

MY WEIRD PROMPTS

Podcast Transcript

EPISODE #374

The Walls Have Eyes: The Reality of Hidden Travel Cameras

Published January 30, 2026 • Runtime: 28:29

<https://myweirdprompts.com/episode/hidden-camera-travel-privacy/>

EPISODE SYNOPSIS

In this milestone 365th episode of My Weird Prompts, Corn and Herman dive into the unsettling world of hidden surveillance in short-term rentals and hotels. Inspired by a listener's trip to Israeli "spy shops," the brothers explore how \$30 devices are changing the privacy landscape and why Airbnb was forced to ban indoor cameras entirely. They break down the technology used by both voyeurs and professional bug-sweepers, offering practical tips for travelers to reclaim their peace of mind.

DANIEL'S PROMPT

Daniel

For those of us who travel internationally, do we need to be worried about hidden cameras in our Airbnbs and hotels? Is that really a credible threat? And for these professional bug-sweeping services, who is actually ordering this kind of service and where does the demand come from?

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. We are hitting a pretty big milestone today, this is episode three hundred sixty-five. That is a full year of episodes if we were doing this daily, but since we are weekly, it represents a whole lot of deep dives and rabbit holes we have explored together. I am Corn, and I am joined as always by my brother.

Herman

Herman Poppleberry, at your service. Three hundred sixty-five episodes, Corn. That is a lot of talking. I feel like we have covered everything from military probes to the geometry of secrets, but today's prompt brings us right back into the home, or at least, the homes we stay in when we travel.

Corn

Exactly. Our housemate Daniel sent us a fascinating audio clip this week. He was actually out looking for a new digital voice recorder, a Sony model to replace one he has had for over a decade. In the process of searching for it here in Israel, he ended up down a rabbit hole of spy shops. We are talking about websites like spy dot org dot i-I or Doctor Spy.

Herman

I love those names. It is so on the nose. It is like something out of a low-budget detective novel.

Corn

It really is. But Daniel noticed something a bit more unsettling than just voice recorders. These shops were selling hidden cameras disguised as everyday objects, things like Jewish skullcaps, religious mezuzahs, and even standard Israeli power plugs. It got him thinking about the reality of international travel. Do we actually need to worry about hidden cameras in our Air-B-N-Bs and hotels? Is the threat credible, or is it just marketing for these spy shops? And who on earth is paying for professional bug-sweeping services?

Herman

That is such a great set of questions. It touches on that intersection of high-end technology, basic human privacy, and the creeping feeling of being watched that seems to be a hallmark of life in two thousand twenty-six.

Corn

So let's start with the credibility of the threat. Herman, you have been looking into the data on this. When we hear these horror stories about someone finding a camera in a smoke detector in their vacation rental, is that a one-in-a-million freak occurrence, or is it a systemic issue?

Herman

It is somewhere in the middle, but the trend line is what is really interesting. If you look at the last few years, the accessibility of this technology has plummeted. Ten years ago, if you wanted a pinhole camera that could stream high-definition video over Wi-Fi, you needed a decent budget and some technical know-how. Today, you can go on a site like Ali Express and buy a camera hidden inside a functional USB wall charger for less than thirty dollars.

Corn

Thirty dollars? That is remarkably cheap. It basically lowers the barrier to entry to zero.

Herman

Exactly. And because the barrier is so low, the number of reported incidents has spiked. There was a major study a couple of years ago where a survey of travelers found that about eleven percent of people staying in short-term rentals reported finding a hidden camera. Now, we have to take that with a grain of salt because some of those might have been disclosed exterior security cameras, but the fear is definitely there. Air-B-N-B actually changed their global policy in early two thousand twenty-four to completely ban indoor security cameras in all listings, regardless of whether they were disclosed or not.

Corn

I remember that. It was a big move, but it also felt like a bit of an admission that they couldn't effectively police the "disclosed" ones. People were hiding them in bedrooms and bathrooms and then claiming it was for "security."

