Security By Kieren McCarthy in San Francisco 8 Feb 2019 | The Register

US lawmakers furious (again) as mobile networks caught (again) selling your emergency location data to bounty hunters (again)

Privacy advocates stunned that explicit rules ignored, blame head of FCC

Obviously, not really dead...

Analysis US lawmakers have again called for an investigation into cell networks after it emerged that they have been selling specially protected user location data intended only for emergency services.

Senator Ron Wyden (D-OR), who has repeatedly highlighted privacy violations by mobile operators, today called out Ajit Pai, boss of America's comms watchdog the FCC, in particular for the latest violation.

"This is more than an oversight. It's flagrant, willful disregard for the safety and security of Americans. Meanwhile, instead of policing these carriers, FCC and Ajit Pai have been rewriting the rules to help phone companies rake in more profit," he tweeted.

FCC Commissioner Jessica Rosenworcel, who signed off on rules that put specific privacy protections around what is called A-GPS data and is designed to provide user location accurate to a few feet, including the height at which someone is located so they can be found within apartment blocks, was also shocked.

"This mobile phone data location scandal keeps getting worse. It's time for the FCC to step it up and complete its investigation," she tweeted. "There is something fundamentally wrong when hundreds of bounty hunters can pay a few hundred dollars and know where any of us are with our mobile devices."

Meanwhile privacy advocates are up in arms, having fought for and achieved specific privacy protections over the A-GPS data.

"This is outrageous," senior VP of privacy advocacy group Public Knowledge, Harold Feld, told us. "This was precisely the danger we were worried about."

Feld also squarely pinned the blame on FCC chair Ajit Pai. "We have a chairman who doesn't want to do his job. Even though it's the law, Pai has made it plain that he doesn't think the FCC should be protecting privacy."

Privacy requirements

Ever since the GPS requirements were introduced in 1996, there has been a requirement for mobile networks to consider user privacy under Section 222 of the Communications Act. But when the FCC proposed in 2015 that more precise location data be gathered because people were increasingly using mobile phones rather than landlines, privacy advocates were alarmed and fought [PDF] for extra provisions to be added that required someone to be explicitly informed that they were being tracked and to give consent before that data can be shared.

After a two-year process, the cellular network industry in 2017 released a "roadmap" for how it would account for user privacy and the FCC put it out for public comment. But, according to documents seen by Motherboard, bounty hunters had already figured out a way around all of those protections.

Mobile phone networks sold location data to third parties under what it has since emerged was a very lax process that they didn't adequately audit. Those third parties then sold that data onto others, with the data eventually ending up in the hands of private citizens.

In the case of A-GPS data, it appears that everyone involved knew it was supposed to have extra protections with the third party in this case – a company called CerCareOne – going to some lengths to keep its service a closely guarded secret within the bounty hunter industry.

Money talks

The company's website has, for years, been "under construction" but it ran a fully functional parallel portal that gave precise location details for specific phone numbers. Those wanting access to the service had to sign a contract that obliged them to keep the service secret, and they were charged up to $1,100 for a single location search.

That is worth paying if it helps locates someone who has skipped a jail hearing because a bounty hunter can expect to make $10,000 if they successful find someone who posted a $100,000 bail. It makes even more sense for a bail bond company that provides the money for bail in the first place.

According to internal documents from CerCareOne, its service was used tens of thousands of times, meaning that the market is worth millions of dollars a year. It's unclear how much mobile network giants have profited from the sale of protected private data but it was clearly sufficient for them to take the risk.

When the requirement for A-GPS data was approved by the FCC, all the regulator's commissioners offered heartbreaking stories of how named individuals has died because of a lack of precise location data.

At the time none of them mentioned the privacy concerns in their public comments but it was assumed that Section 222 would apply. However, in 2017 while the FCC was looking into the case of a company that sells phone services to jails, Securus, the misuse of location data was explicitly and repeatedly raised by concerned companies.

Securus had built a huge database on inmates – and on the people that they called – that used A-GPS data and combined it with other information culled from elsewhere. In letters to the FCC, a group of inmate family member – called the Wright Petitioners – pointed out that the location data in that database explicitly broke Section 222 because no one's consent had been obtained.

The FCC, under chair Pai, dismissed the issue saying that while it "takes seriously allegations regarding possible violations of section 222 of the Act… allegations regarding Securus's rates and practices, any allegations regarding violations of these rules are better handled in the context of an enforcement proceeding and not in that of a transaction."

Active inaction

That refusal to look into privacy violations has been repeatedly compounded by the FCC under Pai.

First, the FCC actively scrapped new privacy protections for broadband internet users that was due to come into effect just days later. Then, when last year it was revealed that mobile network companies had been selling location data without proper authorizations, the FCC repeatedly refused to carry out investigations. It instead appeared to accept cell giants' claims that they had cut off the offending third parties.

But months later it emerged that location data was still being sold through different third parties. When Senator Wyden, among others, insisted on a briefing from the FCC, Pai claimed the

regulator wasn't able to give one because of the partial government shutdown.

Now it has emerged that even the most sensitive location data – that specifically set aside for the emergency services – was also made available for sale. And those that have spent years digging into the privacy aspects of this kind of data are united in their belief that the reason mobile networks did not act earlier to cut off the provision of such data was because of the clear signals from the FCC that they won't investigate breaches of its own rules.

Because telecommunications are legally designated "Title II" communications they are explicitly under the remit of the FCC. It's not even clear that a user would be able to go through the courts and sue a mobile operator for providing access to their personal location data. The buck stops with the FCC. And the FCC is actively refusing to do its job.

In fact, literally yesterday, the FCC's Pai put out a new document calling for even more accurate GPS data to be provided by cellular giants. Of course it would only be for use in emergency alerts.

"The American people want, expect, and deserve the best possible public safety services - including the most precise targeting available for wireless alerts," Pai said. ®