Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it’s anonymous, but the data shows how personal it is.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK  DEC. 10, 2018

Yet another leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her.
An app on the device gathered her location information, which was then sold without her knowledge. It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The New York Times. While Ms. Magrin’s identity was not disclosed in those records, The Times was able to easily connect her to that dot.

The app tracked her as she went to a Weight Watchers meeting and to her dermatologist’s office for a minor procedure. It followed her hiking with her dog and staying at her ex-boyfriend’s home, information she found disturbing.

“It’s the thought of people finding out those intimate details that you don’t want people to know,” said Ms. Magrin, who allowed The Times to review her location data.

Like many consumers, Ms. Magrin knew that apps could track people’s movements. But as smartphones have become ubiquitous and technology more accurate, an industry of snooping on people’s daily habits has spread and grown more intrusive.

At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information, The Times found. Several of those businesses claim to track up to 200 million mobile devices in the United States — about half those in use last year. The database reviewed by The Times — a sample of information gathered in 2017 and held by one company — reveals people’s travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day.

[Learn how to stop apps from tracking your location.]

These companies sell, use or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior. It’s a hot market, with sales of location-targeted advertising reaching an estimated $21 billion this year. IBM has gotten into the industry, with its purchase of the Weather Channel’s apps. The social network Foursquare remade itself as a location marketing company. Prominent investors in location start-ups include Goldman Sachs and Peter Thiel, the PayPal co-founder.
Businesses say their interest is in the patterns, not the identities, that the data reveals about consumers. They note that the information apps collect is tied not to someone’s name or phone number but to a unique ID. But those with access to the raw data — including employees or clients — could still identify a person without consent. They could follow someone they knew, by pinpointing a phone that regularly spent time at that person’s home address. Or, working in reverse, they could attach a name to an anonymous dot, by seeing where the device spent nights and using public records to figure out who lived there.

Many location companies say that when phone users enable location services, their data is fair game. But, The Times found, the explanations people see when prompted to give permission are often incomplete or misleading. An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy.

“Location information can reveal some of the most intimate details of a person’s life — whether you’ve visited a psychiatrist, whether you went to an A.A. meeting, who you might date,” said Senator Ron Wyden, Democrat of Oregon, who has proposed bills to limit the collection and sale of such data, which are largely unregulated in the United States.

“It’s not right to have consumers kept in the dark about how their data is sold and shared and then leave them unable to do anything about it,” he added.

Mobile Surveillance Devices

After Elise Lee, a nurse in Manhattan, saw that her device had been tracked to the main operating room at the hospital where she works, she expressed concern about her privacy and that of her patients.

“It’s very scary,” said Ms. Lee, who allowed The Times to examine her location history in the data set it reviewed. “It feels like someone is following me, personally.”

The mobile location industry began as a way to customize apps and target ads for nearby businesses, but it has morphed into a data collection and analysis machine.
Retailers look to tracking companies to tell them about their own customers and their competitors’. For a web seminar last year, Elina Greenstein, an executive at the location company GroundTruth, mapped out the path of a hypothetical consumer from home to work to show potential clients how tracking could reveal a person’s preferences. For example, someone may search online for healthy recipes, but GroundTruth can see that the person often eats at fast-food restaurants.

“We look to understand who a person is, based on where they’ve been and where they’re going, in order to influence what they’re going to do next,” Ms. Greenstein said.

Financial firms can use the information to make investment decisions before a company reports earnings — seeing, for example, if more people are working on a factory floor, or going to a retailer’s stores.

Health care facilities are among the more enticing but troubling areas for tracking, as Ms. Lee’s reaction demonstrated. Tell All Digital, a Long Island advertising firm that is a client of a location company, says it runs ad campaigns for personal injury lawyers targeting people anonymously in emergency rooms.

“The book ‘1984,’ we’re kind of living it in a lot of ways,” said Bill Kakis, a managing partner at Tell All.

Jails, schools, a military base and a nuclear power plant — even crime scenes — appeared in the data set The Times reviewed. One person, perhaps a detective, arrived at the site of a late-night homicide in Manhattan, then spent time at a nearby hospital, returning repeatedly to the local police station.

