






## A bug in cell phone tracking firm's website leaked millions of Americans' real-time locations

The bug allowed one Carnegie Mellon researcher to track anyone's cell phone in real time. Cell phone tracking firm's website leaked millions of Americans' real-time locations




By [Zack Whittaker](#) for [Zero Day](#) | May 17, 2018 -- 19:45 GMT (12:45 PDT)

# REAL-TIME LOCATION



MapSatellite



Map data ©2018 Google Imagery ©2018, Bluesky, DigitalGlobe, Landsat / Copernicus, Sanborn, USDA Farm Service Agency Terms of Use Report a map error

908 [REDACTED] is located in the neighborhood of:

### LOCATION RESULTS

Address:	36 E 29th St
City, State:	New York, NY
Zip Code:	10016
Country:	US
Latitude/Longitude:	40.744410, -73.985080
Accuracy:	0.21 miles
Response Time:	6.10 seconds

### WHAT'S NEARBY

Cross Street:	Madison Ave
Intersection:	F D R Dr & I- 495
Point Of Interest:	De Plano Group Inc

### DEVICE DETAILS

Carrier:	Verizon Wireless
Type:	Wireless
SMS:	Supported

*A bug allowed anyone to skip a consent requirement in a cell phone location tracking site. (Image: ZDNet)*

A company that collects the real-time location data on millions of cell phone customers across North America had a bug in its website that allowed anyone to see where a person is located -- without obtaining their consent.

Earlier this week, [we reported that four of the largest cell giants](https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/) (<https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/>) in the US are selling your real-time location data to a company that you've probably never heard about before.

The company, LocationSmart, is a data aggregator and [claims to have "direct connections"](https://archive.li/THily) (<https://archive.li/THily>) to cell carriers to obtain locations from nearby cell towers. The site had [its own "try-before-you-buy" page](https://www.locationsmart.com/try/) (<https://www.locationsmart.com/try/>) that lets you test the accuracy of its data. The page [required explicit consent](https://archive.li/TmOa6) (<https://archive.li/TmOa6>) from the user before their location data can be used by sending a one-time text message to the user. When we tried with a colleague, we tracked his phone to a city block of his actual location.

But that website had a bug that allowed anyone to track someone's location silently without their permission.

"Due to a very elementary bug in the website, you can just skip that consent part and go straight to the location," said Robert Xiao, a PhD student at the Human-Computer Interaction Institute at Carnegie Mellon University, in a phone call.

"The implication of this is that LocationSmart never required consent in the first place," he said. "There seems to be no security oversight here."

The "try" website was pulled offline after Xiao privately disclosed the bug to the company, with help from CERT, a public vulnerability database, also at Carnegie Mellon.

Xiao said the bug may have exposed nearly every cell phone customer in the US and Canada, some 200 million customers.

