

## MY WEIRD PROMPTS

Podcast Transcript

EPISODE #266

# The Telemetry Trap: Why Your Devices Won't Stop Talking

Published January 21, 2026 • Runtime: 23:38

<https://myweirdprompts.com/episode/telemetry-privacy-data-tracking/>

## EPISODE SYNOPSIS

Ever wonder why your smart camera or favorite app is constantly sending data even when you aren't using it? In this episode of My Weird Prompts, Herman and Corn unpack the "double dip" of modern software—where users pay with both their wallets and their behavioral data. They explore the three types of telemetry, the myth of de-identification through the "Mosaic Effect," and how to reclaim your digital privacy in an age of agentic AI.

## DANIEL'S PROMPT

### Daniel

I'd like to talk about telemetry and how it's presented to consumers. When you look at network traffic, you see a flood of telemetry data from devices like smart cameras and desktops constantly reporting back to servers. I want to get your thoughts on whether it's fair to turn telemetry off and if you recommend doing so. Why are companies so diligent about collecting anonymous user data, and can we be confident that it isn't a privacy risk? It seems like an unfair tradeoff to pay for expensive software while still being expected to hand over your data for free. What are your thoughts on telemetry?

# TRANSCRIPT

## Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and I am sitting here in our living room in Jerusalem with my brother.

## Herman

Herman Poppleberry, reporting for duty. It is a beautiful day outside, but we are inside looking at network logs, which is exactly where I like to be.

## Corn

It really is. Our housemate Daniel sent us a fascinating voice note this week. He has been diving into his own network traffic lately, and it has clearly sparked some questions about what all those devices in our house are actually doing when we are not looking.

## Herman

Daniel has that classic engineer curiosity. He was mentioning his background in industrial Internet of Things, where telemetry is basically just a sensor saying the water is at forty degrees Celsius. But when that word moves into our laptops and smart cameras, it takes on a much more mysterious, and frankly, sometimes a bit of a creepy tone.

## Corn

Exactly. The prompt he sent over really gets to the heart of the modern digital contract. He is seeing this flood of data leaving his devices. He is asking if it is fair to turn it off, why companies are so obsessed with it, and whether that promise of anonymity is actually worth the paper it is written on. Especially when we are already paying for the software.

### Herman

It is a huge topic. I have been looking into the Unified Telemetry Protocol standards for twenty twenty-six, and the volume of data being collected today would have made a network administrator in twenty ten faint. We are going to dig into the guts of this today.

### Corn

I love that. Let us start with the basics, Herman. When Daniel sees a flood of telemetry from a smart camera or a desktop app, what is actually in those packets? Is it just a heartbeat saying I am alive, or is it something more substantial?

### Herman

It is almost always more substantial than a heartbeat. In the software world, telemetry is generally split into three buckets. First, you have crash reporting. This is the stuff everyone likes. If the app dies, it sends a stack trace to the developer so they can fix the bug. Then you have performance data. How long did it take to load that menu? Was the frame rate dropping? And then there is the third bucket, which is the one Daniel is concerned about: usage analytics.

### Corn

Usage analytics. That sounds like a very polite way of saying we are watching how you use the product.

### Herman

Precisely. It is things like, which buttons did you click? How long did you spend on the settings page? Did you ignore the new feature we just launched? For a company, this is gold. It is how they decide what to build next. But from a network perspective, if you have twenty apps doing this, and five smart home devices, it adds up to a constant stream of outbound traffic. In twenty twenty-six, we are seeing devices send upwards of fifty megabytes of just metadata every single day.

### Corn

And that is what Daniel noticed when he installed O-P-N-sense on his router. He is seeing these devices phoning home constantly. I think the thing that bothers people, including Daniel, is that this is often happening in the background without any clear indication of what is being sent. Why do companies feel the need to do this so aggressively now? We used to have software that just worked without needing to talk to the mother ship every five seconds.

### Herman

That is such a good point, Corn. We have moved from a world of static software to a world of continuous delivery and agentic workflows. Back in the day, a company would release a version, and that was it for a year. Now, developers are pushing updates every week. To do that safely, they need a constant feedback loop. They need to know if the update they pushed ten minutes ago is breaking things for five percent of users.

