

**YOUR PHONE COMPANY SELLS
YOUR LOCATION TO YOUR
ENEMY**

**I Gave a Bounty Hunter \$300.
Then He Located Our Phone**

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

-  SHARE
-  TWEET

Nervously, I gave a bounty hunter a phone number. He had offered to geolocate a phone for me, using a shady, overlooked service intended not for the cops, but for private individuals and businesses. Armed with just the number and a few hundred dollars, he said he could find the current location of most phones in the United States.

The bounty hunter sent the number to his own contact, who would track the phone. The contact responded with a screenshot of Google Maps, containing a blue circle indicating the phone's current location, approximate to a few hundred metres.

Queens, New York. More specifically, the screenshot showed a location in a particular neighborhood—just a couple of blocks from where the target was. The hunter had found the phone (the target gave their consent to Motherboard to be tracked via their T-Mobile phone.)

The bounty hunter did this all without deploying a hacking tool or having any previous knowledge of the phone's whereabouts. Instead, the tracking tool relies on real-time location data sold to

bounty hunters that ultimately originated from the telcos themselves, including T-Mobile, AT&T, and Sprint, a Motherboard investigation has found. These surveillance capabilities are sometimes sold through word-of-mouth networks.

Whereas it's common knowledge that law enforcement agencies can track phones with a warrant to service providers, IMSI catchers, or until recently via other companies that sell location data [such as one called Securus](#), at least one company, called Microbilt, is selling phone geolocation services with little oversight to a spread of different private industries, ranging from car salesmen and property managers to bail bondsmen and bounty hunters, according to sources familiar with the company's products and company documents obtained by Motherboard. Compounding that already highly questionable business practice, this spying capability is also being resold to others on the black market who are not licensed by the company to use it, including me, seemingly without Microbilt's knowledge.

Motherboard's investigation shows just how exposed mobile networks and the data they generate are, leaving them open to surveillance by ordinary citizens, stalkers, and criminals, and comes as media and policy makers are paying more attention than ever to how location and other sensitive data [is collected and sold](#). The investigation also shows that a wide variety of companies can access cell phone location data, and that the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data.

"People are reselling to the wrong people," the bail industry source who flagged the company to Motherboard said.

Motherboard granted the source and others in this story anonymity to talk more candidly about a controversial surveillance capability.

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

Your mobile phone is constantly communicating with nearby cell phone towers, so your telecom provider knows where to route calls and texts. From this, telecom companies also work out the phone's approximate location based on its proximity to those towers.

Although many users may be unaware of the practice, telecom companies in the United States [sell access to their customers' location data](#) to other companies, called location aggregators, who then sell it to specific clients and industries. Last year, one location aggregator called LocationSmart faced harsh criticism for selling data that ultimately ended up in the hands of Securus, a company [which provided phone tracking to low level enforcement without requiring a warrant](#). LocationSmart also exposed the very data it was selling [through a buggy website panel](#), meaning anyone could geolocate nearly any phone in the United States at a click of a mouse.

There's a complex supply chain that shares some of American cell phone users' most sensitive data, with the telcos potentially being unaware of how the data is being used by the eventual end user, or even whose hands it lands in. Financial companies [use phone location data](#) to detect fraud; roadside assistance firms use it to locate stuck customers. But AT&T, for example, told Motherboard the use of its customers' data by bounty

hunters goes explicitly against the company's policies, raising questions about how AT&T allowed the sale for this purpose in the first place.

"The allegation here would violate our contract and Privacy Policy," an AT&T spokesperson told Motherboard in an email.

In the case of the phone we tracked, six different entities had potential access to the phone's data. T-Mobile shares location data with an aggregator called Zumigo, which shares information with Microbilt. Microbilt shared that data with a customer using its mobile phone tracking product. The bounty hunter then shared this information with a bail industry source, who shared it with Motherboard.

The CTIA, a telecom industry trade group of which AT&T, Sprint, and T-Mobile are members, has [official guidelines](#) for the use of so-called "location-based services" that "rely on two fundamental principles: user notice and consent," the group wrote in those guidelines. Telecom companies and data aggregators that Motherboard spoke to said that they require their clients to get consent from the people they want to track, but it's clear that this is not always happening.

microbilt_flowchart

A flowchart showing how the phone location data trickled down from T-Mobile to Motherboard. Image: Motherboard.

A second source who has tracked the geolocation industry told Motherboard, while talking about the industry generally, "If there is money to be made they will keep selling the data."

“Those third-level companies sell their services. That is where you see the issues with going to shady folks [and] for shady reasons,” the source added.

Frederike Kalthener, data exploitation programme lead at campaign group Privacy International, told Motherboard in a phone call that “it’s part of a bigger problem; the US has a completely unregulated data ecosystem.”

Microbilt buys access to location data from an aggregator called Zumigo and then sells it to a dizzying number of sectors, including landlords [to scope out potential renters](#); [motor vehicle salesmen](#), and others who are [conducting credit checks](#). Armed with just a phone number, Microbilt’s “Mobile Device Verify” product can return a target’s full name and address, geolocate a phone in an individual instance, or operate as a continuous tracking service.

“You can set up monitoring with control over the weeks, days and even hours that location on a device is checked as well as the start and end dates of monitoring,” a [company brochure Motherboard found online reads](#).

Posing as a potential customer, Motherboard explicitly asked a Microbilt customer support staffer whether the company offered phone geolocation for bail bondsmen. Shortly after, another staffer emailed with a price list—locating a phone can cost as little as \$4.95 each if searching for a low number of devices. That price gets even cheaper as the customer buys the capability to track more phones. Getting real-time updates on a phone’s location can cost around \$12.95.

“Dirt cheap when you think about the data you can get,” the source familiar with the industry added.

microbilt_pricelist

A section of the price list Motherboard obtained. Image: Motherboard.

It's bad enough that access to highly sensitive phone geolocation data is already being sold to a wide range of industries and businesses. But there is also an underground market that Motherboard used to geolocate a phone—one where Microbilt customers resell their access at a profit, and with minimal oversight.

