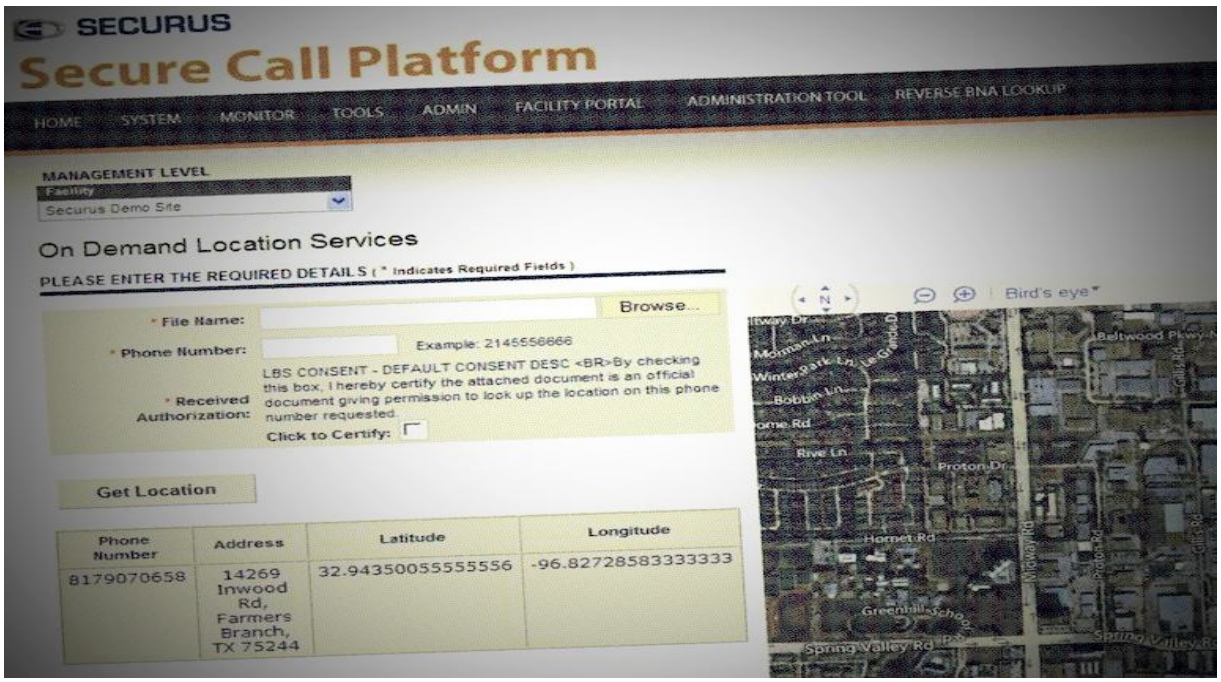
MUST READ US CELL CARRIERS ARE SELLING ACCESS TO YOUR REAL-TIME PHONE LOCATION DATA

US cell carriers are selling access to your real-time phone location data

The company embroiled in a privacy row has "direct connections" to all major US wireless carriers, including AT&T, Verizon, T-Mobile, and Sprint -- and Canadian cell networks, too.

By Zack Whittaker for Zero Day | May 14, 2018 -- 19:00 GMT (12:00 PDT)



(Screenshot: ZDNet. Source: State of Georgia

Four of the largest cell giants in the US are selling your real-time location data to a company that you've probably never heard about before.

In case you missed it, a senator last week sent a letter (https://www.zdnet.com/article/securus-police-cell-phones-warrantless-tracking/) demanding the Federal Communications Commission (FCC) investigate why Securus, a prison technology company, can track any phone "within seconds" by using data obtained from the country's largest cell giants, including AT&T, Verizon, T-Mobile, and Sprint, through an intermediary, LocationSmart.

The story blew up because a former police sheriff snooped on phone location data without a warrant, according *The New York Times* (https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html). The sheriff has pleaded not guilty to charges of unlawful surveillance.

Yet little is known about how LocationSmart obtained the real-time location data on millions of Americans, how the required consent from cell user owners was obtained, and who else has access to the data.

Kevin Bankston, director of New America's Open Technology Institute, explained in a phone call that the Electronic Communications Privacy Act only restricts telecom companies from disclosing data to the government. It doesn't restrict disclosure to other companies, who then may disclose that same data to the government.

He called that loophole "one of the biggest gaps in US privacy law."