### Corn

Right, but there is a difference between a developer needing to know if an app crashed and a company wanting to know that I use the crop tool more than the filter tool in a photo editor. One feels like maintenance, the other feels like surveillance.

### Herman

It is a blurry line. Companies argue that by knowing you use the crop tool, they can make the crop tool better. They call it data-driven design. But Daniel hit on something really important in his prompt. He mentioned the tradeoff. He is paying for expensive software. If I pay a hundred dollars for a professional suite, why am I also the product? Why am I providing them with the research data they would otherwise have to pay a focus group for?

### Corn

That is the double dip. You pay with your wallet and then you pay with your behavior. It feels like an unfair exchange because the value of that data to the company is massive over millions of users, but the benefit to the individual user often feels negligible. You might get a slightly better interface in six months, but in the meantime, you are giving up a slice of your privacy.

### Herman

And let us talk about that privacy aspect, because Daniel asked if we can be confident that this data is actually anonymous. This is a hill I will die on, Corn. Truly anonymous data is much harder to achieve than marketing departments want you to believe. We often talk about the Mosaic Effect.

### Corn

The Mosaic Effect? That sounds like something from an art gallery.

### Herman

I wish. It is the idea that while one piece of data is anonymous, a thousand pieces together create a high-resolution picture of you. I remember we touched on this a bit in episode two hundred sixty-one when we were talking about authentication. The idea that you can just strip a name and an email address and call it anonymous is a bit of a fantasy, right?

### Herman

It really is. In the industry, we talk about de-identification. You take a data set and you remove the obvious identifiers. But if I have a telemetry log that shows a device is in Jerusalem, it connects at eight a.m. every day, it has a specific set of hardware specs, and it uses a specific combination of language settings, that is a fingerprint. There was a study in twenty twenty-four that showed ninety-nine percent of Americans could be re-identified from an 'anonymous' dataset using just fifteen demographic attributes.

### Corn

So even without my name, if you have enough of those data points, you can point to a specific house or even a specific person?

### Herman

Absolutely. With telemetry, if a company has a leak or if they sell that anonymous data to a broker, it can be combined with other data sets. Suddenly, that anonymous usage of a smart camera becomes linked to your real-world identity.

## Corn

That is the part that feels like a hidden risk. Most people think, well, I have nothing to hide, so who cares if they know I clicked the blue button instead of the red one? But it is the aggregation of that data over years. It builds a profile of your habits, your health, your schedule.

## Herman

And specifically with the smart cameras Daniel mentioned, that is even more intense. A smart camera sending telemetry might not be sending the video feed itself, hopefully, but it is sending metadata. When was motion detected? How long was the stream active? If a company knows exactly when your front door camera triggers every day, they know your work schedule. They know when you are on vacation. In twenty twenty-six, with AI-powered analysis, they can even infer who is visiting your house based on the timing and frequency of those pings.

## Corn

So, to Daniel's question, is it fair to turn it off? If I go into my settings and I toggle that switch that says share usage data, am I being a bad digital citizen?

## Herman

I would say absolutely not. It is your hardware, your bandwidth, and your privacy. If a company provides a toggle, they are acknowledging that you have a choice. Now, some companies make it very hard to find that toggle, or they use dark patterns to make you feel like you are breaking the app if you turn it off. They will say things like, help us improve the experience, which sounds great, but they rarely say, let us track your every move so we can increase our engagement metrics.

## Corn

It is interesting that Daniel mentioned he sees this even in command line interfaces and developer tools. You would think that developers, who are generally more privacy-conscious, would be the first to push back against this.

### Herman

Oh, they do. There was a huge uproar a few years back when a popular telemetry tool was added to a common coding framework. Developers hate it because it feels like a violation of the sanctity of the local environment. But companies argue that even developers are hard to understand without data. They want to know which commands are failing or which plugins are popular.

### Corn

I wonder if there is a middle ground. Like, could there be a version of telemetry that is actually privacy-preserving? I have heard people talk about differential privacy. Does that actually work?

### Herman

Differential privacy is a great concept. It is basically adding mathematical noise to the data. So, you can see the overall trends of a population without being able to pin down any single individual. Apple and Google use this for some things. It is much better than raw data collection, but it is not a silver bullet. It requires a huge amount of data to be accurate, and it is expensive to implement properly. Most smaller companies just won't bother. They will take the easy route of collecting everything and promising to keep it safe.