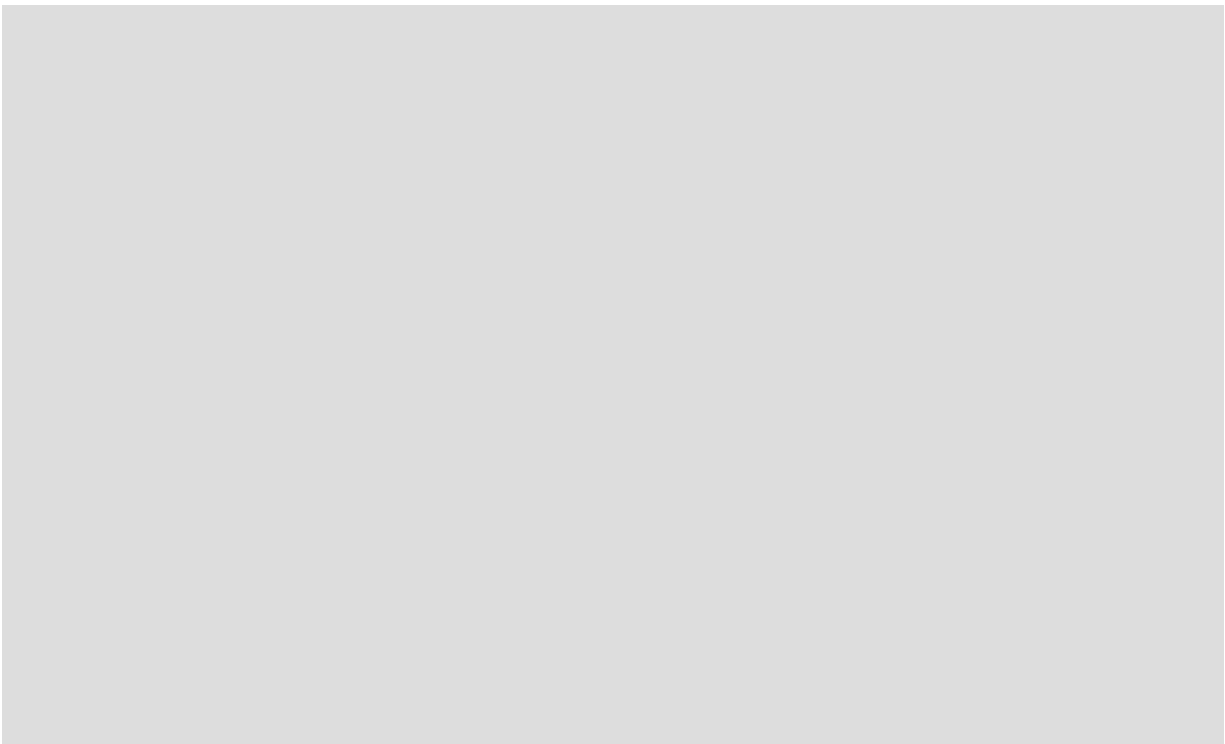
“Blade Runner, the iconic sci-fi movie, is set in 2019. And here we are: there's an unregulated black market where bounty-hunters can buy information about where we are, in real time, over time, and come after us. You don't need to be a replicant to be scared of the consequences,” Thomas Rid, professor of strategic studies at Johns Hopkins University, told Motherboard in an online chat.

The bail industry source said his middleman used Microbilt to find the phone. This middleman charged \$300, a sizeable markup on the usual Microbilt price. The Google Maps screenshot provided to Motherboard of the target phone's location also included its approximate longitude and latitude coordinates, and a range of how accurate the phone geolocation is: 0.3 miles, or just under 500 metres. It may not necessarily be enough to geolocate someone to a specific building in a populated area, but it can certainly pinpoint a particular borough, city, or neighborhood.

In other cases of phone geolocation it is typically done with the consent of the target, perhaps by sending a text message the user has to deliberately reply to, signalling they accept their location being tracked. This may be done in the earlier roadside assistance example or when a company monitors its fleet of trucks. But when Motherboard tested the geolocation service, the target phone received no warning it was being tracked.

The bail source who originally alerted Microbilt to Motherboard said that bounty hunters have used phone geolocation services for non-work purposes, such as tracking their girlfriends. Motherboard was unable to identify a specific instance of this happening, but domestic stalkers have repeatedly used technology, such as mobile phone malware, [to track spouses](#).

As Motherboard was reporting this story, Microbilt removed documents related to its mobile phone location product from its website.





A Microbilt spokesperson told Motherboard in a statement that the company requires anyone using its mobile device verification services for fraud prevention must first obtain consent of the consumer. Microbilt also confirmed it found an instance of abuse on its platform—our phone ping.

“The request came through a licensed state agency that writes in approximately \$100 million in bonds per year and passed all up front credentialing under the pretense that location was being verified to mitigate financial exposure related to a bond loan being considered for the submitted consumer,” Microbilt said in an emailed statement. In this case, “licensed state agency” is referring to a private bail bond company, Motherboard confirmed.

"As a result, MicroBilt was unaware that its terms of use were being violated by the rogue individual that submitted the request under false pretenses, does not approve of such use cases, and has a clear policy that such violations will result in loss of access to all MicroBilt services and termination of the requesting party's end-user agreement," Microbilt added. "Upon investigating the alleged abuse and learning of the violation of our contract, we terminated the customer's access to our products and they will not be eligible for reinstatement based on this violation."

Zumigo confirmed it was the company that provided the phone location to Microbilt and defended its practices. In a statement, Zumigo did not seem to take issue with the practice of providing data that ultimately ended up with licensed bounty hunters, but wrote, "illegal access to data is an unfortunate occurrence across virtually every industry that deals in consumer or employee data, and it is impossible to detect a fraudster, or rogue customer, who requests location data of his or her own mobile devices when the required consent is provided. However, Zumigo takes steps to protect privacy by providing a measure of distance (approx. 0.5-1.0 mile) from an actual address." Zumigo told Motherboard it has cut Microbilt's data access.