"The issue doesn't appear to have been directly litigated before, but because of the way that the law only restricts disclosures by these types of companies to government, my fear is that they would argue that they can do a pass-through arrangement like this," he said.

LocationSmart, a California-based technology company, is one of a handful of so-called data aggregators. It claimed to have "direct connections" (https://archive.li/THily) to cell carrier networks to obtain real-time cell phone location data from nearby cell towers. It's less accurate than using GPS, but cell tower data won't drain a phone battery and doesn't require a user to install an app. Verizon, one of many cell carriers that sells access to its vast amounts of customer location data, counts LocationSmart as a close partner (https://archive.li/tCLrd).

The company boasts coverage of 95 percent of the country, thanks to its access to all the major US carriers, including US Cellular, Virgin, Boost, and MetroPCS, as well as Canadian carriers, like Bell, Rogers, and Telus.

"We utilize the same technology used to enable emergency assistance and this includes cell tower and cell sector location, assisted GPS and cell tower trilateration," said a case study on the company's website.

"With these location sources, we are able to locate virtually any US based mobile devices," the company claimed.

A person's precise location can be returned in as little as 15 seconds, according to another case study, and data is usually not cached for longer than two minutes.

Other companies then buy access to LocationSmart's data -- or the data is obtained by a customer of LocationSmart, like 3Cinteractive, which is said to have supplied location data to Securus.

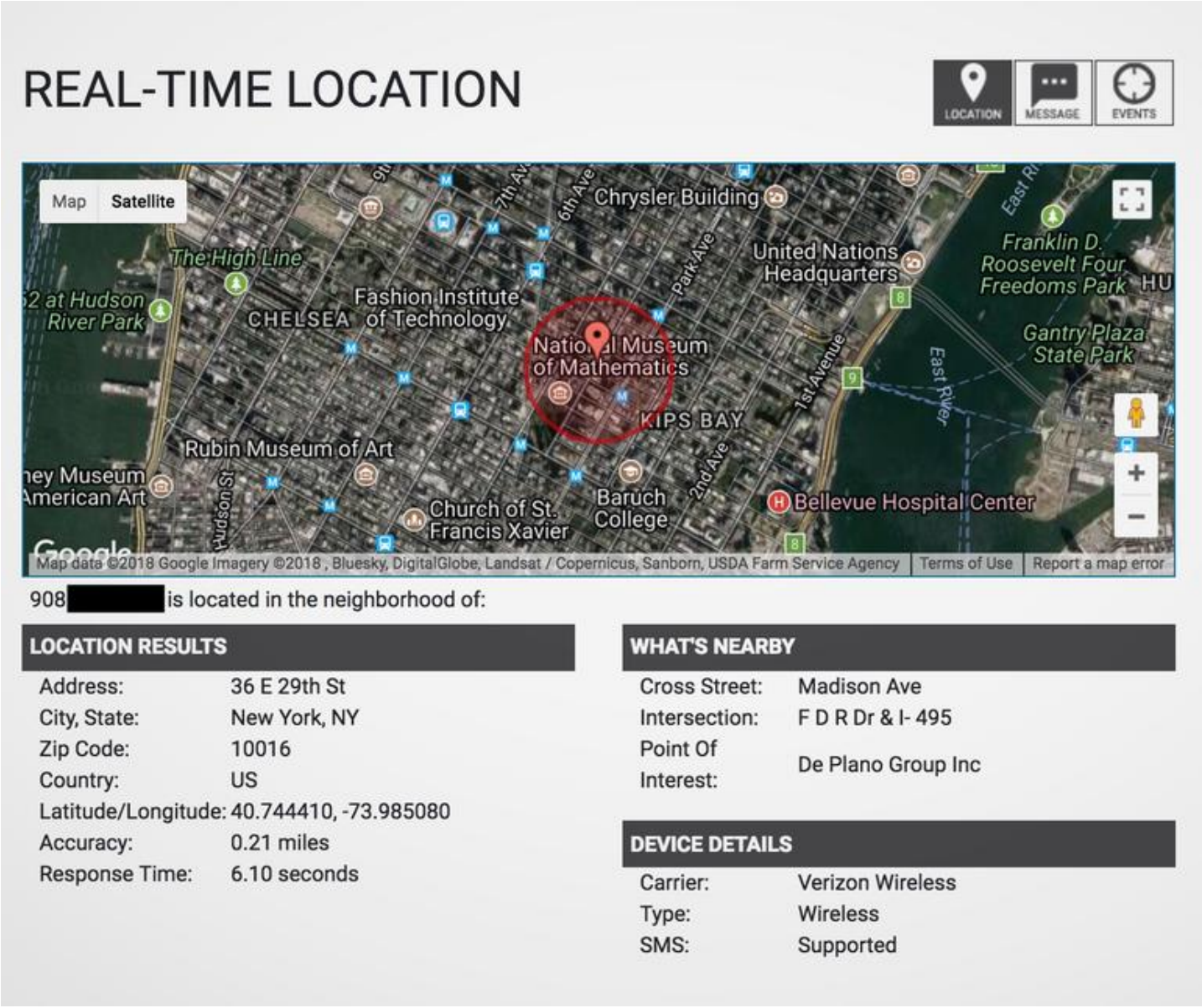
But LocationSmart hasn't said how it ensures its corporate customers protect the location data to prevent abuse and misuse. A spokesperson for LocationSmart did not return an email with several questions sent prior to publication.