Herman

Right. And that is the core of the problem. There is a gray area between legitimate security and voyeurism or corporate espionage. But to answer Daniel's question about whether it is a credible threat, yes, it is. It is not just a paranoid fantasy. We have seen real-world cases, like the one Daniel mentioned in his audio about a diplomat caught with a camera in a changing room at a Tel Aviv beach. When you have devices that are literally designed to look like a religious object or a power outlet, the average person is never going to notice them.

Corn

That is the part that gets me. The power outlet. You and I live in this house in Jerusalem, and we have those exact plugs everywhere. If one of those had a pinhole lens in the little plastic molding, I don't think I would ever see it.

Herman

You wouldn't. The lenses are often less than two millimeters in diameter. They are hidden behind smoked glass or tucked into the natural shadows of the device. And since they draw power directly from the outlet, they never run out of battery. They can stay there for years, just waiting for someone to walk in front of them.

Corn

Okay, so the threat is real in the sense that the technology is available and cheap. But how does it actually work? If someone puts a camera in an Air-B-N-B, how are they getting the footage? Are they coming back to swap out an S-D card, or is this all live-streamed?

Herman

It depends on the sophistication of the attacker. The cheap ones Daniel saw on Ali Express usually offer two modes. One is local storage on a micro S-D card. The attacker has to physically retrieve the device or the card, which is risky for them. The second, and more common now, is Wi-Fi streaming. These devices act as a tiny Wi-Fi client. They connect to the house router and stream the data to a cloud server or a mobile app.

Corn

Wait, if they are on the house Wi-Fi, couldn't a tech-savvy traveler just see them on the network?

Herman

In theory, yes. If you use a network scanning app, you might see a device listed as "Shenzhen Electronic Technology" or something similar. But a clever person will hide the S-S-I-D or use a separate cellular bridge. They can have a tiny four-G or five-G modem hidden in a different part of the room that the camera connects to. That way, it never touches the guest Wi-Fi.

Corn

That brings us to the second part of Daniel's question: the bug-sweeping services. He saw these websites for private investigators offering professional sweeps. Who is the clientele for that? It seems like an expensive thing to do every time you check into a hotel.

Herman

It is definitely not for the average backpacker. The demand for professional Technical Surveillance Counter-Measures, or T-S-C-M, comes from three main sectors. First, you have corporate executives. If you are the C-E-O of a major tech company and you are traveling to a competitor's city for a high-stakes merger negotiation, your hotel room is a goldmine for corporate espionage. One well-placed microphone could be worth billions of dollars in market capitalization.

Corn

I can see that. It is basically the cost of doing business at that level. A five-thousand-dollar sweep is a rounding error compared to the value of the trade secrets they are protecting.

Herman

Exactly. The second group is government officials and diplomats. As Daniel noted, even in "friendly" countries, the assumption is that everyone is listening. When a high-level delegation travels, they often send an advance team. That team's job is to literally strip the room down. They check the vents, the wallpaper, the furniture, everything.

Corn

And the third group?

Herman

This one is a bit more somber. It is people who have a legitimate reason to fear stalking or domestic abuse. High-net-worth individuals who are going through messy divorces or legal battles often hire these services because they are being targeted by someone with the resources to hire a private investigator to track them.

Corn

So, when these professionals show up, what are they actually doing? Is it like in the movies where they have a little wand that beeps when they get close to a wall?

Herman

It is a bit more sophisticated than that, though the "beeping wand" does exist in the form of R-F detectors. Radio Frequency detectors are the most basic tool. They look for signals being transmitted in the common bands, like two point four gigahertz or five gigahertz for Wi-Fi. But here is the catch: if the camera is just recording to an S-D card and not transmitting, an R-F detector won't find it.

Corn

So how do they find a "dumb" camera that isn't broadcasting?

Herman

That is where the cool tech comes in. They use something called a Non-Linear Junction Detector, or N-L-J-D. This is a device that emits a high-frequency radio signal and then listens for the harmonics that bounce back. When that signal hits a semiconductor—which is in every electronic circuit, whether it is turned on or not—it creates a specific kind of reflection.