"People are reselling to the wrong people."

In Motherboard's case, the successfully geolocated phone was on T-Mobile.

"We take the privacy and security of our customers' information very seriously and will not tolerate any misuse of our customers' data," A T-Mobile spokesperson told Motherboard in an emailed statement. "While T-Mobile does not have a direct relationship

with Microbilt, our vendor Zumigo was working with them and has confirmed with us that they have already shut down all transmission of T-Mobile data. T-Mobile has also blocked access to device location data for any request submitted by Zumigo on behalf of Microbilt as an additional precaution.”

Microbilt’s product documentation suggests the phone location service works on all mobile networks, however the middleman was unable or unwilling to conduct a search for a Verizon device. Verizon did not respond to a request for comment.

AT&T told Motherboard it has cut access to Microbilt as the company investigates.

“We only permit the sharing of location when a customer gives permission for cases like fraud prevention or emergency roadside assistance, or when required by law,” the AT&T spokesperson said.

Sprint told Motherboard in a statement that “protecting our customers’ privacy and security is a top priority, and we are transparent about that in our Privacy Policy [...] Sprint does not have a direct relationship with MicroBilt. If we determine that any of our customers do and have violated the terms of our contract, we will take appropriate action based on those findings.” Sprint would not clarify the contours of its relationship with Microbilt.

These statements sound very familiar. When [The New York Times](#) and Senator Ron Wyden published details of Securus last year, the firm that was offering geolocation to low level law enforcement without a warrant, the telcos said they were taking extra measures to make sure their customers’ data would not be

abused again. Verizon announced it was going to limit data access to companies not using it for legitimate purposes. T-Mobile, Sprint, and AT&T [followed suit shortly after](#) with similar promises.

After Wyden's pressure, [T-Mobile's CEO John Legere tweeted](#) in June last year "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."

"It appears these promises were little more than worthless spam in their customers' inboxes."

Months after the telcos said they were going to combat this problem, in the face of an arguably even worse case of abuse and data trading, they are saying much the same thing. Last year, [Motherboard reported on a company](#) that previously offered phone geolocation to bounty hunters; here Microbilt is operating even after a wave of outrage from policy makers. In its statement to Motherboard on Monday, T-Mobile said it has nearly finished the process of terminating its agreements with location aggregators.



"It would be bad if this was the first time we learned about it. It's not. Every major wireless carrier pledged to end this kind of data sharing after I exposed this practice last year. Now it appears these promises were little more than worthless spam in their customers' inboxes," Wyden told Motherboard in a statement. Wyden [is proposing legislation](#) to safeguard personal data.

Due to the [ongoing government shutdown](#), the Federal Communications Commission (FCC) was unable to provide a statement.

“Wireless carriers’ continued sale of location data is a nightmare for national security and the personal safety of anyone with a phone,” Wyden added. “When stalkers, spies, and predators know when a woman is alone, or when a home is empty, or where a White House official stops after work, the possibilities for abuse are endless.”

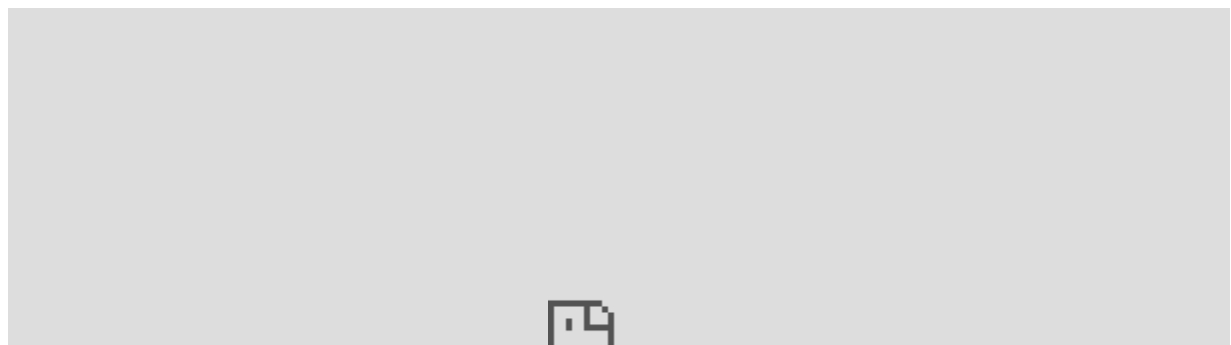
Subscribe to our new cybersecurity podcast, [CYBER](#).



-  SHARE
-  TWEET

- Tagged:
- [spying](#)
- [cybersecurity](#)
- [Bounty Hunter](#)
- [stalking](#)
- [Verizon](#)
- [T-Mobile](#)
- [AT&T](#)
- [securus](#)
- [microbilt](#)

Watch This Next





Where we're going, we don't need email.

Sign up for Motherboard Premium.

[I See You](#)

|

by [Joseph Cox](#)

|

Jun 22 2018, 6:19am

**Bail Bond Company Let
Bounty Hunters Track Verizon,
T-Mobile, Sprint, and AT&T
Phones for \$7.50**

Low-level enforcement were able to monitor phones nationwide with minimal legal oversight. But the predatory bail bonds industry provided a similar, and cheap, service to bounty hunters to track down individuals.

-  SHARE
-  TWEET



Image: Ann Hermes/The Christian Science Monitor via Getty Images

This week [Verizon and other major telcos announced](#) they would stop the sale of customers' location data to certain third parties. The move came after a wave of media reports and [scrutiny from Senator Ron Wyden](#), which showed that data was ultimately ending up in the hands of low-level law enforcement, letting them track nearly any phone in the US with minimal oversight.

But it wasn't just cops. Before going through what appears to be a serious rebranding and discontinuing the product, at least one company, Captira, was selling phone geolocation to another market, according to website archives: bounty hunters. The online records highlight the wide spread of use cases for phone location information; data that customers and ordinary citizens likely did not understand has been sold and re-used by multiple industries for years.