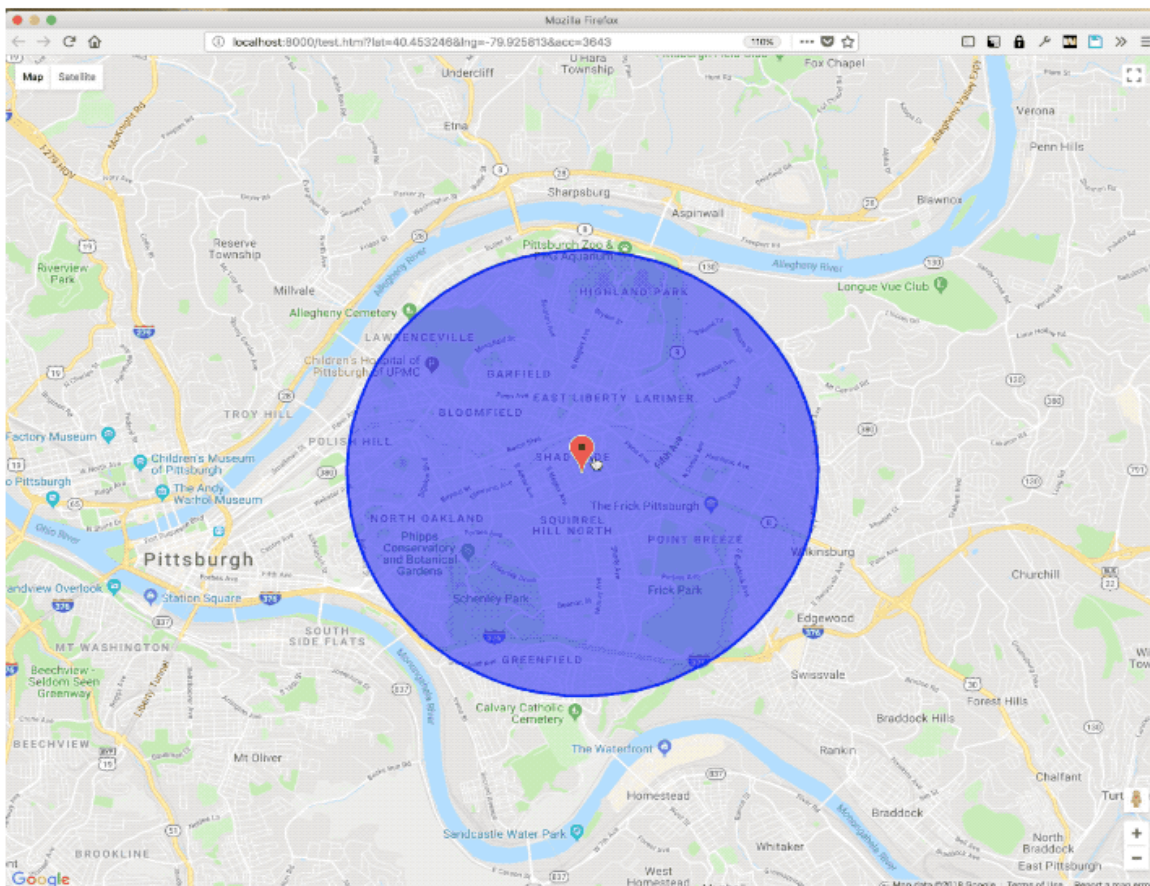
The researcher said he started looking at LocationSmart's website [following ZDNet's report](https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/) (<https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/>) this week, which followed a story from *The New York Times* (<https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>) that revealed how a former police sheriff snooped on phone location data from Securus, a customer of LocationSmart, without a warrant.

The sheriff has pleaded not guilty to charges of unlawful surveillance.

Xiao said one of the APIs used in the "try" page that allowed users to try the location feature out was not validating the consent response properly. Xiao said it was "trivially easy" to skip the part where the API sends the text message to the user to obtain their consent.

"It's a surprisingly simple bug," he said.

Xiao showed *ZDNet* a video of a script he built exploiting the bug in the company's API.



LocationSmart did not immediately respond to a request for comment.



Xiao verified the bug with a few people he knew. Brian Krebs, who [first reported the story](https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/) (<https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/>) earlier today, also verified the bug with several people who allowed him to test the bug.

"None of them got any notification that their location was being tracked," he said.

"I had a friend who was driving around Hawaii and [with permission] pinged the location and I could watch the marker move around the island," he said. "It's the kind of thing that sends chills down your spine."

Sen. Ron Wyden (D-OR), who last week called on the cell carriers to stop sharing data with third parties, offered a statement.

"This leak, coming only days after the lax security at Securus was exposed, demonstrates how little companies throughout the wireless ecosystem value Americans' security," said Wyden.

"It represents a clear and present danger, not just to privacy but to the financial and personal security of every American family. Because they value profits above the privacy and safety of the Americans whose locations they traffic in, the wireless carriers and LocationSmart appear to have allowed nearly any hacker with a basic knowledge of websites to track the location of any American with a cell phone," he said.

Wyden said the dangers from LocationSmart and other companies "are limitless."

"If the FCC refuses to act after this revelation then future crimes against Americans will be the commissioners' heads," he said.

We reached out to the cell providers -- AT&T, Verizon, and Sprint -- which all said they were investigating. T-Mobile did not respond to a request for comment.

But this newly disclosed bug shows the carriers are yet to cut off access -- if at all.

**Contact me securely** (<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

Zack Whittaker can be reached securely on Signal and WhatsApp at 646-755-8849, and his PGP fingerprint for email is: 4D0E 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.