Corn

So it's like a metal detector, but specifically for silicon chips?

Herman

Exactly! You could have a camera buried six inches deep in a concrete wall, with no power and no battery, and a high-end N-L-J-D will still find the junction of the transistor. It is incredible technology, but it requires a lot of skill to use because it will also alert you to the nails in the floor or the rebar in the wall if you aren't careful.

Corn

I can see why that costs thousands of dollars. You aren't just paying for the person's time; you are paying for a piece of equipment that probably costs twenty or thirty thousand dollars.

Herman

Precisely. And they also use thermal imaging. Electronics generate heat. Even a tiny pinhole camera will be a few degrees warmer than the surrounding drywall. If you look at a wall through a high-resolution thermal camera and see a tiny hot spot behind a picture frame, you've probably found something.

Corn

This makes me think about the "spy shops" Daniel was looking at. He mentioned they were selling these services and this gear. Is that stuff actually effective, or is it mostly just theater for people who want to feel like James Bond?

Herman

It is a mix. The shops Daniel saw in Israel are interesting because, as he mentioned, this is a country with a very high density of people with military and intelligence backgrounds. When those guys retire, they often start these private security firms. So the "Doctor Spy" websites might look a bit kitschy, but the people behind them often know exactly what they are doing. They are selling to other private investigators, not just curious hobbyists.

Corn

But what about the average traveler? If I am going to a city I've never been to and staying in an Air-B-N-B, and I don't have thirty thousand dollars for a professional sweep, am I just at the mercy of whoever owns the place?

Herman

Not necessarily. There are some very effective low-tech ways to protect yourself. The most important one is the "flashlight trick."

Corn

Oh, I've heard of this. You turn off all the lights and shine a bright light around the room?

Herman

Yes, but you have to be methodical. Every camera has a lens, and every lens is made of glass or plastic that reflects light in a very specific way. If you hold a flashlight right next to your eye level and scan the room, you are looking for a tiny, pin-sized reflection that stays consistent as you move. It is the same principle as why a cat's eyes glow in the dark. It is called retro-reflection.

Corn

Does that work even if the camera is behind smoked glass, like on a clock face?

Herman

It does, though it is harder. You have to get the angle just right. There are actually cheap little devices called lens finders that are basically a ring of red L-E-Ds around a viewing hole. You look through the hole, and the L-E-Ds flash. If there is a camera lens, it will flash back at you like a bright red dot. You can buy one of those for twenty dollars, and they are surprisingly effective.

Corn

That seems like a much more reasonable investment for Daniel or any of our listeners. But what about the "why"? Why would an Air-B-N-B host risk their entire business and potentially prison time to put a camera in a room? Is it just perversion, or is there a financial angle?

Herman

It is usually one of three things. First, and most unfortunately, is voyeurism. There are entire subcultures online where this kind of footage is traded. It is disgusting, but it is a real driver. Second is what I call "paranoid hosting." Some hosts are so worried about guests throwing parties or smoking or damaging their property that they convince themselves that a hidden camera is the only way to "protect" their investment. They don't see themselves as criminals; they see themselves as diligent business owners.

Corn

Which is a massive violation of trust and the law.

Herman

Absolutely. And the third reason, which we are seeing more of in international business hubs, is data theft. If you can see a guest's laptop screen or watch them type their password into a safe, you have something much more valuable than a video of them sleeping.

Corn

That is a great point. If you are sitting on the bed working on your laptop, a camera in the ceiling or a smoke detector has a perfect view of your keyboard.

Herman

Precisely. This is why a lot of security experts recommend never using your laptop in a position where the screen or keyboard is visible from a vent or a smoke detector. It sounds paranoid until you realize how easy it is to do.

Corn

You know, we talked about travel routers back in episode three hundred twenty-seven. I remember we discussed how they can help secure your data, but I wonder if they also help with this. If you have your own router, you can see every device that connects to it. But if the camera is using its own cellular connection, the router won't see it.

