Ajit Pai’s plan for phone location data never mentions the word “privacy”



reader comments

34 with 32 posters participating

Share this story

Smartphone 911 location data is getting more precise, but the Federal Communications Commission isn’t updating its privacy rules despite carriers’ history of selling their customers’ location data.

AT&T, T-Mobile, and Sprint were recently found to be selling detailed location data to third parties, despite rules banning such sales, and requiring that data to be used only for 911

purposes. The data ended up in the hands of bounty hunters, bail bondsmen, bail agents, and others, Motherboard reported in one of a series of articles detailing such privacy violations.

On Friday this week, the FCC is scheduled to vote on a Further Notice of Proposed Rulemaking (FNPRM) requiring collection of more precise location data. The data, referred to as "Z-axis" data, would identify a person's floor in a multi-story building when someone calls 911. Carriers could gather this data by using the barometric pressure sensors in a customer's phone to determine a person's distance above the ground to within three meters.

But the Z-axis proposal by FCC Chairman Ajit Pai never mentions the word "privacy," and it doesn't say which privacy rules would apply to carriers' collection of Z-axis data from customers' phones. A public notice on the topic issued in September also didn't mention privacy.

No comment

FNPRMs and NPRMs ask the public for comment on FCC proposals, and they are a major part of the process for issuing new rules. The fact that this FNPRM doesn't ask which privacy rules should be applied to Z-axis data limits the kind of input the public can provide to the commission. The FCC also can't impose privacy rules without first raising the possibility in the FNPRM.

"[B]ecause the FCC does not ask about this anywhere in the draft, it is virtually impossible for anyone to bring the issue up in the proceeding without the FCC issuing a new Public Notice," Harold Feld, longtime telecom attorney and senior VP of consumer advocacy group Public Knowledge, wrote in a blog post yesterday.

Feld was able to provide the FCC some input on its omission in

a filing, because FCC Commissioner Geoffrey Starks' office asked Feld if the proposed Z-axis data would be adequately protected in the absence of any specific mention of privacy or security in the FNPRM. Feld's response called the omission "inexcusable in light of continued revelations that carriers appear to be unable to protect… real-time geolocation information."

Different data, different rules

The FCC has previously said that any location data in the National Emergency Address Database (NEAD) "may not be used for any non-911 purpose, except as otherwise required by law." That's a stronger protection than what the FCC applies to other forms of Customer Proprietary Network Information (CPNI).

Section 222 of the Communications Act is the US law that requires carriers to protect CPNI, and it says that carriers may not use or disclose location information "without the express prior authorization of the customer."

As Feld noted in his blog post, CPNI rules do not "prevent people who are *not* the carrier from getting access to the GPS and using this information, so long as these folks have (or *appear* or *claim* to have) subscriber permission. That's why every application you download on your phone can access your location information, and there's virtually no way to stop this."

Unlike standard GPS data, assisted-GPS (A-GPS) data used for 911 location is supposed to get enhanced privacy protections because of its inclusion in the NEAD. Feld argues that the enhanced privacy protections should also apply to Z-axis data, which would also be used for 911 location purposes.

Feld continued:

> *Although carriers can let applications access GPS, they are not allowed to permit applications (or anything else) to access the NEAD information, which contains your exact location. With the proposed FNPRM the FCC will vote on this Friday, the agency proposes a new category of information, called 'Z-axis,' without saying which set of privacy rules governs Z-axis information.*

The FCC could later decide to "clarify" that it always considered Z-axis to be covered by the NEAD rules, but doing so now would be a lot easier. Now would also be a better time, Feld writes, for the FCC to ask the public for "comment on privacy concerns so parties can address it in the proceeding."

Pai could also change the draft FNPRM before tomorrow's vote. But he would likely be able to win a vote even if he doesn't make such changes, because he leads the FCC's 3-2 Republican majority.

"If nothing in the wording changes and the FCC votes to approve the FNPRM, then it becomes much harder for you, the consumer, to prevent other entities—including bounty hunters and stalkers pretending to be cops—from knowing exactly where you are at any given time," Feld wrote.

No word from Pai's office

We asked Pai's office yesterday to explain why the current version of the proposal doesn't address privacy and security as well as whether the FCC plans any specific privacy rules for Z-axis data. We also asked about the status of the FCC's investigation into carriers selling location data. We'll update this story if we get a response.

We did get responses to our inquiries from both Democratic members of the FCC, Starks and Jessica Rosenworcel.

In a statement to Ars, Starks said:

> *Time and again in recent months, we've read about people's location information from use of mobile phones being for sale… If the allegations are true, this is against the law and violates the commission's rules. It's outrageous and needs to stop. With the 911 location NPRM, the commission is creating a new kind of highly accurate location information that has the ability to allow first responders to find you when you need help. But, for this new information, we need to seize the opportunity to put privacy protections in place from the get-go to make sure it's not misused.*

Rosenworcel urged the FCC to be more public about its investigation into sales of location data and said it's not clear whether the FCC "can be trusted" to protect customers as phone location data becomes more accurate.

"Geolocation data is sensitive. But the FCC hasn't provided the public with any details about its investigation into the illicit sale of this consumer data by location aggregators—and how as a result it wound up in the hands of bounty hunters and shady middlemen," Rosenworcel told Ars. "So it's fair to ask if the agency can be trusted to do the right thing when it comes to setting policies related to new classes of location data."

Carriers have pledged to stop selling customer location data, but Sen. Ron Wyden (D-Ore.) told the carriers in a letter this week that "[i]t is now abundantly clear that you have failed to be good stewards of your customers' private location information."

https://arstechnica.com/?p=1473865