Captira caters to the bail bondsman market. That is, people who put money forward to pay for a criminal suspect's bail and demand a percentage of that bail amount as payment, and those who hunt down defendants to make sure they attend a court date. The industry has faced intense criticism due to concerns its for-profit motive [may push low-income defendants](#) into debt as they feel pressured to take money from a bondsman that they ultimately may not be able to pay back. In other words, [low-income defendants don't only end up in debt because they can't afford bail](#), but those who used bail bond agents could face a bounty hunter who then tracks their phone's location.

"There are two general ways in which we can harness technology: gaining knowledge and gaining efficiency. Of course, we can also seek to exploit new technology to gain a unique advantage," Matthew Phillips, CTO of Captira, [wrote in a 2014 article](#) in a trade publication.

Captira allowed customers to "instantly locate defendant cell phone," for as little as \$7.50, according to [a July 2011 archive](#) of the company's website. The "Cell Phone Locator" product worked on all major carriers, such as Verizon, AT&T, Sprint and T-Mobile, and displayed results in a Google Maps interface, the website adds.

Caption: A screenshot of Captira's previously offered cell phone locator product.

Another webpage unearthed by Motherboard shows Captira claiming its phone product could geolocate targets to an accuracy of 2 metres.

“This is especially useful for people who try to jump locations by changing cities in order to avert court hearings,” [another archive](#) discussing Captira’s products reads.

When using a [similar service called Securus](#), law enforcement officials were required to upload some sort of authorization document, such as a warrant, but [Securus previously confirmed](#) that it did not conduct any review of these surveillance requests. With Captira, it is not clear what steps customers had to take to access the service.

But Captira’s bounty hunter customers have successfully used the cell phone locator product to track down defendants, judging by Captira’s tweets.

“North Carolina agent chases a defendant through 3 states, using Cell Phone Locator the whole way. Finally caught at a truck stop,” [one tweet from the company](#) reads. Another [tweet claims a customer](#) used the product to catch a ‘skip’—[a wanted fugitive](#)—with a \$25,000 value.

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.

Today, Captira does not explicitly mention the cell phone locator service on its website, but the company does offer a number of other products, including the ability to comb through images [captured by nationwide license plate readers](#), potentially letting a user trace the historical movements of a particular vehicle across the country.

The cell phone locator product “was withdrawn approximately 6 years ago,” Phillips told Motherboard in an email. “Including Captira in any article will be misleading.” Phillips did not respond to a follow-up question asking why Captira scrapped the service.

But a source who has followed the industry of phone location products told Motherboard that several companies stopped advertising their geolocation products in around 2014 and 2015, perhaps due to increased concern that the services may have been illegal. Motherboard granted the source anonymity to talk about industry developments.

We don't know how Captira obtained data to track phones across all major telcos. LocationSmart, the company that provided location information to Securus, told Motherboard Captira did not obtain its telco data from LocationSmart, nor was Captira a customer of Locaid, a company that LocationSmart acquired in 2015. Zumigo, another location data company, and which Verizon recently mentioned as one of their main middlemen vendors, told Motherboard Captira was not a customer.

In tweets, Captira said it had obtained approval for its cell phone location service [from both Verizon and T-Mobile](#). Neither telco responded to questions on whether they gave Captira customer location data.



Senator Wyden, whose office investigated the sale and exploitation of phone location information, has [asked the Federal Communications Commission \(FCC\)](#) to investigate how companies such as Securus have abused such data, as well as what sort of customer consent each wireless carrier requires from other companies before providing location information.

The FCC [has referred reports](#) about LocationSmart to its enforcement bureau to formally investigate. Robert Xiao, a security researcher at Carnegie Mellon University, [discovered that LocationSmart ran a faulty website](#) that let anyone look up the location of nearly any phone in the US without authorization.

“For far too long, wireless companies sold sensitive location data about Americans to middlemen and then looked the other way when our information was abused. While I am glad to see the carriers have promised to start cleaning up the location data industry, I strongly doubt that Securus was the only company to abuse its access to Americans’ information,” Senator Wyden told Motherboard in a statement.

“It is long past time for the FCC to step up and actually go to work for American consumers, by investigating the shadowy marketplace for our private data. Consumers’ security and privacy shouldn’t be the last item on an agenda that seems larded with items designed to please corporate shareholders,” it added.

