

Stop the Dataminers

Jerome M. Kutche

2026

- [Introduction: Your House Is Talking Behind Your Back](#)
- [Level 1 — Browser \(Anyone, 5 Minutes\)](#)
- [Level 2 — Router \(Intermediate, an Afternoon\)](#)
- [Level 3 — Dedicated Device \(Advanced, a Weekend Project\)](#)
- [Level 4 — Homelab \(Expert\)](#)
- [Verifying It's Actually Working](#)
- [Troubleshooting Common Problems](#)
- [Frequently Asked Questions](#)
- [Glossary](#)
- [Start Here If You're Overwhelmed](#)
- [Getting Data Already Out There Removed](#)

Introduction: Your House Is Talking Behind Your Back

Your smart TV, router, printer, and thermostat are quietly sending data to manufacturers and data brokers right now. The industry calls it “telemetry.” In plain terms, it’s surveillance — usage patterns, device inventories, viewing habits, and network activity, collected continuously and shared with third parties.

None of this requires you to have done anything wrong, or even anything unusual. It happens by default, out of the box, the moment a device connects to your WiFi. Most of it is buried in a privacy policy nobody reads, phrased in language designed to sound routine rather than alarming: “to improve your experience,” “for product development purposes,” “with select partners.” What that actually means, in most cases, is a steady stream of metadata — what you watch, when you’re home, what other devices are on your network, how you use the product — flowing out to servers you’ll never see, for purposes you were never meaningfully asked to consent to.

This guide walks through four levels of defense, from a five-minute browser fix to a full homelab-grade setup. Pick the level that fits your skills and time. Even Level 1 alone makes a real difference. None of these levels require you to throw out your devices or give up convenience — the goal is visibility and control, not a return to dial-up.

Why This Matters

It’s worth being specific about what’s actually at stake, because “privacy” as a word has been used so often it’s started to feel abstract. Three concrete reasons this is worth an afternoon of your time:

The data compounds. A single data point — one show watched, one device connected — is nearly meaningless on its own. But telemetry isn’t collected once; it’s collected continuously, indefinitely, and correlated across every device in your house and often across other accounts you hold with the same company. A pattern built from months of continuous collection is a genuinely detailed picture of your household’s habits, presence, and schedule — far more than any single

data point would suggest.

You don't control where it goes after collection. Most telemetry doesn't stay with the manufacturer. It's routed to analytics platforms, advertising networks, and data brokers, who aggregate it with data from other sources and resell it. Once your data leaves your network, you have no practical way to know who has it or what they've combined it with.

Blocking it costs you almost nothing. This is the part that makes the effort worth it: unlike a lot of privacy trade-offs, blocking telemetry rarely breaks the actual functionality of a device. Your smart TV still plays video. Your printer still prints. What stops working is the surveillance layer riding alongside the feature you actually wanted — which is exactly the layer that shouldn't have been bundled in without a real choice in the first place.

The Prime Example: Amazon eero

Amazon's eero WiFi system is one of the most aggressive data collectors you can plug into your home network. It continuously transmits device inventory and usage data back to Amazon's servers, and Amazon's own privacy policy openly states this data is shared with third parties.

"ET phoned home once. The eero never hangs up."

This isn't unique to eero — most consumer smart-home gear behaves the same way. Eero is simply one of the most visible and well-documented examples, in part because it sits at the center of the network by design, giving it visibility into every other device you own.

How to Read This Guide

Each level below builds on the one before it, but they're independent — you can stop at any level and still have made real progress. A rough guide to picking your starting point:

- **Just want the quick win today?** Start at Level 1.
- **Want every device on your network covered, not just your browser?** Go to Level 2.
- **Want a real-time dashboard of what's being blocked, and full control over the block list?** Go to Level 3.
- **Running a homelab already, or want the most thorough setup possible?** Go to Level 4.

Level 1 — Browser (Anyone, 5 Minutes)

The easiest and fastest win. Covers web browsing only, but it's where most casual tracking happens.

- Install **uBlock Origin** in Firefox or Brave (free, open source ad/tracker blocker) — ublockorigin.com
- On Chrome or Edge, install **uBlock Origin Lite** instead. Google's Manifest V3 change ended support for the full version there; the Lite version is free but weaker (less cosmetic filtering, fewer custom rules), so pair it with encrypted DNS.
- Add **NextDNS** or **ControlD** encrypted DNS for more coverage — nextdns.io

This stops a large share of browser-based tracking immediately, with no technical setup beyond installing an extension and changing a DNS setting.

