Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years

Documents show that bail bond companies used a secret phone tracking service to make tens of thousands of location requests.

By **Joseph Cox** | Feb 6 2019, 5:10pm

Image: Stuart Kinlough / Getty Images

In January, **Motherboard revealed** that AT&T, T-Mobile, and Sprint were selling their customers' real-time location data, which trickled down through a complex network of companies until eventually ending up in the hands of at least one bounty hunter. Motherboard was also able to purchase the real-time location of a T-Mobile phone on the black market from a bounty hunter source for $300. In response, telecom companies said that this abuse was a fringe case.

In reality, it was far from an isolated incident.

Around 250 bounty hunters and related businesses had access to AT&T, T-Mobile, and Sprint customer location data, with one bail bond firm using the phone location service more than 18,000 times, and others using it thousands or tens of thousands of times, according to internal documents obtained by Motherboard from a company called CerCareOne, a now-defunct location data seller that operated until 2017. The documents list not only the companies that had access to the data, but specific phone numbers that were pinged by those companies.

In some cases, the data sold is more sensitive than that offered by the service used by Motherboard last month, which estimated a location based on the cell phone towers that a phone connected to. CerCareOne sold cell phone tower data, but also sold highly sensitive and accurate GPS data to bounty hunters; an unprecedented move that means users could locate someone so accurately so as to see where they are inside a building. This company operated in near-total secrecy for over 5 years by making its customers

agree to “keep the existence of CerCareOne.com confidential,” according to a terms of use document obtained by Motherboard.

Some of these bounty hunters then resold location data to those unauthorized to handle it, according to two independent sources familiar with CerCareOne’s operations.

The news shows how widely available Americans’ sensitive location data was to bounty hunters. This ease-of-access dramatically increased the risk of abuse.

“This scandal keeps getting worse. Carriers assured customers location tracking abuses were isolated incidents. Now it appears that hundreds of people could track our phones, and they were doing it for years before anyone at the wireless companies took action,” Oregon Senator Ron Wyden said in an emailed statement after presented with Motherboard’s findings. “That’s more than an oversight—that’s flagrant, wilful disregard for the safety and security of Americans.”

Between at least 2012 until it closed in late 2017, CerCareOne allowed bounty hunters, bail bondsmen, and bail agents to find the real-time location of mobile phones. The company would sometimes charge up to $1,100 per phone location, according to a source familiar with the company. Motherboard granted a number of sources in this story anonymity to provide details about a controversial industry practice.

Like with the companies involved in Motherboard’s previous investigation, CerCareOne’s real-time location data trickled down first from telecom companies, and then to a so-called location aggregator called Locaid. From there, Locaid sold that data access to a number of different companies, including CerCareOne, which in turn sold it to its own clients. Locaid was purchased by a company called LocationSmart in 2015 . The documents Motherboard obtained indicate that LocationSmart continued to sell data to CerCareOne after it obtained Locaid, and LocationSmart confirmed that to Motherboard.

Often CerCareOne’s phone location service—known in the industry as a phone ping—would use data from cell towers and provide a Google Maps-style interface to the bounty hunter of the device’s approximate location.

But some of the data available to CerCareOne customers included a phone’s “assisted GPS” or A-GPS data, according to documents and screenshots of the service in action provided by two independent sources. A-GPS inherently relies on telecom company

information—it uses a phone's GPS chip in conjunction with information **gleaned from the telecom network** to locate a phone. It is used to locate cell phones that dial 911 in an emergency and it **operates faster than a phone's GPS chip alone**, which can sometimes take minutes to connect to a satellite, according to telecom filings with the Federal Communications Commission. Telecom companies have access to this data, according to letters and filings from telecom lawyers to FCC:

"Carriers and public safety have worked to develop technologies and standards that provide the best possible location estimate," a T-Mobile lawyer **wrote in a letter to the FCC in 2013**. "A-GPS is reasonably the foundation of wireless [emergency] 911 location for both indoor and outdoor locations."