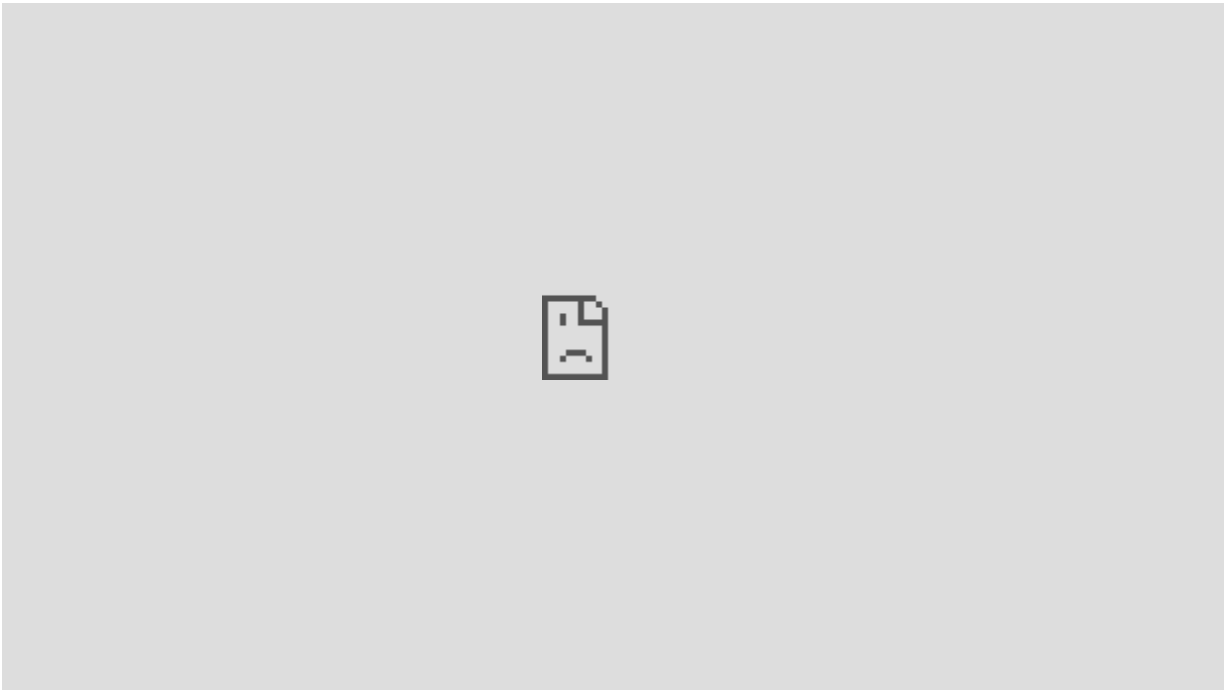


-  SHARE
-  TWEET

- Tagged:
- [SURVEILLANCE](#)
- [bounty_Hunters](#)
- [Verizon](#)
- [bail bondsman](#)
- [T-Mobile](#)
- [σπριγτ](#)

- [Cell Phone Tracking](#)
- [securus](#)
- [locationsmart](#)

Watch This Next



Where we're going, we don't need email.

Sign up for Motherboard Premium.

[trickle down](#)

|

by [Joseph Cox](#)

|

May 11 2018, 6:47am

Cops Can Find the Location of Any Phone in the Country in Seconds, and a Senator Wants to Know Why

Here are the letters Senator Ron Wyden sent to mobile carriers and the FCC demanding answers and action on the recently highlighted law enforcement service to easily track phones across the country.

-  SHARE
-  TWEET



Image: Shutterstock

On Thursday, [the New York Times published](#) a blockbuster piece revealing how US law enforcement have access to a system that can geo-locate nearly any phone in the country without an officer necessarily having a court order. Now, Motherboard has obtained the letters that Senator Ron Wyden sent to the Federal Communications Commission (FCC) and telecommunications companies demanding answers on the controversial surveillance system.

“I am writing to insist that AT&T take proactive steps to prevent the unrestricted disclosure and potential abuse of private customer data, including real-time location information, by at least one other company to the government,” [a May 8 letter sent from Wyden](#) to the President and Chief Executive Officer of AT&T reads.

According to the *New York Times* report, a former sheriff of Mississippi County, Mo., used an obscure service called Securus to surveil targets' cell phones, including a judge and other law enforcement officials. That system is typically used by marketers to obtain location data from mobile carriers. As well as AT&T, the system can exploit data from Sprint, T-Mobile, and Verizon, and law enforcement can essentially self-certify that they have legal authorisation to use the service, the report suggests.

In his letter to AT&T, which has similar text to letters sent to other carriers, Wyden writes that this check amounts of "nothing more than the legal equivalent of a pinky promise."

"The fact that Securus provides this service at all suggests that AT&T does not sufficiently control access to your customers' private information," the letter adds.

Wyden then lays out several steps for carriers to follow, such as undertaking an audit of each third party they sell customer data to, to determine how the company uses that data; notify customers whose location information was disclosed without their consent; terminate relationships with third parties that have misrepresented customer consent or abused their access to sensitive customer data; and provide a service for customers to view a list of third parties their data has been shared with.

"Americans should be able to obtain this information from wireless carriers, just as they can obtain from the consumer credit agencies a list of the private parties who have accessed their credit reports," the letter reads.

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.

In his [additional letter to the FCC](#), Wyden asks the department to “promptly investigate Securus, the wireless carriers’ failure to maintain exclusive control over law enforcement access to their customers’ location data, and also conduct a broad investigation into what demonstration of customer consent, if any, each wireless carrier requires from other companies before the carriers provide them with customer location information and other data.”

Tobias Engel, a security researcher and expert in mobile phone surveillance techniques, told Motherboard in an online chat “this is not about hacking at the core network level or mis-using technical services which were not designed to do this, but simply the US carriers selling out their subscribers.”