What This Actually Blocks

The full uBlock Origin works by intercepting requests your browser makes to known ad and tracking domains before they load — meaning the tracking script never runs at all, rather than running and just being visually hidden. It's meaningfully different from a basic ad blocker in that it also blocks known analytics and fingerprinting scripts, not just banner ads.

Switching your DNS to an encrypted, filtering resolver like NextDNS adds a second layer: even requests uBlock Origin doesn't catch (because they're not initiated by a script it recognizes) get blocked at the DNS level before your device can even look up the tracking server's address.

What This Doesn't Cover

This level only protects the browser it's installed in, and only on the device it's installed on. Your smart TV, your phone's other apps, your game console, your printer — none of that traffic goes through your browser, so none of it is touched by Level 1. That's exactly the gap Level 2 closes.

Level 2 — Router (Intermediate, an Afternoon)

Filtering at the router covers every device on your network — phones, laptops, smart TVs, game consoles — without installing anything on each device individually.

- Point your router's DNS settings to a filtering service (NextDNS, ControlD, or Quad9) instead of your ISP's default or a generic public resolver
- If your router supports it, flash **DD-WRT** firmware for full router-level control over DNS, firewall rules, and traffic shaping — dd-wrt.com

This is the first level that protects devices that can't run their own ad blocker — smart TVs, streaming boxes, IoT gadgets.

Setting the DNS at the Router

Most consumer routers let you set a custom DNS server under WAN or Internet settings, separate from what your ISP hands out automatically. Once set there, every device that connects to your network — including ones you'll never think to configure individually — inherits that DNS setting automatically via DHCP. This single setting is the highest-leverage change in this entire guide relative to the effort required: one change, applied once, covers the whole house.

Why DD-WRT (or Similar Third-Party Firmware) Matters

Stock router firmware is usually locked down to a handful of consumer-friendly settings and, ironically, is itself sometimes a telemetry source back to the router manufacturer. Third-party firmware like DD-WRT (or alternatives like OpenWrt) replaces that stock software entirely, giving you real firewall rule control, VPN support, and traffic visibility that stock firmware simply doesn't expose. This is optional — DNS redirection alone at Level 2 already provides meaningful coverage — but it's the natural next step if you want real control rather than just filtering.

A Word of Caution

Flashing third-party firmware carries a real risk of “bricking” (permanently disabling) a router if interrupted or done with the wrong firmware image for your exact model. Confirm your router model is explicitly supported before attempting this, follow the specific instructions for that model rather than generic ones, and don't attempt it on a router you can't afford to be without for a day if something goes wrong.

Level 3 — Dedicated Device (Advanced, a Weekend Project)

Run a dedicated DNS filtering server on your network. This gives you a real-time dashboard, custom block lists, and far more control than router-level DNS redirection alone.

- **Pi-hole** or **AdGuard Home**, run on a Raspberry Pi or spare PC — pi-hole.net, adguard.com/adguard-home.html
- Point your router's DHCP DNS setting to this device as the primary DNS for the whole network

Important: check for a DNS bypass. Many routers hand out a secondary DNS server (like 1.1.1.1) alongside your filter. If devices can fall back to that secondary when your filter is slow, they bypass it entirely. Set a security-focused resolver like Quad9 (9.9.9.9) as the fallback instead of an unfiltered one — it still blocks known-malicious domains if your primary filter goes down.

Either Pi-hole or AdGuard Home alone, properly configured, blocks a meaningful share of telemetry and ad traffic network-wide.

Pi-hole vs. AdGuard Home

Both tools do fundamentally the same job — DNS-level filtering with a dashboard — but they differ in a few practical ways worth knowing before you pick one:

Pi-hole has the larger, longer-established community and the most third-party guides and blocklists built specifically for it. Its interface leans toward raw data: query logs, top blocked domains, per-client stats.

AdGuard Home ships with a slightly more polished interface out of the box, includes built-in parental control and safe-search enforcement options, and — notably — supports encrypted DNS (DNS-over-HTTPS/TLS) both for its own upstream queries and for serving encrypted DNS to your own devices, which Pi-hole requires additional configuration to match.