A flow chart showing how AT&T, T-Mobile, and Sprint customers' location data ended up in the hands of around 250 bounty hunters and related businesses. Image: Motherboard

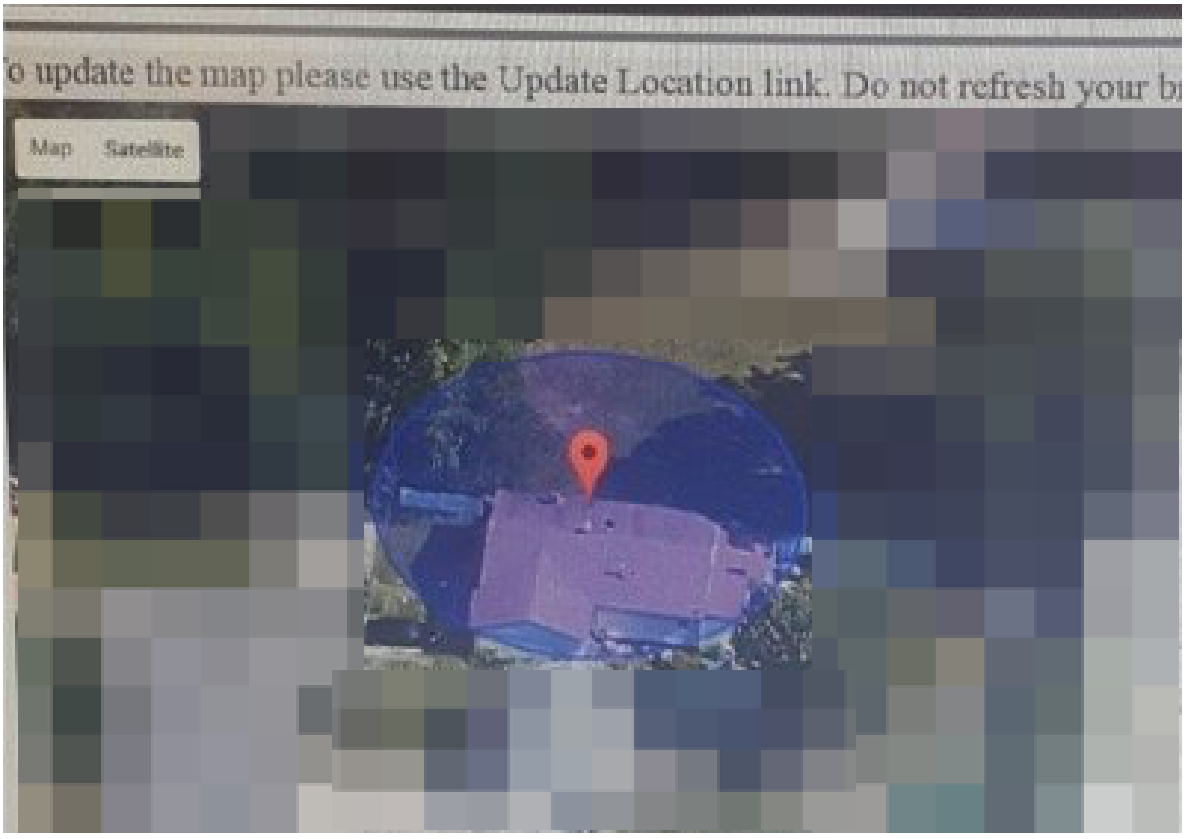
“Oftentimes A-GPS provides location information about where someone is *inside a building*,” Laura Moy, executive director at the Center on Privacy & Technology at

Georgetown University Law Center, told Motherboard in an email.

Blake Reid, associate clinical professor at Colorado Law, told Motherboard in an email that “with assisted GPS, your location can be triangulated within just a few meters. This allows constructing a detailed record of everywhere you travel.”

“The *only* reason we grant carriers any access to this information is to make sure that first responders are able to locate us in an emergency,” Reid added. “If the carriers are turning around and using that access to sell information to bounty hunters or whomever else, it is a shocking abuse of the trust that the public places in them to safeguard privacy while protecting public safety.”

Both Reid and Moy said this was the first instance of a telco selling A-GPS data they had heard of.



A screenshot obtained by Motherboard of a phone being located via its GPS data. Motherboard has blurred and cropped parts of the image to protect individuals’ privacy. Image: Motherboard

A LocationSmart spokesperson told Motherboard in an email “Carrier location services available through LocationSmart are based on a variety of technologies depending on

each carrier's particular location infrastructure implementation. That could include AGPS, cell tower, cell sector, or cell site trilateration. While there is no explicit indicator as to the technology used to provide a specific location response from a carrier, each response includes an accuracy estimate that can be used to infer the technology used."