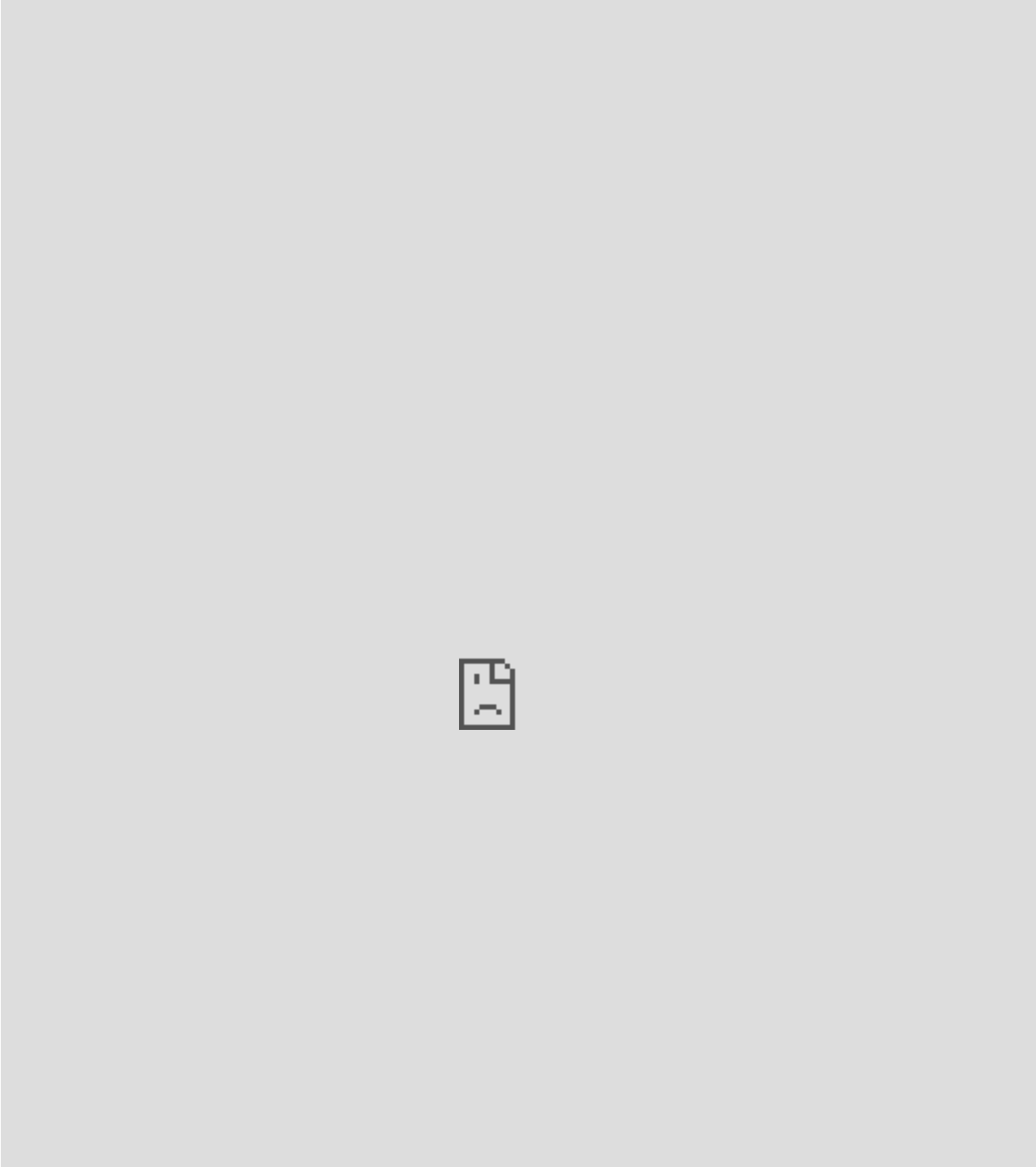
“LE [law enforcement] is piggybacking onto this ‘commercial’ option which seems to have a much lower entry barrier than if they requested this kind of access from the carriers themselves,” he added.

Nicholas Weaver, [a senior researcher](#) at the International Computer Science Institute at the University of California, Berkeley, told Motherboard in a Twitter message "This once again shows that data is like an oil spill: the contamination gets everywhere. The notion that a chain of 3+ companies, including one specifically intended for marketing, is able to resell access to everyone's real-time location with pretty high precision is disturbing but it shouldn't be surprising."

"In the US, we don't have legal protection against the misuse of our data outside limited categories. So for example, we do have



good protection on social security and (depending on the state) DMV info. But our utilities or anybody else not explicitly regulated will sell, resell, rebundle, repackage, and redistribute for practically any purpose they can," he added.

Here are the full letters:







-  SHARE
-  TWEET

- Tagged:
- [tracking](#)
- [SURVEILLANCE](#)
- [mobile_phone](#)
- [ron_wyden](#)
- [Geolocation](#)
- [AT&T](#)
- [σπρλντ](#)
- [securus](#)

Watch This Next

Where we're going, we don't need email.

Sign up for Motherboard Premium.

[BROKEN NETWORKS](#)

|

by [Joseph Cox](#)

|

Jun 19 2018, 9:14am

Verizon Says It Will Stop Selling US Phone Data That Ended Up in Hands of Cops

Verizon and other telcos have been selling phone location data to companies catering to marketers and low level law enforcement. Now, Verizon says it is cutting ties with certain firms that abused that data access.

-  SHARE
-  TWEET



Image: Shutterstock

Verizon says it will stop selling customers' phone location information to companies that have exposed such data, as well as ultimately passed it on to low level law enforcement. Verizon's data was included in products which allowed jail wardens and other officials to geolocate nearly any phone in the United States with minimal legal oversight.

The news signals what may be something of a shift in the telco industry, with a tightening of data that has been traded and exploited largely without customers' direct knowledge.

"We are initiating a process to terminate our existing agreements for the location aggregator program," [a letter](#), dated June 15 and released by Senator Ron Wyden's office on June 19, reads.

In May, [Wyden and The New York Times](#) exposed the practice of telcos selling customers location data. Specifically, they focused

on Securus, a firm allowing prison staff to check where an inmate was calling to. But that system was open to abuse: one case documented by *The New York Times* showed a former sheriff in Mississippi County, Missouri, has used the service to monitor judges and other law enforcement officials. The system did not necessarily require a court order; only some form of document showing that users believed they had legal authority to monitor the device.

And [as Motherboard reported](#), a hacker obtained user information from Securus's own servers, further highlighting the carelessness of companies entrusted with such sensitive data.

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.

"In the case of Securus Technologies, as soon as we determined that Securus was accessing location information for unauthorized purposes, we immediately blocked Securus's access to customer location information through our vendor LocationSmart," the letter from Verizon reads.

LocationSmart is the company that provided geolocation data to Securus. Shortly after the *Times* piece, [security journalist Brian Krebs as well as ZDNet reported](#) that LocationSmart's website was open to a serious vulnerability, where anyone could look up the real-time location of nearly any phone in the United States, for free, without any authorization.

"Use of location information for investigative purposes was not an approved use case in our agreement with LocationSmart,"

Verizon's letter adds. Verizon said it was also ending arrangements with another location buyer called Zumigo.

Verizon's letter to Wyden also spells out some other use cases of phone data, including financial institutions looking up a customer's location when they apply for a new credit card to help confirm their identity, and vehicle rental companies doing it to "provide better assistance to customers who experience problems on the road."

Verizon spokesperson Rich Young told Motherboard In a statement that "when these issues were brought to our attention, we took immediate steps to stop it. Customer privacy and security remain a top priority for our customers and our company. We stand-by [sic] that commitment to our customers."

