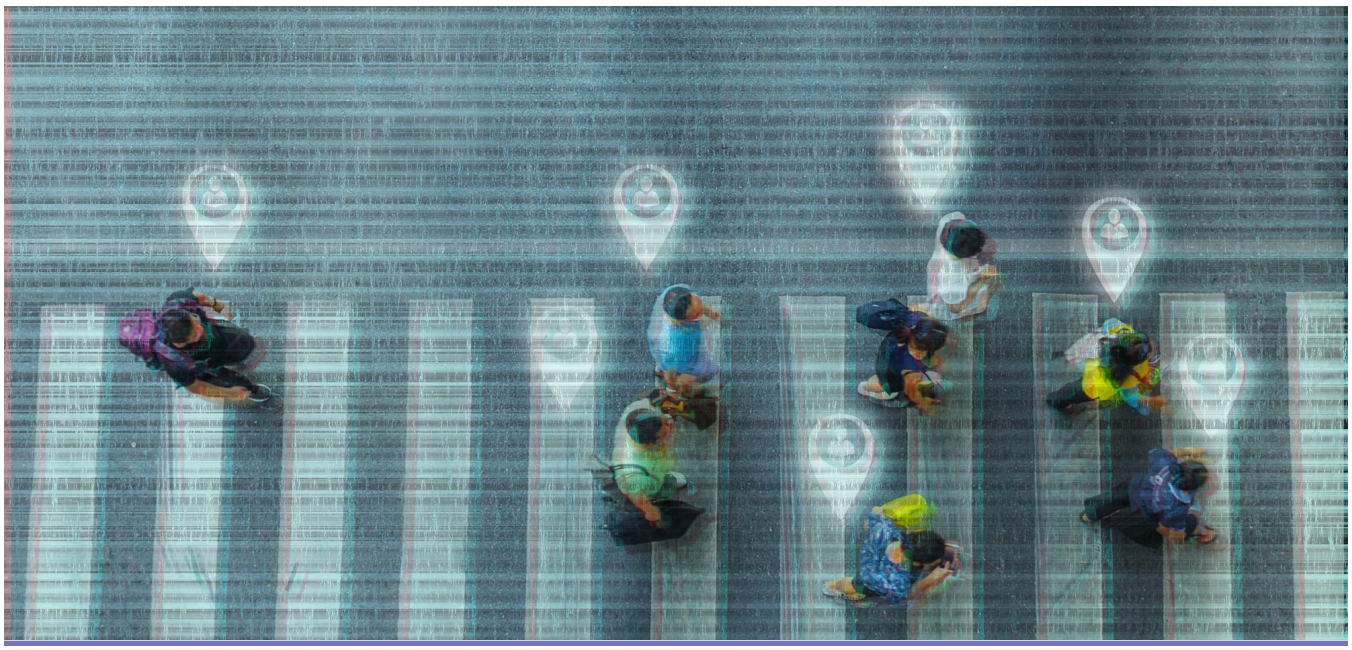


SURVEILLANCE

# 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.**

By Joseph Cox | Jan 8 2019, 12:08pm

SHARE TWEET

Image: Shutterstock. Remix: Jason Koebler

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


Dockets.Justia.com

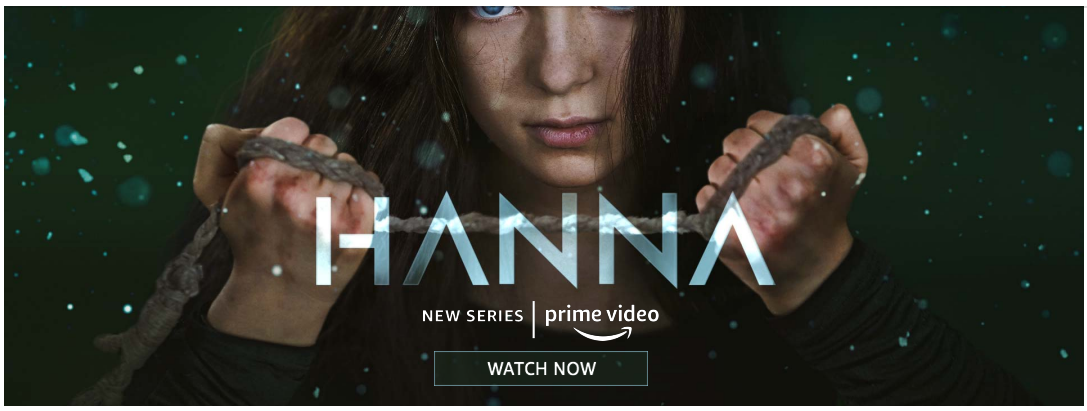
The bounty hunter sent the number to his own contact, who would track the phone. The contact responded with a screenshot of Google Maps, containing a blue circle indicating the phone's current location, approximate to a few hundred metres.

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.

ADVERTISEMENT




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,***

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.