A Sprint spokesperson did not directly answer whether the company has ever sold A-GPS data.

"The chips are inserted by the device manufacturers, and every major carrier offers devices with chips included. In fact, the FCC mandates that devices be GPS enabled," the company said in an email. "This is a necessary step to provide customers with services like rideshare services, GPS enabled maps, roadside assistance and 9-1-1 location service."

When asked if T-Mobile has sold A-GPS data, a company spokesperson told Motherboard in an email "We don't have anything further to add at this stage." AT&T did not respond to a request to clarify whether it sells or has ever sold A-GPS data.

None of the telecom companies specifically denied selling A-GPS data.

HUNTING AT SCALE

CerCareOne's phone tracking service was not a one-off tool for bounty hunters and bail agents. A list of a particular customer's phone pings obtained by Motherboard stretches on for around 450 pages, with more than 18,000 individual phone location requests in just over a year of activity. The bail bonds firm that initiated the pings did not respond to questions asking whether they obtained consent for locating the phones, or what the pings were for.

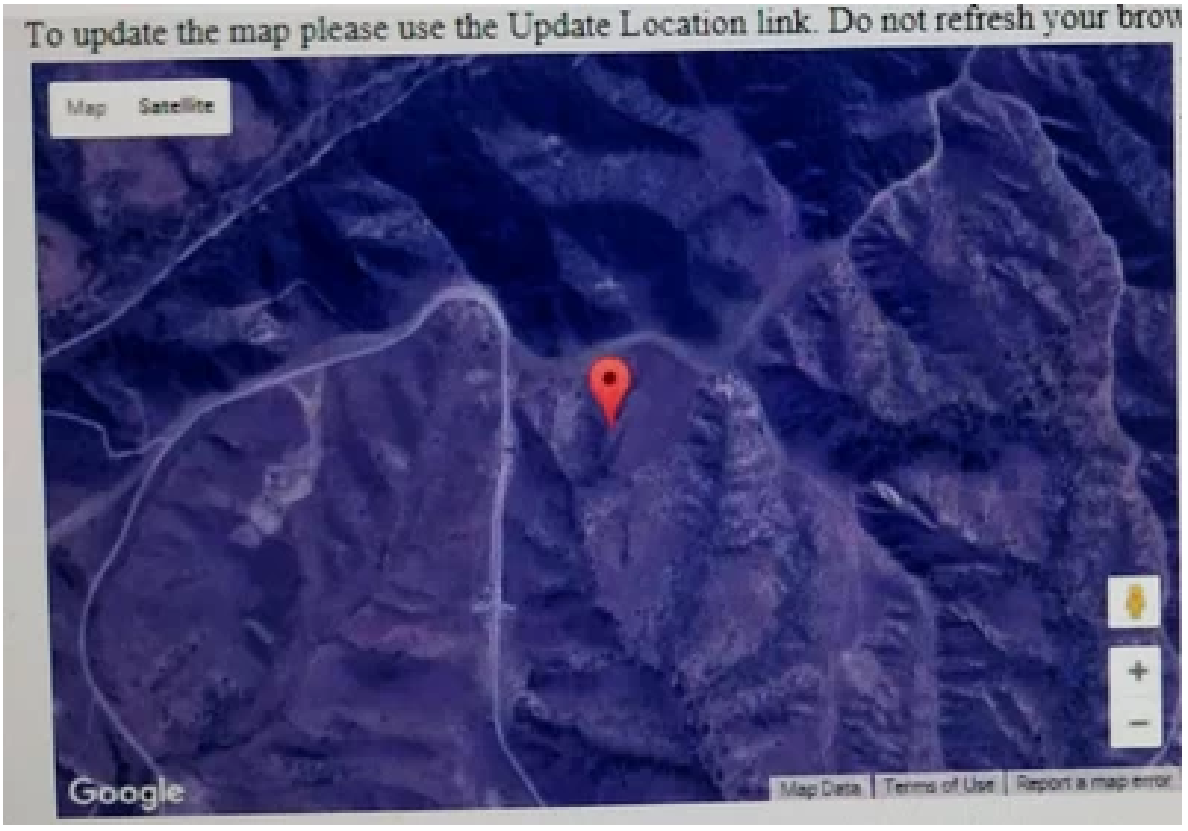
Another set of data is more than 250 pages long and covers around 10,000 phone pings. Another list of a different bounty hunter's activity includes nearly 1,000 phone location requests in less than a year; a third details more than 4,500 pings.