Two location firms, Fysical and SafeGraph, mapped people attending the 2017 presidential inauguration. On Fysical’s map, a bright red box near the Capitol steps indicated the general location of President Trump and those around him, cellphones pinging away. Fysical’s chief executive said in an email that the data it used was anonymous. SafeGraph did not respond to requests for comment.

More than 1,000 popular apps contain location-sharing code from such companies, according to 2018 data from MightySignal, a mobile analysis firm. Google’s Android system was found to have about 1,200 apps with such code, compared with about 200 on Apple’s iOS.
The most prolific company was Reveal Mobile, based in North Carolina, which had location-gathering code in more than 500 apps, including many that provide local news. A Reveal spokesman said that the popularity of its code showed that it helped app developers make ad money and consumers get free services.

To evaluate location-sharing practices, The Times tested 20 apps, most of which had been flagged by researchers and industry insiders as potentially sharing the data. Together, 17 of the apps sent exact latitude and longitude to about 70 businesses. Precise location data from one app, WeatherBug on iOS, was received by 40 companies. When contacted by The Times, some of the companies that received that data described it as “unsolicited” or “inappropriate.”

WeatherBug, owned by GroundTruth, asks users’ permission to collect their location and tells them the information will be used to personalize ads. GroundTruth said that it typically sent the data to ad companies it worked with, but that if they didn’t want the information they could ask to stop receiving it.

The Times also identified more than 25 other companies that have said in marketing materials or interviews that they sell location data or services, including targeted advertising.

[Read more about how The Times analyzed location tracking companies.]

The spread of this information raises questions about how securely it is handled and whether it is vulnerable to hacking, said Serge Egelman, a computer security and privacy researcher affiliated with the University of California, Berkeley.

“There are really no consequences” for companies that don’t protect the data, he said, “other than bad press that gets forgotten about.”

A Question of Awareness

Companies that use location data say that people agree to share their information in exchange for customized services, rewards and discounts. Ms. Magrin, the teacher, noted that she liked that tracking technology let her record her jogging routes.
Brian Wong, chief executive of Kiip, a mobile ad firm that has also sold anonymous data from some of the apps it works with, says users give apps permission to use and share their data. “You are receiving these services for free because advertisers are helping monetize and pay for it,” he said, adding, “You would have to be pretty oblivious if you are not aware that this is going on.”

But Ms. Lee, the nurse, had a different view. “I guess that’s what they have to tell themselves,” she said of the companies. “But come on.”

Ms. Lee had given apps on her iPhone access to her location only for certain purposes — helping her find parking spaces, sending her weather alerts — and only if they did not indicate that the information would be used for anything else, she said. Ms. Magrin had allowed about a dozen apps on her Android phone access to her whereabouts for services like traffic notifications.

But it is easy to share information without realizing it. Of the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising. Only one app, GasBuddy, which identifies nearby gas stations, indicated that data could also be shared to “analyze industry trends.”

More typical was theScore, a sports app: When prompting users to grant access to their location, it said the data would help “recommend local teams and players that are relevant to you.” The app passed precise coordinates to 16 advertising and location companies.

A spokesman for theScore said that the language in the prompt was intended only as a “quick introduction to certain key product features” and that the full uses of the data were described in the app’s privacy policy.

The Weather Channel app, owned by an IBM subsidiary, told users that sharing their locations would let them get personalized local weather reports. IBM said the subsidiary, the Weather Company, discussed other uses in its privacy policy and in a separate “privacy settings” section of the app. Information on advertising was included there, but a part of the app called “location settings” made no mention of it.
The app did not explicitly disclose that the company had also analyzed the data for hedge funds — a pilot program that was promoted on the company’s website. An IBM spokesman said the pilot had ended. (IBM updated the app’s privacy policy on Dec. 5, after queries from The Times, to say that it might share aggregated location data for commercial purposes such as analyzing foot traffic.)

