

REPORT 24

The transparent citizen is already a reality: AI cracks "anonymous" location data for \$2.24

• 02. September 2026



(C) Raport 24/AI

Billions of people carry their smartphones with them practically around the clock – leaving a trail throughout their entire lives. Data brokers have been collecting and selling such location information for years as a supposedly anonymous commodity. Swiss researchers have now shown just how little "anonymity" actually exists: On average, an AI needed only 17 minutes and \$2.24 to identify a specific person from location data.

A smartphone repeatedly spends the night at the same address. In the morning, it travels to an office building, stays there for several hours, and returns in the evening. It doesn't take an intelligence analyst to develop an obvious suspicion: someone lives here, someone works there. Oscar Thees, Roman Müller, and Matthias Templ from the University of Applied Sciences Northwestern Switzerland had [an AI do this work](#). It was designed to identify residences and workplaces from movement data and then search publicly available information until a name emerged behind the supposedly anonymous GPS track.

The [result](#) should interest anyone who still clicks through to websites with the phrase "anonymized data." Of 25 test subjects who were fundamentally identifiable based on publicly available information, the system found 18. When the AI provided a specific name, it was correct in 18 out of 19 cases. And it needed an average of just 17 minutes and \$2.24 to do so. While a human investigator can only ever scrutinize a limited number of people at once, the situation is quite different with such AI searches. Computers can process these tasks in parallel.

Anonymity effectively no longer exists.

Location data has been collected, bundled, and sold en masse for years. Data brokers remove names and other obvious identifying characteristics and instead assign identifiers to devices. On paper, this appears to be cleanly anonymized. In reality, a movement pattern often reveals more than a name in a spreadsheet. Where does the device "sleep"? Where is it located between 8 and 5 pm, Monday through Friday? Which company is located there? Who lives at the overnight address and works for that very company? Suddenly, little remains of the anonymity.

For data privacy reasons, the Swiss researchers used simulated GPS tracks around the actual homes and workplaces of volunteer participants. This revealed that the search for the person behind a trail of location data can now easily be outsourced to artificial intelligence. And such supposedly "anonymized" data packages are readily available.

The data used for surveillance has long been sold.

This would be far less worrying if such location data were difficult to obtain. But the exact opposite is true. The "[Databroker Files](#)" have already revealed the scale of the industry's operations. Journalists from Netzpolitik.org and international partners received massive data packages from data brokers, sometimes simply as free samples for potential buyers. One dataset examined contained approximately 380 million location data points from 137 countries, linked to about 47 million device identifiers. The data originated from roughly 40,000 apps, including applications such as Wetter Online, Focus Online, classifieds sites, and Flightradar24. For some data points, a smartphone could be located to within a few meters.

The research team now [claims to](#) possess more than 13 billion location data records from various vendors. In Belgium, the journalists found thousands of location data points originating from EU and NATO buildings. Around 2,000 location reports came from the European Commission headquarters, approximately 5,800 from the European Parliament, and about 9,600 from NATO headquarters. This is far from a harmless game. Anyone who possesses such data can search for government employees, soldiers, diplomats, or security agency personnel. From official locations, the movement trails can then potentially lead directly to a private address.

The bug is already in the trouser pocket.

Report24 [already reported](#) in January on how advertising data has become a veritable surveillance tool. Under the term "advertising intelligence," commercially collected information is analyzed to track devices and create movement profiles. What was originally intended for more targeted advertising has long since become interesting to security authorities and intelligence services. The Swiss study now adds a crucial piece to the puzzle.

It is no longer sufficient to rely on the fact that only some device identifier, rather than a name, is stored in the database. AI can help close precisely this gap.

Once a tracking device is linked to a person, the coordinates become a diary of their life. Home, workplace, and regular routes are just the beginning. Added to this are doctor's appointments, political events, demonstrations, churches, mosques, hotels, brothels, or other places that are nobody else's business. Criminals can deduce absence patterns and habits from this data. Foreign intelligence agencies can be interested in government employees and their contacts. For authoritarian regimes, the data offers opportunities to persecute opposition members or members of their own diaspora, even abroad. The infrastructure for this doesn't need to be built; it already exists.

AI turns the mountain of data into a surveillance tool.

Until now, there was at least one natural brake: someone had to analyze the data. Millions of location points are, in themselves, just a gigantic pile of coordinates. Only analysis transforms them into usable information. And AI is now beginning to remove this brake. Finding a place of residence, identifying an employer, searching public registers, comparing possible names – such tasks suddenly no longer require hours of human research. In the Swiss experiment, the system completed them for just a few dollars.

This transforms a commercial data repository into a tool that even smaller players can use. Comprehensive analysis no longer necessarily requires the resources of a large intelligence agency. And anyone running a freely available AI model on their own computer doesn't even need the consent of a commercial provider. No terms of service from an AI corporation prevent analysis when the model runs locally.

The transparent citizen has long since been created.

The surveillance of modern humans doesn't begin with some super-database of government data. We generate the necessary information ourselves every day. Smartphones track our location. Various apps provide data to advertising networks. Modern vehicles collect GPS and usage information. Cameras capture license plates, and digital payments leave further traces. Each data set on its own may seem harmless. But together, they paint an increasingly detailed picture. Report24 [has already reported](#) on the data that modern cars now collect and why intelligence agencies are also interested in this information.

The promise of anonymity was already flimsy. AI now makes it clear that apparently no one is safe from such surveillance measures anymore. The advertising industry and its data brokers have amassed a gigantic mountain of raw material from our digital footprints over the years. Now tools are available that can extract names, addresses, jobs, and movement profiles from this data for a pittance. The transparent citizen isn't coming sometime in the future. He's already here. And he recharges his own mobile tracking device every evening.