The location requests stretch from 2012 up to 2017, with some phones being located in quick succession multiple times over minutes, hours, and days, according to timestamps included in the documents.

“The scale of this abuse is outrageous,” Eva Galperin, director of cybersecurity at campaign group the Electronic Frontier Foundation, told Motherboard in an email.

Bail agents included in a CerCareOne customer list obtained by Motherboard defended their use of phone location data.

“This type [of] information is solely used for and extremely beneficial in locating and tracking wanted fugitives who have jumped bond and are also wanted by law enforcement for absconding from justice,” Charles Rhea Shaw III, a bail agent in Georgia whose information was included in the customer list, told Motherboard in an email.



A screenshot obtained by Motherboard of a phone being located via its cell tower data. Motherboard has cropped parts of the image to protect individuals’ privacy. Image: Motherboard

William Munck, another bail agent whose information was included in the CerCareOne data, wrote in an email “all of our contracts stipulate that in the event of a forfeiture (bond skip) we are authorized to used electronic phone location services on them.” In some cases, agents will have someone released on bail sign a contract saying that if they fail to repay their bail cost, the agent has authority to track them. Munck said he could not recall if he used CerCareOne’s services.

CerCareOne's terms and conditions claimed the company audited its systems to monitor for abuse.

Both agents said they had authority from their clients in their bail recovery contracts to use phone location services—Munck said they had to provide documentation to CerCareOne saying they had permission from the phone owner to track them; Shaw said they always "executed a privacy waiver."

A copy of CerCareOne's terms of use obtained by Motherboard says users are required to obtain written consent from those they wish to track.

> ***Got a tip? You can contact this reporter securely on Signal on +44 20 8133 5190, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.***

Two sources said target phones received no text message warning that they were being tracked. This leaves open the possibility for phones to be tracked without the target's knowledge or consent.

Telecom companies and location aggregators have previously told Motherboard that they require clients to obtain consent from people they wish to track. Sprint also said it requires aggregators to get permission to share its customers' data with another company; LocationSmart did not obtain this, Sprint said.

"We contractually require location aggregators to obtain prior written consent from Sprint 60 days before the use of any sub-aggregator, and we received no such request related to CerCareOne," a Sprint spokesperson wrote in an email.

A BOUNTY HUNTER'S SECRET

The existence of CerCareOne was a tightly held secret among the bounty hunter and bail community.

"The subscriber agrees to keep the existence of CerCareOne.com confidential by not communicating any information relating to same in any way, shape, or form and will not attempt *[sic]* make said site known to the public or business community under any circumstances or access will be terminated without notice," a copy of CerCareOne's terms of use, obtained by Motherboard, reads.

Visiting the CerCareOne domain at the time of writing brings up a site under construction message; that message has been on the landing page since at least 2013, according to online archives. However, visiting another specific URL reveals a login portal for the service.

Despite CerCareOne's secrecy, the company seems to originate from a much more public, almost brazen phone location service.

Motherboard found the CerCareOne website is hosted on the same IP address as another phone pinging service. Operational at the same time as CerCareOne, LocateUrCell.com offered to use telecom data to find phones for a wide array of purposes including finding lost elderly relatives and children, tracking down a misplaced phone, or monitoring employees.

In a local news report from 2011 by the *Naples Daily News*, LocateUrCell CEO Frank Rabbito claimed he used the service to help a woman find her lost phone in a supermarket parking lot. LocateURCell also worked with AT&T, T-Mobile, and Sprint phones, according to that article.

"With AT&T, Sprint and T-Mobile phones, LocateURcell.com utilizes GPS technology to track registered cell phones to within a few feet of their location," the article reads. "With Verizon, they use less-precise cellular triangulation technology."

A screenshot of CerCareOne's fake landing page. Image: Motherboard

Rabbito did not respond to a request for comment sent through AshleyNorman, a debt collection and skip-tracing (bounty hunting) service that he co-founded and still works at.

Munck, one of the bail agents in the CerCareOne data, told Motherboard that “years ago it was far easier to access this type of data.”

LocationSmart told Motherboard it cut ties with CerCareOne in 2017. Two independent sources said that CerCareOne is no longer in operation.