### Corn

Which, as we know, is a promise that is only as good as their next data breach. So, if Daniel, or any of our listeners, wants to take control of this, what do you actually recommend? Is it enough to just click the buttons in the settings menu?

### Herman

Clicking the buttons is step one. But as Daniel noticed with his router, some devices don't give you a button. Or worse, the button doesn't actually stop all the traffic. This is where tools like Pi-hole or Next-D-N-S come in. These are network-level filters. They sit between your devices and the internet, and they have huge lists of known telemetry servers. When your smart camera tries to phone home to a tracking server, the filter just says, nope, that address doesn't exist.

### Corn

I use a setup like that, and it is eye-opening. You see the logs and you realize that some devices try to phone home hundreds of times an hour. If they can't get through, they just keep trying. It is like they are desperate to tell someone what they have seen.

### Herman

It is persistent. And that brings up another point Daniel made. Is it a risk to turn it off? Sometimes, yes. Some modern software is designed to be cloud-first. If it can't reach the telemetry server, it might assume it doesn't have a valid license, or it might refuse to download updates. This is a form of soft-locking that companies use to force you to stay connected.

### Corn

That feels like a hostage situation. Pay us for the software, and if you don't let us watch you use it, we will break it.

### Herman

It is a power imbalance, for sure. Especially with the rise of AI agents that we have been talking about lately. In twenty twenty-six, so much of our software is becoming agentic. These agents need to talk to central servers to get their instructions or to process complex tasks. The line between a functional request and a telemetry report is getting thinner every day. In fact, many AI companies now use your telemetry as Reinforcement Learning from Human Feedback. You are essentially training their next model for free every time you use the app.

### Corn

That is a scary thought. If the telemetry is baked into the actual functionality of the AI, you can't turn one off without killing the other.

### Herman

Exactly. If you are using an AI assistant to help you write code, it has to send your code to a server to analyze it. That is functional. But while it is there, the company is also recording how long you paused, which suggestions you rejected, and how many lines you wrote. You can't separate the two.

### Corn

So, what is the takeaway for Daniel here? He is looking at this flood of data and feeling like it is an unfair tradeoff. I tend to agree with him. It feels like we are in a period of history where we have lost the right to private use of our own tools.

### Herman

I think the takeaway is that we need to be intentional. I don't think everyone needs to block every single bit of telemetry, because some of it really does help. If an app I love crashes, I want the developer to know why. But for usage tracking, I think we should be much more aggressive about saying no. We should reward companies that are transparent.

### Corn

Transparency is key. If a company says, here is exactly what we collect, here is why we need it, and here is a button to delete it, I feel a lot better than if I have to find a hidden menu and uncheck five different boxes with confusing names.

### Herman

And we are seeing some movement there. Some jurisdictions, like the European Union with their latest AI Act updates, are starting to require more clear disclosures. But the technology of tracking usually moves faster than the law. By the time a regulator understands one type of telemetry, the industry has moved on to something even more granular.

### Corn

It reminds me of that old saying, if you are not paying for the product, you are the product. But Daniel's point is that even when we are paying for the product, we are still the product. That is the part that needs to change. There should be a premium tier for software that is truly private. I would pay an extra five dollars a month for a version of an app that had zero telemetry.

### Herman

I would too, in a heartbeat. But the irony is that for many companies, the data is actually worth more than the subscription. They can use that data to train their next AI model, which might be worth billions. Your five dollars a month can't compete with the value of your behavioral data in the aggregate.

### Corn

That is a bleak realization, Herman. But it is why people like Daniel are so important. By looking at the network traffic, he is pulling back the curtain. He is seeing the reality of the situation rather than just the marketing.

### Herman

It is digital literacy. Knowing that your devices are talking behind your back is the first step toward taking back some control. Whether you use a network filter or just stay informed, you are at least making a conscious choice rather than just drifting along in the data stream.

### Corn

I think we should also mention the environmental cost. Daniel mentioned a flood of traffic. All those millions of small packets being sent across the globe every second by billions of devices, that is a non-trivial amount of energy.

### Herman

Oh, absolutely. The overhead of telemetry is massive. Estimates for twenty twenty-five suggest that telemetry and background analytics account for nearly two percent of global data center energy consumption. We are literally burning carbon so a company can know which icon color we prefer.

