Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site

Published: 2018-05-19 · Archived: 2026-04-05 18:04:16 UTC

LocationSmart, a U.S. based company that acts as an aggregator of real-time data about the precise location of mobile phone devices, has been leaking this information to anyone via a buggy component of its Web site — *without the need for any password or other form of authentication or authorization* — KrebsOnSecurity has learned. The company took the vulnerable service offline early this afternoon after being contacted by KrebsOnSecurity, which verified that it could be used to reveal the location of any **AT&T**, **Sprint**, **T-Mobile** or **Verizon** phone in the United States to an accuracy of within a few hundred yards.

On May 10, *The New York Times* broke the news that a different cell phone location tracking company called **Securus Technologies** had been selling or giving away location data on customers of virtually any major mobile network provider to a sheriff's office in Mississippi County, Mo.

On May 15, *ZDnet.com* ran a piece saying that Securus was getting its data through an intermediary — Carlsbad, CA-based LocationSmart.

Wednesday afternoon *Motherboard* published another bombshell: A hacker had broken into the servers of Securus and stolen 2,800 usernames, email addresses, phone numbers and hashed passwords of authorized Securus users. Most of the stolen credentials reportedly belonged to law enforcement officers across the country — stretching from 2011 up to this year.

Several hours before the Motherboard story went live, KrebsOnSecurity heard from **Robert Xiao**, a security researcher at **Carnegie Mellon University** who'd read the coverage of Securus and LocationSmart and had been poking around a demo tool that LocationSmart makes available on its Web site for potential customers to try out its mobile location technology.

LocationSmart's demo is a free service that allows anyone to see the approximate location of their own mobile phone, just by entering their name, email address and phone number into a form on the site. LocationSmart then texts the phone number supplied by the user and requests permission to ping that device's nearest cellular network tower.

Once that consent is obtained, LocationSmart texts the subscriber their approximate longitude and latitude, plotting the coordinates on a Google Street View map. [It also potentially collects and stores a great deal of technical data about your mobile device. For example, according to their privacy policy that information "may include, but is not limited to, device latitude/longitude, accuracy, heading, speed, and altitude, cell tower, Wi-Fi access point, or IP address information"].