Neither is a wrong choice. If you're already comfortable in a terminal and want the most third-party documentation available, Pi-hole's community size is an asset. If you want native encrypted DNS support and a slightly more modern interface with less initial tinkering, AdGuard Home is the more turnkey option.

Setting Up the Dashboard for Real Visibility

Once running, don't just set it and forget it — the dashboard is where the actual value of this level shows up. Spend a little time in the query log after the first few days of normal use. You'll typically see:

- A running percentage of total DNS queries being blocked
- The specific domains generating the most blocked requests
- Which devices on your network are the most persistent about phoning home

That last one is often the most eye-opening part of Level 3: seeing, by device name, exactly which of your gadgets is making the most tracking attempts per hour.

Preventing the DNS Bypass

This deserves repeating because it's the single most common way a Level 3 setup silently stops working: if your router is configured to hand out a secondary DNS server alongside your Pi-hole or AdGuard Home address, any device (or any app on a device) that's written to try the secondary DNS server when the primary is slow to respond will bypass your filtering entirely, with no error and no indication anything changed. Check your router's DHCP settings specifically for a secondary/backup DNS field, and either leave it blank or point it to a security-focused (not just "any public") resolver like Quad9, so a bypass at least still blocks known-malicious domains even if it skips your custom filtering.

Level 4 — Homelab (Expert)

A real, working setup — built through hands-on technical collaboration with Claude AI (Anthropic) — not theory.

Architecture

- **AdGuard Home** running as a dedicated VM on a Proxmox server (not just a Raspberry Pi — full virtualized infrastructure)
- A router firewall (e.g. MikroTik/RouterOS) handling IP-level blocking as a second layer behind DNS filtering
- IoT devices isolated on a separate VLAN, away from trusted PCs and phones

This layered approach matters because DNS filtering alone has a blind spot: any device hardcoded to use a specific IP address instead of a domain name skips DNS entirely, and therefore skips DNS-based filtering entirely too. A second layer — IP-level blocking at the router firewall — catches that traffic even when DNS filtering can't see it coming.

Why VLAN Isolation Matters

Putting IoT devices — smart TVs, streaming boxes, smart plugs, voice assistants — on their own VLAN, separate from the VLAN your trusted computers and phones use, adds a layer of protection that has nothing to do with DNS filtering at all. If one of those devices is ever compromised, or if its "telemetry" turns out to include something closer to active scanning of your local network, VLAN isolation prevents it from ever reaching your trusted devices in the first place. This is defense in depth: DNS filtering blocks the known trackers, IP-level firewall rules catch what DNS filtering

misses, and VLAN isolation limits the blast radius of anything that gets through both.

Blocklists in Active Use

Blocklist	Purpose
HaGeZi Multi Pro	All-around telemetry and ad blocking
OISD Big	Broad ad and telemetry coverage
WindowsSpyBlocker	Microsoft/Windows telemetry domains
Perflyst Smart-TV Blocklist	Smart TV telemetry (Samsung, LG, Roku, Hisense, etc.)
HaGeZi Samsung Tracker	Samsung-specific tracking domains
HaGeZi Windows/Office Tracker	Microsoft Office telemetry
HaGeZi Threat Intelligence Feeds	Known malicious/tracking infrastructure
Phishing URL Blocklist	Phishing protection
Stalkerware Indicators List	Blocks known stalkerware command-and-control domains

A few notes on managing multiple blocklists at once: overlapping lists are normal and not wasteful — different maintainers catch different domains at different speeds, so redundancy actually improves coverage. Update frequency matters more than list count; a handful of actively-maintained lists outperforms a large pile of stale ones. Most DNS filtering tools show you, per list, how many domains it’s currently blocking and how recently it was updated — periodically check for lists that have gone stale (no update in 6+ months) and either find a maintained replacement or accept it’s now mostly dead weight.