Companies buy into LocationSmart's location data for many reasons. Sometimes it's to help locate a nearby store, or to send a marketing text message when a person visits a rival store. Location data can even be used by companies to track deliveries or shipments, or by banks to fight fraud, such as if a person is making card transactions miles apart within just a few minutes of each other.

In any case, the company requires explicit consent (https://archive.li/TmOa6) from the user before their location data can be used, by sending a one-time text message or allowing a user to hit a button in an app.

LocationSmart also said it allows some customers to obtain "implied" consent, used on a case-by-case basis, when "the nature of the service implies that location will be used." The company said one example could be when a stranded motorist calls roadside assistance, and the event implies the person is "calling to be found."

The company even has its own "try-before-you-buy" page (https://www.locationsmart.com/try/) that lets you test the accuracy of its data. With a colleague's consent, we tracked his phone to within a city block of his actual location.



(Screenshot: ZDNet)

The data aggregator said it has access (https://archive.li/TmOa6) to carrier network location data "because privacy is built into its cloud-based platform."

While that may be true, the requirement to obtain a person's consent collapses if a search warrant for that data is issued. That's exactly how companies like Securus can reveal location data without asking a person's permission.

According to a Nebraska state government document (http://das.nebraska.gov/materiel/purchasing/5289/5289%20centurylink%20proposal%202%20alternate.pdf), an application "can also be configured -- with carrier approval and appropriate warrant documentation -- to retrieve location data without the user opting-in." Securus was able to return real-time location data on users without their consent because the system required a valid order be submitted first.

However, as the *The New York Times* reported (https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html), Securus never verified orders before spitting back results.

We reached out to the four major US carriers prior to publication. We asked how each carrier obtains consent from customers to sell their data and what safeguards they put in place to prevent abuse.

Sprint spokesperson Lisa Belot said the company shares personally identifiable location data "only with customer consent or in response to a lawful request such as a validated court order from law enforcement."

The company's privacy policy (https://www.sprint.com/en/legal/sprint-corporation-privacy-policy.html#infoshare), which governs customer consent, said third-parties may collect customers' personal data, "including location information."

Sprint said the company's relationship with Securus "does not include data sharing," and is limited "to supporting efforts to curb unlawful use of contraband cell phones in correctional facilities."

When asked the same questions, Verizon spokesperson Rich Young provided a boilerplate response regarding Securus and would not comment further.

"We're still trying to verify their activities, but if this company is, in fact, doing this with our customers' data, we will take steps to stop it," he said.

AT&T spokesperson Jim Greer said in a statement: "We have a best practices approach to handling our customers' data. We are aware of the letter and will provide a response." Our questions were also not answered.

A spokesperson for T-Mobile did not respond by our deadline.

"It's important for us to close off that potential loophole and that can easily be done with one line of legislative language," said Bankston, "which would also have the benefit of making every other company careful about always getting consent before disclosing your data to anyone."

Ron Wyden, a Democratic senator from Oregon, called on each carrier to stop sharing data with third parties. Wyden argued the sharing "skirts wireless carriers' legal obligation to be the sole conduit by which the government may conduct surveillance of Americans' phone records."

In a blog post, Electronic Frontier Foundation (EFF) said law enforcement may be violating the law (https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-verizon.pdf) by not seeking data directly from the phone carriers. "Law enforcement shouldn't have unfettered access to this data, whether they get it from Securus or directly from the phone companies," said the EFF.

Wyden has also called on the FCC to investigate the carriers for allegedly not obtaining user consent.

The FCC has not said yet if it will investigate.

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.

Read More **(https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756)**