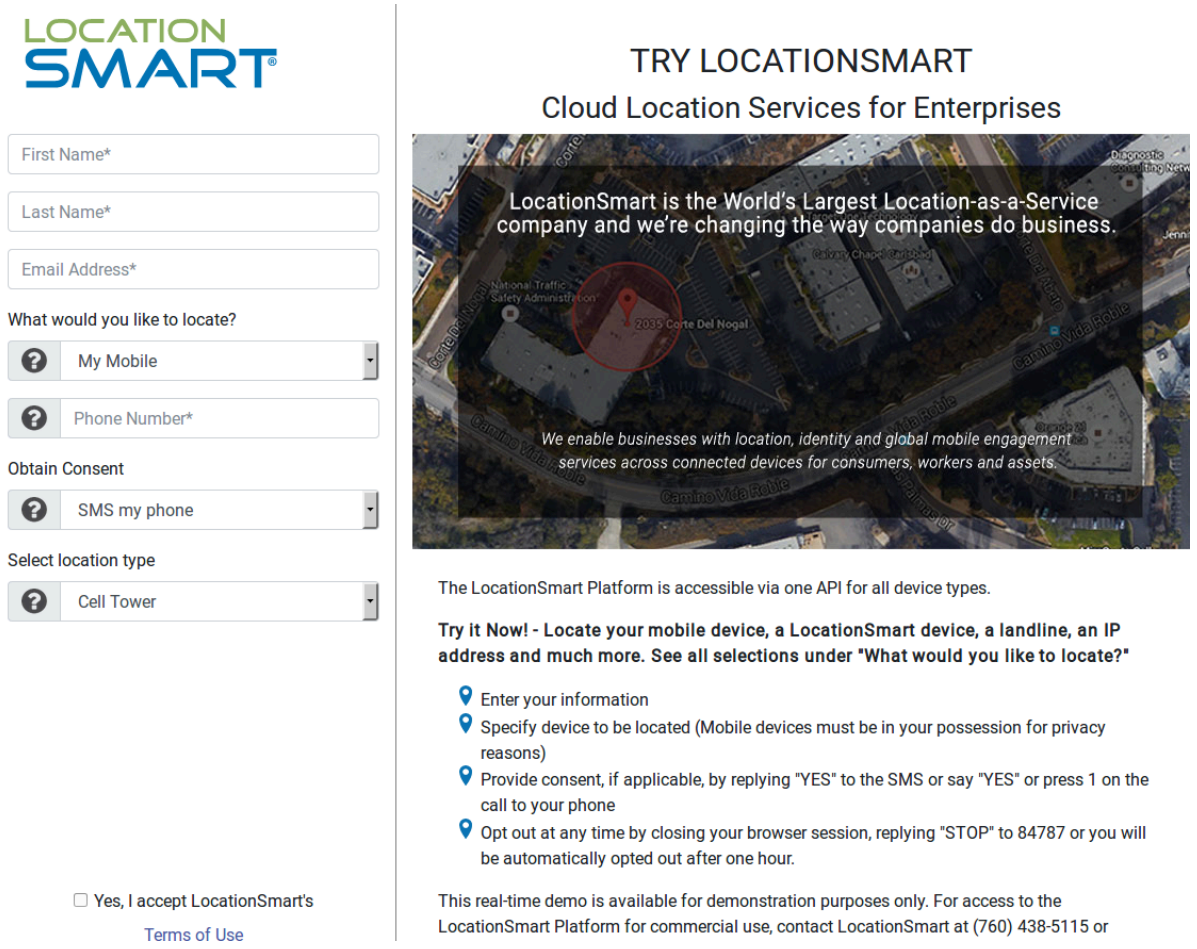
But according to **Xiao**, a PhD candidate at **CMU's** Human-Computer Interaction Institute, this same service failed to perform basic checks to prevent anonymous and unauthorized queries. Translation: Anyone with a modicum of knowledge about how Web sites work could abuse the LocationSmart demo site to figure out how to conduct mobile number location lookups at will, *all without ever having to supply a password or other credentials*.

"I stumbled upon this almost by accident, and it wasn't terribly hard to do," Xiao said. "This is something anyone could discover with minimal effort. And the gist of it is I can track most peoples' cell phone without their consent."

Xiao said his tests showed he could reliably query LocationSmart's service to ping the cell phone tower closest to a subscriber's mobile device. Xiao said he checked the mobile number of a friend several times over a few minutes while that friend was moving and found he was then able to plug the coordinates into Google Maps and track the friend's directional movement.

"This is really creepy stuff," Xiao said, adding that he'd also successfully tested the vulnerable service against one **Telus Mobility** mobile customer in Canada who volunteered to be found.

Before LocationSmart's demo was taken offline today, KrebsOnSecurity pinged five different trusted sources, all of whom gave consent to have Xiao determine the whereabouts of their cell phones. Xiao was able to determine within a few seconds of querying the public LocationSmart service the near-exact location of the mobile phone belonging to all five of my sources.