Custom Rules

Manufacturer-specific ACR (Automatic Content Recognition) vendors often slip past general blocklists. Watch your query log for unexpected outbound domains from smart TVs and add custom rules as needed. Example — blocking a Hisense third-party ACR vendor:

```
||vidonme.cn^
```

ACR is worth understanding specifically because it’s one of the more invasive forms of smart TV telemetry: it works by taking periodic snapshots or audio fingerprints of whatever is currently displayed on screen — including content from an HDMI-connected device, not just the TV’s own apps — and matching that against a database to identify exactly what you’re watching, when, for how long, and often on which specific device. It’s usually enabled by default and buried several menus deep to disable through the TV’s own settings, which is exactly why blocking its outbound domains at the DNS level is more reliable than hunting for a toggle in the TV’s UI.

Mobile Coverage

DNS blocking at the router only catches WiFi traffic. Phones can also be covered over cellular (4G/5G) using a local VPN-based blocker (AdGuard or Blokada app), so telemetry is blocked even off the home network.

This closes a gap that’s easy to overlook: a phone that’s perfectly protected on home WiFi is completely unprotected the moment it steps outside on cellular data, unless a separate mobile-specific solution is running. A local VPN-based blocker works differently from a traditional VPN — instead of routing your traffic through a remote server, it creates a local VPN tunnel on the device itself purely so the app can inspect and filter DNS requests before they leave the phone, without your actual browsing traffic ever leaving your device through a third party.

Results

A well-tuned setup like this blocks 25-30% of ALL network traffic — most of it telemetry you never knew existed. That’s measured directly from the AdGuard Home dashboard, not a marketing number.

That figure is worth sitting with for a moment: nearly a third of everything your network was sending out, before any filtering, was going somewhere other than where you actually intended it to go.

PC-Level Supplement (Windows)

DNS blocking can't reach telemetry baked into the OS itself (registry entries, hosts file, background services). For full coverage on Windows PCs, run all three together:

- **Spybot Anti-Beacon** — handles registry/hosts file telemetry
- **Group Policy** — set Windows telemetry to Security or Basic
- **Disable the DiagTrack service** (Connected User Experiences and Telemetry)

DNS + firewall + VLAN isolation + Anti-Beacon + Group Policy, layered together, covers every level a typical home network can be tracked at once: DNS, registry, hosts file, services, and cellular.

Verifying It's Actually Working

Blocking telemetry is one thing; confirming it's actually happening is another, and it's a step worth taking regardless of which level you stop at.

At Level 1 or 2: browse to a known ad/tracker-heavy site and check your browser's network inspector (or your blocker's own badge count) for blocked requests. A quick, low-effort sanity check.

At Level 3 or 4: your DNS filter's dashboard is the real test. Watch the query log live while a smart TV is powered on and idle — you should see periodic outbound query attempts to known telemetry domains getting blocked, even with nothing actively "in use" on the TV. That's the ambient telemetry traffic this whole guide is aimed at.

A useful habit: check the dashboard's block percentage weekly for the first month after setup, then monthly after that. A sudden drop in block percentage with no configuration change is usually a sign something is bypassing your filter — worth investigating rather than ignoring.

Troubleshooting Common Problems

"A smart TV app / streaming service stopped working after I set up filtering." Some legitimate app functionality is occasionally bundled with the same domains used for telemetry, especially with poorly-separated CDN infrastructure. Check your filter's query log for what was blocked right before the failure, and add a specific allow-list exception for that one domain rather than disabling the whole blocklist.

"My block percentage dropped to near zero overnight." Almost always a DNS bypass — check your router's secondary/fallback DNS setting (see the Level 3 section above), and confirm no device has been manually configured with its own DNS server that skips your router's DHCP-assigned setting entirely (this is common on some Android and Google/Chromecast devices, which can silently use their own hardcoded DNS).

"A blocklist I added didn't seem to change anything." Confirm the list actually loaded and updated — most tools show a domain count and last-updated timestamp per list. A list that failed to download silently sits at zero blocked domains and does nothing.

"I flashed DD-WRT and now my router won't boot." This is the risk mentioned in the Level 2 section. Recovery depends entirely on the specific router model — consult that model's specific DD-WRT recovery documentation before attempting anything further, since generic recovery steps can make things worse on some hardware.

Frequently Asked Questions

Will this slow down my internet? DNS-level filtering adds a negligible amount of latency — typically single-digit milliseconds — because it's just an extra lookup step, not a traffic inspection bottleneck. If anything, blocking ad and tracking scripts before they load often makes pages feel faster, since your device isn't waiting on dozens of third-party trackers to finish loading in the background.

