Public Knowledge

March 12, 2019

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Wireless E911 Location Accuracy Reuirements
PS Docket No. 07-114

Dear Ms. Dortch:

On March 12, 2019, Randy Clark, Acting Legal Advisor on Wireline and Public Safety to Commissioner Stark, called me and asked whether I believed the proposed Z-Axis information was adequately protected in the absence of any specific mention of privacy or information security in the FNPRM.

I responded most emphatically that the failure of the FNPRM to mention privacy or security is inexcusable in light of continued revelations that carriers appear to be unable to protect properly customer real-time geolocation information. Only last week, Vice ran a third story on the ease with which stalkers, bounty hunters and debt collectors and others can obtain access to A-GPS information.[1] This is precisely the sort of "pretexting" the Commission sought to address in the 2007 CPNI Pretexting Order by obligating carriers to take reasonable precautions to protect CPNI. Nevertheless, this pretexting practice appears quite common. As the Vice article explains:

> "So many people are doing that and the telcos have been very stupid about it. They have not done due diligence and called the police [departments] directly to verify the case or vet the identity of the person calling," Valerie McGilvrey, a skiptracer who said she has bought phone location data from those who obtained access to it, told Motherboard. A skiptracer is someone tasked with finding out where people, typically fugitives on the run or those who owe a debt, are located.

In the 2014 *Third Further Notice of Proposed Rulemaking*, the FCC acknowledged the sensitivity of enhanced geolocation information and took care to solicit comment on a range of privacy concerns.[2] In 2015, in response to comments filed by Public Knowledge and others

[1] Joseph Cox, "Stalkers and Debt Collectors Impersonate Cops To Trick Big Telecom Into Giving Them Cell Phone Location Data," Motherboard (March 6, 2019). Available at: https://motherboard.vice.com/en_us/article/panvkz/stalkers-debt-collectors-bounty-hunters-impersonate-cops-phone-location-data

[2] *Third FNPRM*, FCC 14-13 at ¶136.

raising these privacy concerns, the Commission adopted specific additional privacy and security requirements for NEAD database access.[3]

Particularly in light of the recent articles highlighting the willingness of carriers to sell geolocation information,[4] and apparent inability to adequately protect A-GPS location data,[5] the Commission should strongly reaffirm its commitment to privacy of geolocation information collected for 911 purposes, and seek comment on whether to impose requirements similar to (or stronger than) the requirements imposed in 2015 for access to the NEAD database.

This notice is filed in compliance with 47 C.F.R. §1.1206(b)(2)(v). If you have any questions, please feel free to contact me at (202) 861-0020.

Respectfully submitted,

/s/ Harold Feld
Harold Feld
Senior V.P.
Public Knowledge
1818 N Street, NW
Washington, DC 20036

cc: Randy Clark

[3] *Fourth R&O*, 15-9.
[4] *See* Joseph Cox, "I Gave a Bounty Hunter $300. Then He Located Our Phone." Motherboard (January 8, 2019). Available at: https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile
[5] *See* Joseph Cox, "Hundreds of Bounty Hunters Had Access To AT&T, T-Mobile and Sprint Customer Data For Years," Motherboard (February 6, 2019). Available at: https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years