Phone data-leak company: No record of location-data abuse

19 May 2018, by Frank Bajak

In this June 6, 2017, file photo, a man checks his phone in an alley in downtown Chicago. A security researcher says a website flaw at a U.S. company could have allowed anyone to pinpoint the location of nearly any cellphone in the United States. The lapse at LocationSmart, a company that gathers real-time data on cellular wireless devices, is the latest to highlight how little protection consumers have from trafficking in data about their location. (AP Photo/G-Jun Yam, File)

A California company confirmed that a flaw in its website allowed outsiders to pinpoint the location of mobile phones in the United States without authorization.

But LocationSmart, which gathers real-time data on cellular wireless devices, says it has no evidence that anyone exploited the vulnerability before May 16, when a security researcher at Carnegie Mellon discovered it.

Brenda Schafer, a LocationSmart vice president, said via email Friday that the company is still seeking to verify that no location data was accessed without individual subscribers' consent. She did not respond to questions about LocationSmart's business practices or how long the flaw had existed.

Privacy advocates say the case is the latest to underscore how easily wireless carriers can share or sell consumers' geolocation information without their consent. The LocationSmart flaw was first reported by independent journalist Brian Krebs.

LocationSmart operates in a little-known business sector that provides data to companies for such uses as tracking employees and texting e-coupons to customers near relevant stores. Among the customers LocationSmart identifies on its website are the American Automobile Association, FedEx and the insurance carrier Allstate.

The New York Times reported earlier this month that a firm called Securus Technologies provided location data on mobile customers to a former Missouri sheriff accused of using the data to track people without a court order. On Wednesday, Motherboard reported that Securus' servers had been breached by a hacker who stole user data that mostly belonged to law enforcement officials.

Securus may have obtained its location data indirectly from LocationSmart. Securus officials told the office of Sen. Ron Wyden, an Oregon Democrat, that they obtained the data from a company called 3Cinterative, said Wyden spokesman Keith Chu. LocationSmart lists 3Cinteractive among its customers on its website.

Wyden said the LocationSmart and Securus cases underscore the "limitless dangers" Americans face due to the absence of federal regulation on geolocation data.

"A hacker could have used this site to know when you were in your house so they would know when to rob it. A predator could have tracked your child's cellphone to know when they were alone," he said in a statement.

A spokeswoman for the Federal Communications Commission said the LocationSmart case had been referred to the agency's enforcement bureau for investigation.

LocationSmart took the flawed webpage offline Thursday, a day after Carnegie Mellon University computer science student Robert Xiao discovered the software bug and notified the company, Xiao told The Associated Press.

The bug "allowed anyone, anywhere in the world, to look up the location of a U.S. cellphone," said Xiao, a doctoral researcher. "I could punch in any 10-digit phone number," he added, "and I could get anyone's location."

The web page was designed to let visitors test out LocationSmart's service by entering their cellphone number. The service would then ring their phone or send a text message to obtain consent, after which it would display the phone's location—generally to within several hundred yards.

But Xiao found a flaw that allowed him to bypass consent in just 15 minutes. "It would not take anyone with sufficient technical knowledge much time to find this," he said. He wrote a script to exploit it.

Xiao's research indicated that LocationSmart had offered the service since at least January 2017.

LocationSmart touts itself as the "world's largest location-as-service company." It says it obtains location information from all major U.S. and Canadian wireless companies, with 95 percent coverage.

Verizon spokesman Rich Young said the company has taken steps to ensure that Securus can no longer request information on the company's wireless customers and that it was reviewing its relationship with LocationSmart. T-Mobile likewise said it has "addressed issues that were identified with Securus and LocationSmart."

Representatives for AT&T and Sprint said they don't allow sharing of location information without individual consent or a lawful order such as a warrant.

Gigi Sohn, a former top aide at the FCC during the Obama administration, said user location data has been at high risk since last year. That's when Congress repealed FCC privacy rules barring mobile wireless carriers from sharing or selling it without customers' express "opt-in" consent.

"At a bare minimum, consumers should be able to choose whether a company like LocationSmart should have access to this data at all," she said.