Do I need to do all four levels? No. Each level stands on its own and provides real protection. Most households get

the large majority of the benefit from Level 2 or Level 3 alone; Level 4 is for people who already run other home infrastructure and want the most complete, layered coverage.

Will my smart TV / voice assistant stop working? In the large majority of cases, no — blocking telemetry domains doesn't touch the domains actually required for core functionality (streaming video, responding to voice commands). Occasionally a specific feature is tied to a domain that's also used for telemetry, in which case the Troubleshooting section above covers how to add a targeted exception.

Is this legal? Yes. You're not intercepting or modifying anyone else's traffic — you're configuring how your own network resolves domain names and what your own devices are allowed to connect to. This is the same category of control as an ad blocker or a firewall rule, both long-standing, uncontroversial practices.

What about devices I can't put behind a VLAN or DNS filter at all — like a cellular-only device? Those are genuinely harder to cover, since they bypass your home network's DNS and firewall entirely by using the cellular carrier's own DNS. The mobile-specific local VPN blocker described in the Level 4 Mobile Coverage section is currently the most practical option for that case.

Glossary

DNS (Domain Name System): the system that translates human-readable domain names (like example.com) into the numeric IP addresses computers actually use to connect. DNS-level filtering works by refusing to resolve known tracking/ad domains, which prevents the connection before it starts.

Telemetry: data automatically collected by a device or app about its own usage and sent back to the manufacturer or a third party, typically without an active, specific choice by the user each time it happens.

ACR (Automatic Content Recognition): a smart TV feature that identifies exactly what's being displayed on screen — including content from external devices — by fingerprinting audio or video snapshots, usually for advertising and analytics purposes.

VLAN (Virtual Local Area Network): a way of logically separating devices on the same physical network into isolated groups, so devices on one VLAN can't directly reach devices on another unless explicitly allowed.

Blocklist: a maintained list of domains known to serve ads, trackers, telemetry, or malicious content, used by a DNS filter to decide what to block.

DNS-over-HTTPS / DNS-over-TLS (DoH / DoT): methods of encrypting DNS queries so they can't be read or tampered with in transit, as opposed to traditional DNS, which is sent in plain text.

Start Here If You're Overwhelmed

- Install uBlock Origin (Firefox/Brave) or uBlock Origin Lite (Chrome/Edge) — today
- Switch to NextDNS on your router — this week
- Set up Pi-hole or AdGuard Home — when you're ready to go further

You don't have to jump straight to Level 4. Each level is a real improvement on its own, and you can build up over time.

Built through real technical collaboration with Claude AI (Anthropic) — documenting an active, working setup, not theory. Every blocklist, custom rule, and configuration note in this guide is pulled directly from a live network.

Getting Data Already Out There Removed

Everything above stops *new* telemetry from leaving your network. It does nothing about data that has already been collected and published by people-search and data broker sites — Spokeo, WhitePages, BeenVerified, MyLife, and dozens more. These sites collect and sell your name, address, phone numbers, and relatives, usually without you ever agreeing to it.

Know Your Rights First

Most states now have a consumer data protection law requiring data controllers to honor deletion requests within a set window — commonly 45 days. Check your own state’s law and cite the correct one before sending anything.

Where to Send Requests

- **Spokeo:** privacy@spokeo.com — also offers a Universal Opt-Out option.
- **WhitePages:** whitepages.com/suppression_requests
- **BeenVerified:** beenverified.com/app/optout/search
- **MyLife:** privacy@mylife.com
- **FindUsLocal / AllPeople:** Check the listing page footer for an “opt-out” or “remove” link.
- **Others:** Search your name + city/state, and site-scope search major brokers at once to find more.

Removal Request Template

Fill in the brackets and send to the broker’s privacy contact:

Subject: Data Deletion Request – [Your State] Consumer Data Protection Law

To the [Broker Name] Privacy Team,

Pursuant to [Your State's Law + Citation], I am requesting the deletion of all personal data associated with me from your database, search index, and any affiliated third-party networks.

Subject Information:

Full Name: [Your Full Name]

Address: [Your Address]

Email: [Your Email]

Please confirm deletion in writing within [45 days / your state's required window].

Sincerely,
[Your Name]

If you don’t get a response within your state’s required window, send a firmer second notice citing your state Attorney General’s office and the FTC as next steps.