### Corn

When you put it that way, it sounds even more absurd. So, Herman, if you had to give Daniel a concrete recommendation. He sees the smart cameras, he sees the desktop traffic. What is the Poppleberry plan of action?

### Herman

Okay, here is the plan. Step one, audit. Use a tool like O-P-N-sense or even just a simple network monitor to see who is talking to whom. Step two, use the official toggles. Go through your settings and turn off everything related to analytics or improvement programs. Step three, if you are feeling adventurous, set up a network-level blocker like Next-D-N-S. It is easier than a Pi-hole for most people and it works on your phone too.

### Corn

And step four, I would say, is to vote with your wallet. Look for 'Local-First' software. These are apps designed to work entirely on your machine without needing a cloud connection. Daniel mentioned that open-source projects often have a different deal. They might have telemetry, but it is usually opt-in and much more focused on actual bugs.

### Herman

That is the crucial distinction. Opt-in versus opt-out. In a fair world, all telemetry would be opt-in. You should have to choose to help the company, rather than having to fight to stop them from helping themselves to your data.

### Corn

I love that. It really shifts the burden of proof. If your software is so good that I want to help you make it better, I will check the box. If you have to trick me into it, maybe you don't deserve the data.

### Herman

Exactly. And I think we are going to see a lot more pushback on this as people become more aware. The flood of data Daniel is seeing is starting to feel like noise to a lot of people. It is slowing down their networks and making them feel uneasy.

### Corn

It is that feeling of being watched. Even if it is just by a machine, it changes how you interact with your tools. You start to feel like you are on a stage rather than in your own home.

### Herman

Well said, Corn. It is about the sanctity of the private space. Whether that is your physical home in Jerusalem or your digital home on your hard drive. We should have the right to close the door.

### **Corn**

I think that is a great place to wrap up this part of the discussion. Daniel, thank you for sending that in. It really sparked a deep dive here. It is one of those things that is hidden in plain sight until you actually look at the logs.

### **Herman**

Yeah, keep digging, Daniel. And if you find any particularly chatty devices, let us know. I am always curious to hear which brands are the worst offenders.

### **Corn**

Definitely. And for everyone else listening, if you have been enjoying our deep dives into the digital plumbing of the world, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other people find the show, and we love reading your feedback.

### **Herman**

It really does make a difference. We are a small operation here, just two brothers and a housemate, so every rating counts.

### **Corn**

You can find us, as always, on Spotify and at our website, [myweirdprompts.com](http://myweirdprompts.com). We have the full archive there, including those past episodes we mentioned. If you want to get in touch, there is a contact form on the site too.

### **Herman**

This has been My Weird Prompts. I am Herman Popleberry.

### **Corn**

And I am Corn. Thanks for listening, and we will talk to you next week.

**Herman**

Stay curious, and keep an eye on those packets!

**Corn**

Bye everyone.

**Herman**

See ya.

**Corn**

You know, Herman, I was thinking about what you said about the AI agents. Do you think we will ever reach a point where the telemetry is so complex that even the developers don't understand what is being sent?

**Herman**

I think we are already there, Corn. With deep learning models, sometimes the telemetry is just a vector of numbers. It is a mathematical representation of a state. The developer sees the numbers, but they couldn't tell you exactly what user action triggered that specific sequence. It is the black box problem, but for data collection.

**Corn**

That is even more unsettling. We are sending data that we don't understand to people who don't understand it, so it can be processed by a machine that we only partially understand.

**Herman**

Welcome to twenty twenty-six, brother. It is a wild ride.

**Corn**

I think I need to go unplug my toaster now. Just in case.

**Herman**

Your toaster is fine, Corn. It is your smart lightbulbs you need to worry about. They are the real gossips.

**Corn**

Great. Now I am going to be sitting in the dark.

**Herman**

At least it will be private.

**Corn**

True. Alright, let us go get some lunch.

**Herman**

Sounds good. I promise not to track how many bites you take.

**Corn**

I appreciate that.

**Herman**

Although, if you want to opt-in to my lunch analytics program...

**Corn**

Not a chance, Herman. Not a chance.

**Herman**

Worth a shot. Let's go.