Herman

Right. The travel router protects your data stream, but it doesn't protect your physical space. It is two different layers of security. It is like having a bulletproof vest but leaving your front door unlocked.

Corn

So, let's look at the legal side for a second. If I find a camera in my room in Jerusalem or London or New York, what actually happens? Is the law caught up to this?

Herman

In most Western jurisdictions, it is a serious crime. In the United States, for example, it often falls under "video voyeurism" laws, which can be felonies. In Israel, the privacy laws are quite strict. If you find a camera in a place where you have a "reasonable expectation of privacy"—like a bedroom or a bathroom—that is a criminal offense.

Corn

But what about a hotel lobby or the hallway of an Air-B-N-B?

Herman

That is where it gets tricky. Most laws allow for cameras in "common areas." But the definition of a common area in a private rental is very different from a hotel. If you are renting an entire house, the living room is generally considered a private area where you have an expectation of privacy. If you are just renting a room, the kitchen might be considered a common area. This ambiguity is exactly why Air-B-N-B just banned them all. It removes the "well, I thought it was a common area" excuse.

Corn

It is interesting that Daniel mentioned the mezuzas and the skullcaps. Those are such culturally specific items here in Israel. It adds a layer of psychological discomfort. You are taking something that is supposed to be a symbol of protection or faith and turning it into a tool of surveillance.

Herman

It is the ultimate "wolf in sheep's clothing" tactic. And it's not just here. In other countries, they hide them in crosses, in Buddhas, in any object that people are conditioned to respect and not touch. It is a very deliberate choice to use objects that a guest would feel uncomfortable moving or inspecting closely.

Corn

So, if someone is listening to this and they are about to head out on a trip, what is the Herman Popleberry checklist for a "five-minute sweep"?

Herman

Okay, here is the quick version. Step one: the physical inspection. Look for the "big three"—smoke detectors, alarm clocks, and USB wall chargers. Those are the most common hiding spots because they have a clear view of the room and easy access to power. Look for any "extra" smoke detectors. If there are two in a small room, one of them is suspicious.

Corn

Step two?

Herman

The flashlight test. Turn off the lights, close the curtains, and use your phone's flashlight. Hold it at eye level and scan the room slowly. Look for that pinprick of light reflecting back at you. Pay special attention to mesh screens on speakers or any small holes in plastic moldings.

Corn

Step three?

Herman

Check the Wi-Fi. Download an app like Fing or Wi-Fi Man. Scan the network. If you see a device that you don't recognize, and especially if it has a name like "I-P Camera" or "C-A-M-Five-Zero-Two," that is a huge red flag.

Corn

And step four?

Herman

This is the simplest one: cover what you can't verify. If there is an alarm clock you don't need, put it in a drawer. If there is a weird-looking USB charger plugged into the wall, unplug it. If there is a hole in a vent that looks suspicious, put a piece of blue painter's tape over it. It won't stop a professional spy, but it will stop ninety-nine percent of the cameras Daniel saw in those spy shops.

Corn

I love the blue painter's tape idea. It's non-destructive, so the host can't complain that you damaged the property, but it's totally effective.

Herman

Exactly. And it sends a message. If a host sees tape over a "security" camera when they come to clean, they know the guest was aware and looking.

Corn

You know, we should probably talk about the demand side of this again. Daniel asked where the demand for these high-end services comes from. We talked about executives and diplomats, but is there a market for "counter-surveillance" for the average person? Like, are there people who are just chronically paranoid?

Herman

Oh, absolutely. There is a whole industry built on "targeted individuals." These are people who believe they are being followed or watched by the government or shadowy organizations. It is often a mental health issue, but these spy shops will happily sell them thousands of dollars of equipment that won't actually solve their problem. It is the darker side of the industry. They profit off of people's fears, whether those fears are grounded in reality or not.

