connections to streaming services, the manufacturer, and other third parties continue to exist,” the report states – in a tone that suggests the authors would like to scream.

One device forwarded over 98% of its standby traffic to the OS provider.

What is transmitted

The data flowing from these devices reads like the menu of an all-you-can-track buffet:

- Private IP addresses
- Device IDs
- Account IDs
- Advertising identifiers
- Firmware versions
- Settings
- Usage logs
- Timestamp

Exactly what you don't want to silently transmit to a third-party network while watching series.

All of this supports a business model that has less to do with building televisions than with selling the people who watch them.

Manufacturers duck away

The report states: "The consumer (data subject) is confronted with many companies or entities when using their smart TV. All manufacturers studied work with partners."

This friendly language masks a cynical money-making machine where manufacturers make deals, pre-install apps, force content, and monetize every second of your viewing.

In some cases, these apps couldn't be deleted. In others, apps were installed automatically without user notification. Personal data was even shared without even having an account with the provider.

Under the GDPR, the data controller is actually responsible. But the manufacturers act as if they were only distant cousins to your data—not the ones who installed the spyware.

Many shift the responsibility to OS providers or app developers. Some reluctantly sign data processing agreements, which, however, provide little transparency.

The end result is an opaque system in which users are forced to accept complex terms of use from multiple parties – just to be able to watch television at all.

“Across all brands, users encounter situations where they have no realistic option other than to accept comprehensive privacy policies in order to use the device,” the report said.

Watch TV? Only if you give up your privacy.

Fragmented supervision

All of the manufacturers examined are headquartered outside the EEA. This means there is no uniform oversight under the GDPR.
Each national authority must act individually – with “local teeth” against a multinational hydra.

What you can do about it

Here are steps to curb the built-in surveillance device in your living room. It can't be completely prevented—smart TVs are designed to keep listening even when you say "stop." But you can stem the flood of data:

1. Disable tracking and telemetry

Go to Settings → Privacy / Advertising / General / Support.

Disable options such as:

- „Viewing Information“
- „Interest-Based Advertising“
- „Live Plus“
- „Home Promotion“
- „Smart TV Experience“
- „Limit Ad Tracking“

Examples:

- Samsung: Turn off “Viewing Information Services” and “Interest-Based Ads.”
- LG: Turn off “Live Plus,” disable “Home Promotion,” and turn on “Limit Ad Tracking.”

Also turn off diagnostic and usage reports.

2. Turn off the camera and microphone

- Revoke access rights (“Voice Services”, “Microphone Access”).
- Use physical switches if available.
- Cover or push back the camera.
- Disable “Always Listening” and voice control.

3. Do not create a manufacturer account

Skip registration for brand accounts (Samsung, LG).
Avoid additional permissions in apps (e.g. location).

4. Disconnect from the Internet

No internet = no data transfer.

- Turn off Wi-Fi or unplug the LAN cable if not needed.
- Use offline mode, updates manually via USB.

Disadvantage: Streaming and smart features will not work.

5. Set up network blocks

Block tracking at the router level:

- **Pi-hole** for DNS blocking
- Firewall rules for specific IPs
- Guest network for TV with minimal rights
- Router with domain filter

This gives you central control.

6. VPN at the router level

Route TV traffic through a VPN.
This obscures IP and location.

But: Some streaming services block VPNs, and setting them up can be technical.

7. Monitor data traffic

- Check router logs, block new domains.
- Be careful with system services (e.g. updates).
- Think of “digital pest control” – ongoing and laborious, but necessary.

8. Abandon smart functions altogether

The most radical solution: **Buy a “dumb” TV** without internet.
Use streaming sticks or external speakers that are easier to control.

This turns the television back into a pure display, not an informant.

Conclusion

Turning off tracking results in a loss of convenience – voice control, personalization, and recommendations are no longer available.
Some data collection can only be prevented if the device is completely offline.
And manufacturers regularly change their tracking methods – users have to constantly keep up.

This means that anyone who buys a smart TV today is not just getting a display in their living room – but also a permanent data pipeline to third-party companies.

Quelle: Big Brother Comes Built Into the Screen