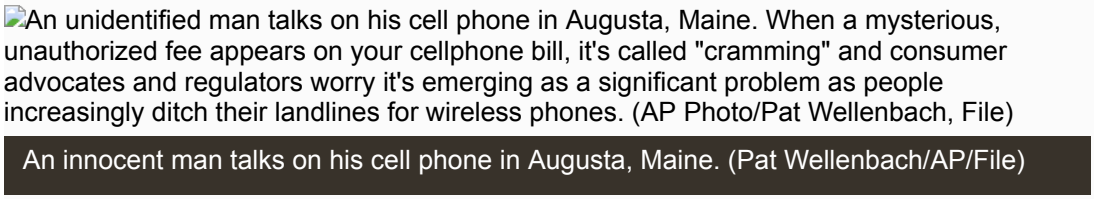
Any hacker or sex partner can see the location of your phone or your car at any given moment

Website flaw exposed most U.S. cellphones' real-ti locations



An unidentified man talks on his cell phone in Augusta, Maine. When a mysterious, unauthorized fee appears on your cellphone bill, it's called "cramming" and consumer advocates and regulators worry it's emerging as a significant problem as people increasingly ditch their landlines for wireless phones. (AP Photo/Pat Wellenbach, File)

An innocent man talks on his cell phone in Augusta, Maine. (Pat Wellenbach/AP/File)

By **FRANK BAJAK** | Associated Press

A website flaw at a California company that gathers real-time data on cellular wireless devices could have allowed anyone to pinpoint the location of any AT&T, Verizon, Sprint or T-Mobile cellphone in the United States to within hundreds of yards, a security researcher said.

The company involved, LocationSmart of Carlsbad, 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. LocationSmart did not immediately respond to emails and telephone messages seeking comment on the flaw and its business practices.

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

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.

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 doctoral researcher said the bug "allowed anyone, anywhere in the world, to look up the location of a U.S. cellphone," said Xiao. "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.

“It was just surreal when I discovered this,” he said. 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.

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. 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 did not immediately respond to a request for comment.

Gigi Sohn, a former top aide at the Federal Communications Commission 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.

AP Technology Writer Matt O’Brien contributed to this report.

Related Articles

Magid: Facebook cleanup doesn’t replace your need to be diligent

How many fake accounts did Facebook quash so far this year?

Is Google tracking location without permission? FTC probe urged, Australia inquiry begins

Facebook suspends 200 apps, including one that reportedly exposed data of 3 million

Tim Cook takes swipe at Facebook (and Google?) in

commencement speech

Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US (motherboard.vice.c

by un1ty to **news** (+18|-0)

comments