Even industry insiders acknowledge that many people either don’t read those policies or may not fully understand their opaque language. Policies for apps that funnel location information to help investment firms, for instance, have said the data is used for market analysis, or simply shared for business purposes.

“Most people don’t know what’s going on,” said Emmett Kilduff, the chief executive of Eagle Alpha, which sells data to financial firms and hedge funds. Mr. Kilduff said responsibility for complying with data-gathering regulations fell to the companies that collected it from people.

Many location companies say they voluntarily take steps to protect users’ privacy, but policies vary widely.

For example, Sense360, which focuses on the restaurant industry, says it scrambles data within a 1,000-foot square around the device’s approximate home location. Another company, Factual, says that it collects data from consumers at home, but that its database doesn’t contain their addresses.

Some companies say they delete the location data after using it to serve ads, some use it for ads and pass it along to data aggregation companies, and others keep the information for years.

Several people in the location business said that it would be relatively simple to figure out individual identities in this kind of data, but that they didn’t do it. Others suggested it would require so much effort that hackers wouldn’t bother.

It “would take an enormous amount of resources,” said Bill Daddi, a spokesman for Cuebiq, which analyzes anonymous location data to help retailers and others, and raised more than $27 million this year from investors including Goldman Sachs and Nasdaq Ventures. Nevertheless, Cuebiq encrypts its information, logs employee queries and sells aggregated analysis, he said.
There is no federal law limiting the collection or use of such data. Still, apps that ask for access to users’ locations, prompting them for permission while leaving out important details about how the data will be used, may run afoul of federal rules on deceptive business practices, said Maneesha Mithal, a privacy official at the Federal Trade Commission.

“You can’t cure a misleading just-in-time disclosure with information in a privacy policy,” Ms. Mithal said.

**Following the Money**

Apps form the backbone of this new location data economy.

The app developers can make money by directly selling their data, or by sharing it for location-based ads, which command a premium. Location data companies pay half a cent to two cents per user per month, according to offer letters to app makers reviewed by The Times.

Targeted advertising is by far the most common use of the information.

Google and Facebook, which dominate the mobile ad market, also lead in location-based advertising. Both companies collect the data from their own apps. They say they don’t sell it but keep it for themselves to personalize their services, sell targeted ads across the internet and track whether the ads lead to sales at brick-and-mortar stores. Google, which also receives precise location information from apps that use its ad services, said it modified that data to make it less exact.

Smaller companies compete for the rest of the market, including by selling data and analysis to financial institutions. This segment of the industry is small but growing, expected to reach about $250 million a year by 2020, according to the market research firm Opimas.

Apple and Google have a financial interest in keeping developers happy, but both have taken steps to limit location data collection. In the most recent version of Android, apps that are not in use can collect locations “a few times an hour,” instead of continuously.

Apple has been stricter, for example requiring apps to justify collecting location details in pop-up messages. But Apple’s instructions for writing
these pop-ups do not mention advertising or data sale, only features like getting “estimated travel times.”

A spokesman said the company mandates that developers use the data only to provide a service directly relevant to the app, or to serve advertising that met Apple’s guidelines.

Apple recently shelved plans that industry insiders say would have significantly curtailed location collection. Last year, the company said an upcoming version of iOS would show a blue bar onscreen whenever an app not in use was gaining access to location data.

The discussion served as a “warning shot” to people in the location industry, David Shim, chief executive of the location company Placed, said at an industry event last year.

After examining maps showing the locations extracted by their apps, Ms. Lee, the nurse, and Ms. Magrin, the teacher, immediately limited what data those apps could get. Ms. Lee said she told the other operating-room nurses to do the same.

“I went through all their phones and just told them: ‘You have to turn this off. You have to delete this,’” Ms. Lee said. “Nobody knew.”

Adam Satariano contributed reporting.

Related Coverage

- How Game Apps That Captivate Kids Have Been Collecting Their Data | SEPT. 12, 2018

- Service Meant to Monitor Inmates’ Calls Could Track You, Too | MAY 10, 2018

- Hundreds of Apps Can Empower Stalkers to Track Their Victims | MAY 19, 2018

© 2018 The New York Times Company