Corn

That is the tricky part of being an "expert" in this field, I imagine. You have to distinguish between a legitimate threat and a delusion. If a professional bug-sweeper gets a call from someone saying their toaster is talking to them, they have a choice to make.

Herman

Most reputable firms will do a preliminary interview. If the client sounds like they are experiencing a mental health crisis, they will often decline the work. But the "Doctor Spy" type shops? They are often just retail outlets. They'll sell a signal jammer to anyone with a credit card, even though signal jammers are highly illegal in almost every country, including Israel.

Corn

Wait, jammers are illegal? I can see why—they could interfere with emergency services.

Herman

Exactly. If you turn on a powerful R-F jammer to stop a hidden camera, you might also be stopping your neighbor from calling an ambulance. It is a huge public safety risk. That is why the professional sweepers use detectors, not jammers. They find the problem; they don't just blast the airwaves with noise.

Corn

This whole conversation makes me realize how much the "hidden" part of hidden cameras is a moving target. As soon as we learn to look for smoke detectors, they start putting them in the heads of screws or inside the actual drywall.

Herman

It is a classic arms race. We saw this in episode three hundred sixty-three when we talked about the anatomy of failure in military probes. When one side develops a detection method, the other side develops a counter-measure. Now, there are cameras that use "spread spectrum" transmission, which makes them look like background noise to a basic R-F detector. They only transmit in tiny bursts, or they "hop" between frequencies.

Corn

So even the "beeping wand" would miss them if they weren't transmitting at that exact second?

Herman

Precisely. That is why the professional sweepers will stay in a room for four or five hours. They are waiting for those bursts. They might even use a "stimulator," which is a device that broadcasts a signal designed to "wake up" any hidden bugs and get them to report back to their home base.

Corn

It's like a digital roll call. That is fascinating. It's so much more involved than I ever imagined.

Herman

It really is. But I think for Daniel's sake, and for our listeners, the takeaway shouldn't be one of total paranoia. It's about "informed awareness." The threat is credible, but it's also manageable for the average person. You don't need a twenty-thousand-dollar Non-Linear Junction Detector to feel safe in an Air-B-N-B. You just need a flashlight, a network scanning app, and a bit of common sense.

Corn

And maybe a roll of blue painter's tape.

Herman

Always the tape. It is the ultimate low-tech solution to a high-tech problem.

Corn

You know, looking at the time, we have really covered a lot of ground here. We went from Daniel's search for a Sony voice recorder to the harmonics of semiconductor junctions. This is exactly why I love this show.

Herman

It's the rabbit holes, Corn. They are infinite. And I think Daniel's observation about the "mezuzas" and "skullcaps" is such a great reminder that technology doesn't exist in a vacuum. It's always filtered through our culture and our environment. In a different country, they'd be hiding cameras in different objects, but the intent remains the same.

Corn

Well, I think that is a perfect place to start wrapping up. We've looked at the credibility of the threat—which is real but rare—and we've explored the world of the professional "bug-sweepers" who serve the high-stakes worlds of business and diplomacy.

Herman

And we've given everyone a few practical tools to take back some of that privacy. It's a weird world out there, but you don't have to be a victim of it.

Corn

Absolutely. Before we go, I want to say a huge thank you to everyone who has been with us for these three hundred sixty-five episodes. It genuinely means the world to us that you choose to spend your time in these rabbit holes with us. If you are enjoying the show, we would really appreciate it if you could leave us a quick review on your podcast app or on Spotify. It really does help other curious people find us.

Herman

Yeah, it makes a huge difference. We love seeing the community grow. And remember, if you have a weird prompt of your own, or if you've found something strange in a hotel room and want us to talk about it, you can get in touch with us through the contact form at my-weird-prompts dot com.

Corn

You can also find our full archive and the R-S-S feed there. This has been My Weird Prompts. I'm Corn.

Herman

And I'm Herman Poppleberry.

Corn

Thanks for listening, and we will talk to you next week.

Herman

Stay curious, and maybe keep an eye on your smoke detectors. Just in case.

Corn

Goodbye, everyone!