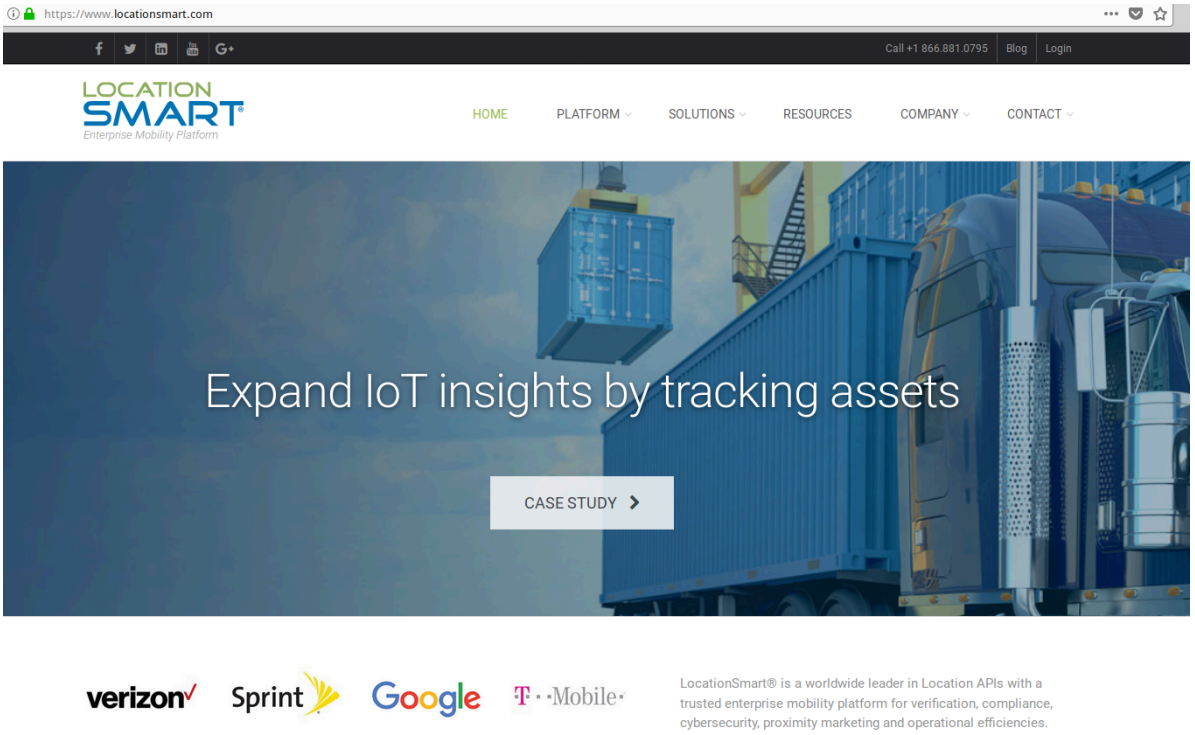
LocationSmart's demo page.

One of those sources said the longitude and latitude returned by Xiao's queries *came within 100 yards of their then-current location*. Another source said the location found by the researcher was 1.5 miles away from his current location. The remaining three sources said the location returned for their phones was between approximately 1/5 to 1/3 of a mile at the time.

Reached for comment via phone, LocationSmart Founder and CEO **Mario Proietti** said the company was investigating.

"We don't give away data," Proietti said. "We make it available for legitimate and authorized purposes. It's based on legitimate and authorized use of location data that only takes place on consent. We take privacy seriously and we'll review all facts and look into them."

LocationSmart's home page features the corporate logos of all four the major wireless providers, as well as companies like **Google**, **Neustar**, **ThreatMetrix**, and **U.S. Cellular**. The company says its technologies help businesses keep track of remote employees and corporate assets, and that it helps mobile advertisers and marketers serve consumers with "geo-relevant promotions."



LocationSmart's home page lists many partners.

It's not clear exactly how long LocationSmart has offered its demo service or for how long the service has been so permissive; this link from archive.org suggests it dates back to at least January 2017. This link from The Internet Archive suggests the service may have existed under a different company name — loc-aid.com — since mid-2011, but it's unclear if that service used the same code. Loc-aid.com is one of four other sites hosted on the same server as locationsmart.com, according to Domaintools.com.

LocationSmart's privacy policy says the company has security measures in place…"to protect our site from the loss or misuse of information that we have collected. Our servers are protected by firewalls and are physically located in secure data facilities to further increase security. While no computer is 100% safe from outside attacks, we believe that the steps we have taken to protect your personal information drastically reduce the likelihood of security problems to a level appropriate to the type of information involved."