Responses from AT&T, Sprint, and T-Mobile that Wyden's office also published indicate that those telcos have not yet ended their business relationships with LocationSmart.

Wyden said in a statement that Verizon "deserves credit for taking quick action to protect its customers' privacy and security."

"After my investigation and follow-up reports revealed that middlemen are selling Americans' location to the highest bidder without their consent, or making it available on insecure web portals, Verizon did the responsible thing and promptly announced it was cutting these companies off," Wyden said. "In contrast, AT&T, T-Mobile, and Sprint seem content to continuing to sell their customers' private information to these shady middle men, Americans' privacy be damned."



UPDATE: After Verizon's announcement, AT&T [also pledged](#) to stop selling customer's information.

A Securus spokesperson sent the following statement:

"Securus Technologies takes privacy and security extremely seriously and we are supportive of efforts to ensure individual data is protected. Under our contract with a third party that accesses location data from LocationSmart, Securus is authorized to provide law enforcement and correctional officials the approximate location of a mobile telephone, based on either consent by the called party or lawful process such as a search warrant or affidavit. Securus adheres to the terms of our contract and requires customers to acquire all legal approvals needed to access an individual's location. This information has been successfully used to locate missing children and adults suffering from dementia, as well preventing a planned escape attempt before it could be carried out. We believe that ending the ability of law enforcement to use these critical tools will hurt public safety and put Americans at risk."

Get six of our favorite Motherboard stories every day [by signing up for our newsletter](#).



-  SHARE
-  TWEET
- Tagged:
- [SURVEILLANCE](#)
- [senator ron wyden](#)
- [Verizon](#)

- [Cell Phone Tracking](#)
- [securus](#)
- [Securus Technologies](#)
- [locationsmart](#)

Watch This Next

Where we're going, we don't need email.

Sign up for Motherboard Premium.



Image: Shutterstock / Remix: Jason Koebler

[FREE FOR ALL](#)

|

by [Joseph Cox](#)

|

May 16 2018, 10:16am

Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US

A hacker has provided Motherboard with the login details for a company that buys phone location data from major telecom companies and then sells it to law enforcement.

-  SHARE
-  TWEET

A hacker has broken into the servers of Securus, a company that allows law enforcement to easily track nearly any phone across the country, and which a US Senator [has exhorted federal authorities to investigate](#). The hacker has provided some of the stolen data to Motherboard, including usernames and poorly secured passwords for thousands of Securus' law enforcement customers.

Although it's not clear how many of these customers are using Securus's phone geolocation service, the news still signals the incredibly lax security of a company that is granting law enforcement exceptional power to surveil individuals.

"Location aggregators are—from the point of view of adversarial intelligence agencies—one of the juiciest hacking targets imaginable," Thomas Rid, a professor of strategic studies at Johns Hopkins University, told Motherboard in an online chat.

Last week, [the New York Times reported](#) that Securus obtains phone location data from major telcos, such as AT&T, Sprint, T-Mobile, and Verizon, and then makes this available to its customers. The system by which Securus obtains the data is

typically used by marketers, but Securus provides a product for law enforcement to track phones in the US nationwide with little legal oversight, the report adds. In one case, a former sheriff of Mississippi County, Mo., used the Securus service to track other law enforcement official's phones, according to court records.

The hacker who breached Securus provided Motherboard with several internal company files. A spreadsheet allegedly from a database marked "police" includes over 2,800 usernames, email addresses, phone numbers, and hashed passwords and security questions of Securus users, stretching from 2011 up to this year. A hash is a cryptographic representation of a piece of data, meaning a company doesn't need to store the password itself. But the hashes themselves were created using the notoriously weak MD5 algorithm, meaning attackers could learn a user's real password in many cases. Indeed, some of the passwords have seemingly been cracked and included in the spreadsheet. It is not immediately clear if the hacker that provided the data to Motherboard cracked these alleged passwords or if Securus stored them this way itself.

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.

Most of the users in the spreadsheet are from US government bodies, including sheriff departments, local counties, and city law enforcement. Impacted cities include Minneapolis, Phoenix, Indianapolis, and many others. The data also includes Securus staff members, as well as users with personal email addresses that aren't explicitly linked to a particular government department.

Motherboard verified the data by using Securus' website's forgotten password feature. When typing in a gibberish email address, the site returned an error. But when presented with a username and email address from the hacked data, the site progressed to the next stage of the password reset process, confirming that those credentials are stored within Securus' systems. Every set of credentials Motherboard tested was successful. Securus also confirmed a set of data had been "unlawfully accessed."

"While our forensic investigation continues, evidence at this point indicates that impacted data is a very limited scope of administrative user account information," Securus' statement to Motherboard reads. "We intend to provide law enforcement authorities with the details from our investigation and ask for aggressive prosecution when warranted," it added.

It is not totally clear how many of these users have access to Securus' phone location service. But other parts of the data indicate that many of the users are likely to be working in prisons: some of the users' roles are marked as "jail administrator," "jail captain," and "deputy warden." On its website, Securus markets its "Location Based Services" product to prisons so staff can know where inmates are calling.

"Track mobile devices even when GPS is turned off," the Securus website reads. "Call detail records providing call origination and call termination geo-location data," it adds. This is the same product that is being abused by some law enforcement officials. In a statement, Securus told Motherboard it had found no evidence that the stolen information is related to the Location

Based Services product, but out of an abundance of caution it had disabled access to the location data for the time being.

“Securus was enabling tracking without a warrant and allowing users of their system to claim authority to do so without checking it. That’s a problem,” Andrew Crocker, staff attorney at campaign group the Electronic Frontier Foundation told Motherboard in a phone call. “A concern with any system is if it’s not limited to authorized users who have the authority to engage in surveillance, then it’s doubly problematic.” In other words, a hacker gaining access to a list of Securus users and their login details could be particularly dangerous.

Read more: [Motherboard's Security Tuneup](#)

The hacker explained to Motherboard how they allegedly obtained the data, and from that account, it appears the hack was relatively simple. And a hack of Securus was also the basis for [a previous 2015 investigation from The Intercept](#), which included 70 million prisoner phone calls.

