



October 2026

Citizen Surveillance

By Mark Costlow

We wrote in our [July 2024 issue](#) about how we are tracked online, specifically [through internet ads and phone apps](#). It would be nice if anything had improved since then, but obsessive tracking of Americans has only increased. Many of the tracking vectors are well-known, like phone location data and online behavior monitors, but surprising new ones are popping up every day. And some are being baked into society by laws that nobody can opt out of. The worst part is the sophisticated systems which synthesize dozens of these disparate databases to create complete pictures of a person's whole existence.

Buckle in, it's a wild ride.

Where do you shop?

At least as far back as 2015, the FTC was warning us about the [privacy concerns of retail industry](#) tracking of consumers. Our phones, smart watches, and other wearables constantly emit Wi-Fi and Bluetooth signals. These can be passively observed and used to identify and [track us as we move through stores](#), malls, airports and other spaces.

There was some initial backlash over use of these technologies, as they were "stealing" your location information by using these wireless protocols in a way you did not intend. After all, you were just walking through Nordstrom with your phone turned on, not trying to connect to Nordstrom's WiFi network. The [FTC settled a complaint in 2014 with a company called Nomi](#) who provided this technology for retailers. The complaint was that Nomi had promised in-store opt-out options which they did not provide. At the time, many retailers, including Nordstrom, voluntarily ceased using that technology due to the bad optics.

Fast forward a decade, and they are all using the equivalent of this technology, and more. The difference is they found a way to get everybody to opt-in. Many retailers are tracking users through their branded apps. If you allow location services for the app (usually a question at installation time), the app will use WiFi and [Bluetooth beacons](#) to know when you enter a store, and exactly where you spend your time within it. The privacy policy

you agreed to when you installed the app explicitly gives permission for this and other forms of tracking.

It may seem harmless, but remember that you probably have no assurances that the data will only be used for the purpose of sending you a coupon when you enter the store. The privacy policy for any given store very likely puts very few limitations on what the company can do with the data or who they can share it with.

Thousands of retailers in the US use a system called [Auror](#) to track shoplifting and other crimes committed at the retailers. The system uses video from inside and outside retail locations, and Automated License Plate Readers (ALPRs) to gather data. It synthesizes events across all of the subscribed retail locations to [track criminals \(and everyone else\)](#) as they move in or near different stores. [Law enforcement agencies subscribe](#) to access video evidence online without having to visit each place. For example, Auror's [law enforcement pitch page](#) shows a list of people with a name and picture of each one, number of events with associated cash value, and number of accomplices. Officers can drill down to find information on accomplices and what vehicles each have used, and from there, where each vehicle has been seen recently.

Your specific frame of mind will shape your opinion of this. In one light, this is an exciting fusion of computer technology and network effects that makes it possible to capture and prosecute costly or dangerous criminals. Beyond that, it reveals links among the perpetrators to [uncover shoplifting rings and other criminal gangs, maybe even organized crime](#) and human trafficking.

Or, you may see this as a dystopian surveillance system just waiting to be weaponized against innocent people. The [ACLU opposes](#) the building of massive unregulated databases used to track any and all persons in this way. There are several problems with the concept:

- The data can be stolen and used by unknown 3rd parties. [404 Media reported](#) that hackers stole a Flock camera from a roadway and reverse engineered the software inside. Flock says the videos are protected by on-device encryption, but the hackers quickly found the encryption key was stored on the device, which unlocked thousands of vehicle detection videos.
- The data can be shared with law enforcement on purpose in a way that [violates Fourth Amendment rights](#), or misused by supposed legitimate users. The [Institute for Justice documented hundreds of incidents](#) of ALPR systems used to stalk current and ex- wives and girlfriends.
- The data can have errors which badly harm innocent people. Two innocent sisters in Es-

panola, NM were held at gunpoint by officers because a **Flock camera misread a digit** of a license plate.

Beyond Inconvenience

In July 2025 **Angela Lipps was arrested at gunpoint** by US Marshals in Tennessee because a facial recognition camera in Fargo, ND falsely identified her. She was jailed in Tennessee for four months and extradited to North Dakota where she served two more months, all while she had the very good alibi of being many states away at the time of the crime. Released into the freezing cold on Christmas Eve with no resources, she had lost her home, car, and personal property. AI facial recognition should not have been trusted to a degree that would wreck an innocent person's life, but we humans have a tendency to accept the computer's very confident assertions as unassailable fact.

Less Obvious Methods

Video surveillance and ALPR are well known, having been in the news a lot this year. Now let's look at some ways we're being observed that many are unaware of.

Apps

Every app that collects your location data is at least sharing it with the app owner and **may combine it with other data and sell it on** to data brokers. Many apps use 3rd-party libraries for the location tracking, and some of those libraries leak your location trails to data brokers. **Some have been shut down**, but your best defense is to refuse location access to most apps. If you must allow it, limit it to when the app is running, not full time.

Cars

All car makers offer apps for their customers to connect with and manage their vehicles. Modern cars are a hive of sensors, microphones and cameras **collecting all manner of data**. Not just where you go and how fast you drive, but what songs or podcasts you listen to. The **Mozilla Foundation studied 25 car makers** and it was the first time **every single product in a category failed** their consumer privacy scorecard.

They read the privacy policies of the car makers and a few items stand out. **Nissan** and Kia said they can collect and share information about your sexual activity. Six companies said they can collect your "genetic information" or "genetic characteristics". 84% share or sell some or all of this data with brokers and 19 of the 25 say they can sell your personal data. Over half say they can share your data with law enforcement in response to a "request" (not a court order). Hyundai's wording is particularly troubling: they will comply with "lawful requests, whether formal or informal."

Data collected in these ways is never used solely for the initial stated purpose. It will be har-

vested and monetized, and combined with other databases to make ever more detailed dossiers describing every individual. It will quite possibly be stolen and then used by criminals.

Ultimate Stalker Tool

The EFF reports that cars are frequently used to further harass and stalk domestic abuse survivors. When the abuser has access to the victim's car via an app they can still access the car's location and even disable it so it can't be used. **The EFF is lobbying for laws** to fix this, but it's complicated.

Under Pressure

Newer cars have **Tire Pressure Monitoring Systems, TPMS**, which alert if one of your tires is low. Have you ever wondered how they get the air pressure sensor in the spinning wheel wired back to the car computer? How do they pass a wire through the spinning wheel hub? They don't - they use wireless. The sensor in the wheel uses something like a Bluetooth connection to report the current pressure to the car computer. The message includes a unique ID number, broadcast in the clear.

The problem is, a low-cost roadside radio receiver can collect these ID numbers from passing cars. A **research team deployed a few** and collected 6 million tire messages from over 20,000 cars.

The next step is the scary one. When these receivers are paired with ALPR cameras, the database gets 2 bits of info, your license number combined with your tire sensor IDs. Now these cheap and nearly invisible receivers can be deployed anywhere to track those cars. They can be on any street or road or garage, with no bulky cameras to betray their presence.

That's Not All ...

Well, we have run out of room before we ran out of new surveillance methods to discuss. Watch this space for more.

This Month in Ideas & Coffee

Check out the free talks and classes this month!

- **October 13 6pm - 7:30pm** - Using AI with self-hosted WordPress.
- **October 20 6pm - 7:30pm** - *WordPress Work Along* - Answers to your pressing WordPress questions. Bring your laptop!
- **October 14 6pm - 8pm** - Basic Computer Use - email, browsers, and staying safe online.

Watch the **Ideas & Coffee** event calendar at <https://swcp.com/calendar> for future info.

Southwest Cyberport - swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on **[bold blue type](#)** in browser for links.

|