But these assurances may ring hollow to anyone with a cell phone who's concerned about having their physical location revealed at any time. The component of LocationSmart's Web site that can be abused to look up mobile location data at will is an insecure "application programming interface" or API — an interactive feature designed to display data in response to specific queries by Web site visitors.

> Although the LocationSmart's demo page required users to consent to having their phone located by the service, LocationSmart apparently did nothing to prevent or authenticate direct interaction with the API itself.

Although the LocationSmart's demo page required users to consent to having their phone located by the service, LocationSmart apparently did nothing to prevent or authenticate direct interaction with the API itself.

API authentication weaknesses are not uncommon, but they can lead to the exposure of sensitive data on a great many people in a short period of time. In April 2018, KrebsOnSecurity broke the story of an API at the Web site of fast-casual bakery chain **PaneraBread.com** that exposed the names, email and physical addresses, birthdays and last four digits of credit cards on file for tens of millions of customers who'd signed up for an account at PaneraBread to order food online.

In a May 9 letter sent to the top four wireless carriers and to the **U.S. Federal Communications Commission** in the wake of revelations about Securus' alleged practices, **Sen. Ron Wyden** (D-Ore.) urged all parties to take "proactive steps to prevent the unrestricted disclosure and potential abuse of private customer data."

"Securus informed my office that it purchases real-time location information on AT&T's customers — through a third party location aggregator that has a commercial relationship with the major wireless carriers — and routinely shares that information with its government clients," Wyden wrote. "This practice skirts wireless carrier's legal obligation to be the sole conduit by which the government may conduct surveillance of Americans' phone records, and needlessly exposes millions of Americans to potential abuse and unchecked surveillance by the government."

Securus, which reportedly gets its cell phone location data from LocationSmart, told *The New York Times* that it requires customers to upload a legal document — such as a warrant or affidavit — and to certify that the activity was authorized. But in his letter, Wyden said "senior officials from Securus have confirmed to my office that it never checks the legitimacy of those uploaded documents to determine whether they are in fact court orders and has dismissed suggestions that it is obligated to do so."

Securus did not respond to requests for comment.

THE CARRIERS RESPOND

It remains unclear what, if anything, AT&T, Sprint, T-Mobile and Verizon plan to do about any of this. A third-party firm leaking customer location information not only would almost certainly violate each mobile providers own stated privacy policies, but the real-time exposure of this data poses serious privacy and security risks for virtually all U.S. mobile customers (and perhaps beyond, although all my willing subjects were inside the United States).

None of the major carriers would confirm or deny a formal business relationship with LocationSmart, despite LocationSmart listing them each by corporate logo on its Web site.

AT&T spokesperson **Jim Greer** said AT&T does not permit the sharing of location information without customer consent or a demand from law enforcement.

"If we learn that a vendor does not adhere to our policy we will take appropriate action," Greer said.

T-Mobile referred me to their privacy policy, which says T-Mobile follows the "best practices" document (PDF) for subscriber location data as laid out by the **CTIA**, the international association for the wireless telecommunications industry.

A T-Mobile spokesperson said that after receiving Sen. Wyden's letter, the company quickly shut down any transaction of customer location data to Securus and LocationSmart.

"We take the privacy and security of our customers' data very seriously," the company said in a written statement. "We have addressed issues that were identified with Securus and LocationSmart to ensure that such issues were resolved and our customers' information is protected. We continue to investigate this."

Verizon also referred me to their privacy policy.

Sprint officials shared the following statement:

> "Protecting our customers' privacy and security is a top priority, and we are transparent about our Privacy Policy. To be clear, we do not share or sell consumers' sensitive information to third parties. We share personally identifiable geo-location information only with customer consent or in response to a lawful request such as a validated court order from law enforcement."
>
> "We will answer the questions raised in Sen. Wyden's letter directly through appropriate channels. However, it is important to note that Sprint's relationship with Securus does not include data sharing, and is limited to supporting efforts to curb unlawful use of contraband cellphones in correctional facilities."