But this latest data breach is not the only sign that Securus is careless with sensitive information. Rid pointed Motherboard to a Securus user manual available online. One part shows a map and user interface for a Securus product, but instead of populating the screen with fake data for demonstration purposes, the guide appears to include the real name, address, and phone number of a specific woman. (Motherboard confirmed the details with those in online databases, as well as a media report that mentions the woman).

“The PII [personally identifying information] exposure in the (still) public user guide raises one question: does Securus have



the culture and the procedures in place to protect sensitive PII? The answer appears to be no," Rid told Motherboard.

Senator Ron Wyden, who sent letters to major telcos and the FCC pushing for more answers around Securus before the *New York Times'* piece, told Motherboard in a statement that "If this account is true, it demonstrates, yet again, that Securus is failing cybersecurity 101, in total disregard for the privacy of the Americans whose communications and private data it should be protecting. This incident is further evidence that the wireless carriers and FCC need to step up and do much more to ensure that Americans' location information and other personal information isn't sold to companies like Securus that have demonstrated that they simply don't care about cybersecurity."

Jason Koebler contributed reporting.

Update: This piece has been updated to include extra context around another Securus data breach reported by The Intercept, and more information from a Securus statement.



-  SHARE
-  TWEET
- Tagged:
- [SURVEILLANCE](#)
- [law enforcement](#)
- [data breach](#)
- [State of Surveillance](#)
- [surveillance](#)
- [Cell Phone Tracking](#)

- [securus](#)
- [Securus Technologies](#)

Watch This Next

Where we're going, we don't need email.

Sign up for Motherboard Premium.

[State of Surveillance](#)

|

by [Karl Bode](#)

|

Jan 17 2018, 7:30am

**There's No Public Evidence
Huawei Spies on Americans,
But the Company Is Getting
Blackballed Anyway**

Telecom companies scrapping plans to sell Huawei phones reeks of hysteria and protectionism.

-  SHARE
-  TWEET

Image: Shutterstock

American telecom companies are being pressured by the government to avoid doing business with Chinese hardware manufacturer Huawei due to concerns that the Chinese government would use Huawei devices to spy on Americans. The problem: nobody has provided a shred of hard evidence that the company has done anything wrong, raising the question of whether this is glorified protectionism hiding behind the banner of national security.

Huawei, which makes the Huawei Mate 10, the P10, and helped Google build the 2015 Nexus 6P, has been eager to gain a foothold in the U.S. smartphone and network hardware market, but has routinely run face-first into roadblocks erected both by both lawmakers and companies eager to avoid the added overseas competition. Similar obstacles have faced Chinese vendor ZTE and wireless carrier China Mobile.

Earlier this decade, Huawei's efforts to make inroads in the U.S. quickly resulted in numerous allegations over the company's alleged connections to Chinese intelligence. Despite breathless

hysteria, numerous investigations (one 18 months in length) found [absolutely no evidence of such a threat](#).

“We knew certain parts of government really wanted (evidence of active spying),” one person familiar with the probe told Reuters at the time. “We would have found it if it were there.”

Fast forward to this month, when *The Wall Street Journal* [published a report](#) stating that a new smartphone collaboration between AT&T and Huawei was scrapped just days before it was scheduled to be revealed at CES. The reason? An unpublished December 20 letter by the Senate and House Intelligence Committee urging the FCC and AT&T to scrap the deal over Huawei spying concerns.

Image: Shutterstock

The nature of these concerns has not been clearly documented, and public evidence of spying still hasn't emerged. Regardless, [a follow up report by Reuters](#) indicates that there has been pressure applied on U.S. telcos to avoid doing business with Huawei, with companies like Verizon and AT&T being told they risk losing their lucrative government business contracts if they strike deals with the massive Chinese multinational.

According to Reuters, telcos are being told to not only avoid selling Huawei smartphones, but to avoid using Huawei networking gear as they rush toward deployment of 5G wireless broadband networks. They're even being warned to avoid selling Huawei phones through their prepaid wireless subsidiaries.

“One of the commercial ties senators and House members want AT&T to cut is its collaboration with Huawei over standards for the high-speed next generation 5G network,” the report said, citing anonymous government insiders. “Another is the use of Huawei handsets by AT&T’s discount subsidiary Cricket,” these sources claimed.

AT&T is [a close ally](#) in the United States government’s own intelligence gathering efforts, and isn’t likely to put that relationship at jeopardy. The telco is also currently trying to gain regulatory approval of the company’s \$86 billion acquisition of Time Warner.

While Reuters highlights the fact that there have been numerous investigations into these allegations, it didn’t note that its own reporting showed that those investigations have resulted in [no hard evidence](#) of Huawei spying. Reuters also didn’t note that Huawei’s rumored spying habit is something propped up by U.S. hardware vendors looking to avoid the threat of added competition.

A 2012 [Washington Post report](#) highlighted how Cisco routinely lobbies the government to encourage scrutiny of Huawei. The company was also caught circulating marketing material highlighting the state surveillance allegations: “Despite denials, Huawei has struggled to de-link itself from China’s People’s Liberation Army and the Chinese government,” one paper authored by Cisco reads.

With many details of the allegations classified, the ground is fertile for the encouragement of hysteria.

“What happens is you get competitors who are able to gin up lawmakers who are already wound up about China,” one source told the *The Washington Post*. “What they do is pull the string and see where the top spins.”

This renewed flare up over Huawei’s alleged spying practices comes not coincidentally, as Texas Representative Mike Conaway has introduced a bill dubbed the [Defending U.S. Government Communications Act](#), which aims to ban US government agencies from using phones and equipment built by Huawei or ZTE.

Both China and Huawei have frequently complained that the regulatory hurdles imposed on Huawei and other Chinese networking companies is an example of the kind of arbitrary trade barriers the United States routinely accuses China of. Huawei has denied the spying allegations, noting that such cooperation would put its global business relationships at risk.