CYBER

acast

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

Jan 24, 2019 · 42 min

View terms

***[Subscribe to CYBER on Apple Podcasts or any podcast app.]***

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,


How Motherboard got cell phone location data using only a phone number
T · ·Mobile·
Zumigo
Mobile in Context
microbilt
Bail Bond Company


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 Kaltheuner, 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.”

ADVERTISEMENT

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.

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.


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

Hopkins University, told Motherboard in an online chat.

ADVERTISEMENT

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.

To print the document, click the "Original Document" link to open the original PDF. At this time it is not possible to print the document with annotations.

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.

ADVERTISEMENT

“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."**

ADVERTISEMENT

“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.

ADVERTISEMENT

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

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.

ADVERTISEMENT

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."

SHARE TWEET

TAGGED: SPYING, CYBERSECURITY, BOUNTY HUNTER, STALKING, VERIZON, T-MOBILE, AT&T, SECURUS, MICROBILT

## Watch This Next

CREATED WITH GEICO

**Want to go to grad school? Learn the common pitfalls of student debt.**

Sign up for Motherboard Premium.

Your email SUBSCRIBE

ADVERTISEMENT

SURVEILLANCE

# Google Demanded That T-Mobile, Sprint Not Sell Google Fi Customers' Location Data

**Google's phone, text, and data service relies on infrastructure provided by T-Mobile and Sprint. A Motherboard investigation found both telcos selling customers' location data that ultimately ended up in the hands of bounty hunters.**

By Joseph Cox | Jan 11 2019, 8:47am

Image: Shutterstock

SHARE TWEET

On Thursday, AT&T announced it was stopping the sale of its customers' real-time location data to all third parties, in response to a Motherboard investigation showing how data from AT&T, T-Mobile, and Sprint trickled down through a complex network of companies until eventually landing in the hands of bounty hunters and people unauthorized to handle it. To verify the existence of this trade, Motherboard paid $300 on the black market to successfully locate a phone.

ADVERTISEMENT

Google, whose Google Fi program offers phone, text, and data services that use T-Mobile and Sprint network infrastructure in the United States, told Motherboard that it asked those companies to not share its customers' location data with third parties.

"We have never sold Fi subscribers' location information," a Google spokesperson told Motherboard in a statement late on Thursday. "Google Fi is an MVNO (mobile virtual network operator) and not a carrier, but as soon as we heard about this practice, we required our network partners to shut it down as soon as possible." Google did not say

An MVNO is essentially a company that provides the usual telecommunication services such as calls and texts, but which uses infrastructure from a telco carrier. Launched in 2015, Fi has international coverage in 170 countries and also offers data only SIMs. Google recently announced an expansion of Fi's availability to more Android devices as well as iPhones.

**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.

Motherboard / Joseph Cox / Jan 8

T-Mobile which sold to a so-called location aggregator named Zumigo. Zumigo then sold the access to Microbilt, a firm which offers phone location services to the bounty hunter industries as well as other sectors. A Microbilt customer then offered a phone lookup to a source, and that source provided Motherboard with a Google Maps screenshot showing the location of the phone itself. The location data was accurate to a range of around 500m, enough to, in our case, correctly point to a specific area of Queens, New York.

T-Mobile had previously said it was cutting its relationships with location aggregators. In tweets posted in response to Motherboard's story, T-Mobile CEO John Legere reiterated that the company is continuing to ramp down all of its location aggregator contracts, and plans to have this completed by March.

ADVERTISEMENT

Sprint has not responded to Motherboard's request for comment on whether it plans to mirror the actions of T-Mobile and AT&T and shut down all location aggregator access. Google suggested the telco may be taking some action: Google told Motherboard its partners, namely T-Mobile and Sprint, have already stopped the practice or plan to do so in the coming months (Google clarified to Motherboard that the company told T-Mobile and Sprint to shut down the sale of Fi customers' data, rather than the telcos' customers more widely.)

> ***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.***

In a previous, more general statement to Motherboard, a Sprint spokesperson said "Protecting our customers' privacy and security is a top priority, and we are transparent about that in our Privacy Policy. We do not knowingly share personally identifiable geo-location information except with customer consent or in response to a lawful request such as a validated court order from law enforcement."

This isn't the first time telcos have said they will take action against location

level law enforcement to track down phones without a warrant. In response, AT&T, Verizon, T-Mobile, and Sprint cut access to Securus, the company that was acting as a middleman between LocationSmart and the end users. Since then, the telcos have continued to provide location data access for other purposes, such as to roadside assistance firms for locating stranded customers for fraud prevention.

ADVERTISEMENT

On Thursday Verizon told *The Washington Post* it is winding down its own four remaining location aggregator contracts, which are all with roadside assistance companies. After that, customers will have to give Verizon permission to share their location with the firms. Verizon has not responded to Motherboard's multiple requests for comment over the past week.