WHAT NOW?

Stephanie Lacambra, a staff attorney with the the nonprofit Electronic Frontier Foundation, said that wireless customers in the United States cannot opt out of location tracking by their own mobile providers. For starters, carriers constantly use this information to provide more reliable service to the customers. Also, by law wireless companies need to be able to ascertain at any time the approximate location of a customer's phone in order to comply with emergency 911 regulations.

But unless and until Congress and federal regulators make it more clear how and whether customer location information can be shared with third-parties, mobile device customers may continue to have their location information potentially exposed by a host of third-party companies, Lacambra said.

"This is precisely why we have lobbied so hard for robust privacy protections for location information," she said. "It really should be only that law enforcement is required to get a warrant for this stuff, and that's the rule we've been trying to push for."

Chris Calabrese is vice president of the Center for Democracy & Technology, a policy think tank in Washington, D.C. Calabrese said the current rules about mobile subscriber location information are governed by the Electronic Communications Privacy Act (ECPA), a law passed in 1986 that hasn't been substantially updated since.

"The law here is really out of date," Calabrese said. "But I think any processes that involve going to third parties who don't verify that it's a lawful or law enforcement request — and that don't make sure the evidence behind that request is legitimate — are hugely problematic and they're major privacy violations."

"I would be very surprised if any mobile carrier doesn't think location information should be treated sensitively, and I'm sure none of them want this information to be made public," Calabrese continued. "My guess is the carriers are going to come down hard on this, because it's sort of their worst nightmare come true. We all know that cell phones are portable tracking devices. There's a sort of an implicit deal where we're okay with it because

we get lots of benefits from it, but we all also assume this information should be protected. But when it isn't, that presents a major problem and I think these examples would be a spur for some sort of legislative intervention if they weren't fixed very quickly."

For his part, Xiao says we're likely to see more leaks from location tracking companies like Securus and LocationSmart as long as the mobile carriers are providing third party companies *any* access to customer location information.

"We're going to continue to see breaches like this happen until access to this data can be much more tightly controlled," he said.

Sen. Wyden issued a statement on Friday in response to this story:

> "This leak, coming only days after the lax security at Securus was exposed, demonstrates how little companies throughout the wireless ecosystem value Americans' security. 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."
>
> "The threats to Americans' security are grave – 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 cell phone to know when they were alone. 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."

Sen. Mark Warner (D-Va.) also issued a statement:

"This is one of many developments over the last year indicating that consumers are really in the dark on how their data is being collected and used," Sen. Warner said. "It's more evidence that we need 21st century rules that put users in the driver's seat when it comes to the ways their data is used."

In a statement provided to KrebsOnSecurity on Friday, LocationSmart said:

> "LocationSmart provides an enterprise mobility platform that strives to bring secure operational efficiencies to enterprise customers. All disclosure of location data through LocationSmart's platform relies on consent first being received from the individual subscriber. The vulnerability of the consent mechanism recently identified by Mr. Robert Xiao, a cybersecurity researcher, on our online demo has been resolved and the demo has been disabled. We have further confirmed that the vulnerability was not exploited prior to May 16th and did not result in any customer information being obtained without their permission."
>
> "On that day as many as two dozen subscribers were located by Mr. Xiao through his exploitation of the vulnerability. Based on Mr. Xiao's public statements, we understand that those subscribers were located only after Mr. Xiao personally obtained their consent. LocationSmart is continuing its efforts to verify that not a single subscriber's location was accessed without their consent and that no other

> vulnerabilities exist. LocationSmart is committed to continuous improvement of its information privacy and security measures and is incorporating what it has learned from this incident into that process."

It's not clear who LocationSmart considers "customers" in the phrase, "did not result in any customer information being obtained without their permission," since anyone whose location was looked up through abuse of the service's buggy API could not fairly be considered a "customer."

Update, May 18, 11:31 AM ET: Added comments from Sens. Wyden and Warner, as well as updated statements from LocationSmart and T-Mobile.