It seems likely Locaid, LocationSmart’s precursor, knew what CerCareOne was doing with cell phone location data. Included in the CerCareOne customer list obtained by Motherboard are Locaid email addresses, which could have been used to audit the service. When asked, LocationSmart didn’t dispute Motherboard’s speculation that these accounts may have been for auditing purposes, and said that theory is a fair one. But that raises more questions around why CerCareOne was allowed to operate for so many years.

A LocationSmart spokesperson told Motherboard in an email that this story "relates to a legacy Locaid customer relationship. LocationSmart acquired Locaid in 2015. In 2017, the customer did not meet the terms of LocationSmart's Master Services Agreement, and the contract was terminated." When asked why that contract was terminated, the spokesperson did not respond.

After Motherboard's original investigation, AT&T, T-Mobile, and Sprint **all said theywere going to** cut their relationships with location aggregators. In a statement, an AT&T spokesperson tried to downplay CerCareOne's significance.

"We are not aware of any misuse of this service which ended two years ago," an AT&T spokesperson wrote in an email, after Motherboard explicitly said the data was being provided to bounty hunters. "We've already decided to eliminate all location aggregation services—including those with clear consumer benefits—after reports of misuse by other location services involving aggregators."

Sprint's statement added, "As we previously announced, we [...] are in the process of ending our contracts with data aggregators for location based services."

T-Mobile declined to provide a new statement, and instead pointed to one it previously provided saying it is ending its relationships with location aggregators.

> "If the carriers are turning around and using that access to sell information to bounty hunters or whomever else, it is a shocking abuse of the trust that the public places in them to safeguard privacy while protecting public safety."

Even if CerCareOne is no longer operational, it still provides vital context on how American cell phone users' data has been sold and traded without their knowledge or proper consent.

"This is an issue of national and personal security," Jessica Rosenworcel, a commissioner at the Federal Communications Commission told Motherboard in an email. "The FCC needs to act with urgency. There have been press reports calling out the **sale of consumer location data since May**. I've asked for the letters of inquiry that typically kick off an investigation like this. They have not yet provided them."

Geoffrey Starks, another recently appointed commissioner of the FCC, told Motherboard in an email that “the for-profit location data industry has flourished in the shadows without any government oversight. The lights are starting to come on, and I believe that the FCC should use its authority to stop this practice, safeguard the public, and hold those responsible for this outrageous conduct accountable.”

On Friday, a spokesperson for the House Committee on Energy and Commerce told Motherboard the Committee had met with the FCC on the issue.

“In a bipartisan briefing with the FCC [on Friday], Committee staff reiterated their serious concerns about the wireless carriers’ unauthorized disclosure of real-time location data and urged the FCC to swiftly and thoroughly carry out its investigation,” the spokesperson wrote in an emailed statement.

After Motherboard’s original investigation, **15 senators called on the FCC and Federal Trade Commission** to investigate how consumers location data ended up in the hands of bounty hunters.

The FCC declined to answer specific questions about whether it knew of CerCareOne’s existence, and whether it was aware that CerCareOne was selling location data to bounty hunters.

“We are investigating carriers’ handling of location information, and we can’t comment on what facts we have uncovered in the middle of an active investigation,” an FCC spokesperson told Motherboard in an email.

> "The scale of this abuse is outrageous."

A Federal Trade Commission (FTC) spokesperson told Motherboard in an email that it “cannot comment on specific companies’ practices. And we generally do not comment on whether we are investigating a particular company.”

Senator Mark Warner, presented with Motherboard’s new findings, said in statement that “we have a systemic problem across the digital economy, where consumers remain totally in the dark about how their data is collected, sold or shared, and commercialized.”

“Whether it’s a major smartphone operating system tracking users’ every move, or a weather app selling users’ location data to hedge funds, or cell phone providers allowing intermediaries to sell smartphone location data to bounty hunters, we routinely see companies abusing consumer trust and we’re witnessing a complete failure of by the relevant agencies—the FCC and FTC—to address these practices,” he added.

Galperin from the EFF said that she’s “glad that the company is shut down, but that just leaves me to wonder how many more CerCareOnes we have out there.”

Subscribe to our new cybersecurity podcast, CYBER.

M

TAGGED: PRIVACY BOUNTY HUNTER CELL PHONE SURVEILLANCE SENATOR RON WYDEN T-MOBILE AT&T CELL PHONE TRACKING LOCATION SMART CERCAREONE