Motherboard's investigation showed there is still clear room for abuse with location aggregators. These new steps will, T-Mobile and AT&T say, see them cutting off the sale of location data to all third parties. Multiple senators called for the Federal Communications Commission (FCC) to investigate the issue on Wednesday.

"For the second time in six months, carriers are pledging to stop sharing American's location with middlemen without their knowledge," Wyden told Motherboard Thursday. "I'll believe it when I see it. Carriers are always responsible for who ends up with their customers data—it's not enough to lay the blame for misuse on downstream companies."

***Subscribe to our new cybersecurity podcast, CYBER.***

SHARE TWEET

TAGGED: PRIVACY, CYBERSECURITY, BOUNTY HUNTERS, VERIZON, T-MOBILE, AT&T, CELL PHONE TRACKING, LOCATIONSMART, ZUMIGO

CREATED WITH GEICO

**Want to make a movie? Learn how to do it without going into debt.**

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

Sign up for Motherboard Premium.

Your email SUBSCRIBE

ADVERTISEMENT

SURVEILLANCE

# AT&T to Stop Selling Location Data to Third Parties After Motherboard Investigation

**After Motherboard found that AT&T, T-Mobile, and Sprint are selling their customers' phone location data ultimately to bounty hunters, AT&T has decided to stop service for all location aggregators, an essential part of the data supply chain.**

By Joseph Cox | Jan 10 2019, 6:13pm

Image: Shutterstock

SHARE TWEET

On Tuesday, Motherboard revealed that T-Mobile, AT&T, and Sprint were all selling their customers' phone location data that ultimately ended up in the hands of bounty hunters, as well as people unauthorized to handle it at all. We found this by purchasing the capability to locate a phone from the black market for just $300. In response, several senators called for the Federal Communications Commission (FCC) to investigate, and brought up the prospect of greater regulation of the telecommunications industry.

ADVERTISEMENT

Now, AT&T says it is stopping the sale of all location data to so-called location aggregators, companies that sit in the supply chain between the telcos and clients, and which play a vital role in having that data trickle down to end users.

"Last year we stopped most location aggregation services while maintaining some that protect our customers, such as roadside assistance and fraud prevention. In light of recent reports about the misuse of location services, we have decided to eliminate all

AT&T did not respond to Motherboard's request to elaborate on why it has decided to block those data uses as well. But it may be due to how difficult this industry has proven to police: several parts of the data supply chain were all unaware of the particular case of abuse taking place before Motherboard informed them. Clearly, there is an issue with companies keeping tabs on how customers' location data is being used, and who it is ending up with.

**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.

Motherboard / Joseph Cox / Jan 8

assistance firms to find stranded customers, or financial companies to detect fraud. But AT&T's new stance will cut those off as well.

In Motherboard's investigation, the phone we located was on the T-Mobile network. That data access travelled through a complex chain of different companies, starting with T-Mobile, before going to a location aggregator called Zumigo. Zumigo then sold it to a company called Microbilt, which provides the access to a variety of industries, including bounty hunters. A bounty hunter then sold it to a source, and that source finally provided the phone's location to Motherboard.

ADVERTISEMENT

In several different tweets posted after Motherboard's investigation, T-Mobile CEO John Legere reiterated that the company is **also going to cut off all location aggregators**.

"T-Mobile [...] is completely ending locations aggregation work in March as planned and promised," a T-Mobile spokesperson told Motherboard in an email.

> ***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.***

"MicroBilt suspended delivery of its mobile device geolocation verification service while we work with the wireless carriers and relevant technology partners to mitigate fraud risks," Microbilt, the company in the supply chain that sold location data access to a bail bondsman company, told Motherboard in a statement. "We also look forward to cooperating with governmental authorities to insure *[sic]* that these types of breaches do not occur again."

Zumigo and LocationSmart, another location aggregator, did not immediately respond to a request for comment.

Senator Ron Wyden, who along with the ***New York Times*** **previously revealed** other

“For the second time in six months, carriers are pledging to stop sharing American’s location with middlemen without their knowledge. I’ll believe it when I see it. Carriers are always responsible for who ends up with their customers data—it’s not enough to lay the blame for misuse on downstream companies,” Wyden said in a statement.

ADVERTISEMENT

He added “The time for taking these companies at their word is long past—Congress needs to pass strong legislation to protect Americans’ privacy and finally hold corporations accountable when they put your safety at risk by letting stalkers and criminals track your phone on the dark web.”

*Update: This piece has been updated to include additional comment from T-Mobile and Microbilt.*

***Subscribe to our new cybersecurity podcast, CYBER.***

SHARE TWEET

TAGGED: PRIVACY, CYBERSECURITY, BOUNTY HUNTERS, SENATOR RON WYDEN, T-MOBILE, AT&T, SПRINT, CELL PHONE TRACKING, MICROBILT

## Watch This Next

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

Sign up for Motherboard Premium.

Your email SUBSCRIBE

ADVERTISEMENT