



August 22, 2022

Via Electronic Mail

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Re: Response to Request for Information Concerning Geolocation Services

Dear Chairwoman Rosenworcel:

I am writing in response to your July 19, 2022 letter requesting information concerning how U.S. Cellular Corporation (“UScellular”) treats geolocation data collected from its customers (the “Information Request”). Detailed responses to the Information Request are attached as an appendix to this letter. We note that UScellular is re-submitting this response at the Commission’s request to ensure that its answers are available for public inspection.

UScellular is committed to safeguarding the privacy of its subscribers’ data and to being transparent with subscribers about the data it collects and how it uses it. UScellular’s Privacy Center provides information about the company’s privacy practices that is readily accessible and easy to follow so that subscribers know its policies and their rights. The Privacy Center is available at <https://www.uscellular.com/privacy>.

Consistent with that, UScellular has taken significant steps to protect any geolocation data that it collects from subscribers using its wireless network. As the responses show, UScellular, among other things:

- Manages access and use to the systems containing such data on a strict need-to-know basis.
- Imposes strict limitations on vendors to protect such data.
- Does not sell subscriber geolocation data or otherwise share it with third parties, except pursuant to a valid request from law enforcement or a court order.
- Regularly purges such data on a specified schedule.

UScellular notes that it does not control all geolocation data generated by its subscribers. In particular, applications on a subscriber’s smart phone, tablet, and other devices may collect and obtain subscriber geolocation data without accessing UScellular’s network and without UScellular’s involvement or knowledge.

Respectfully submitted,

/s/

Adriana Rios Welton
Head of Legal and Government Affairs

Appendix

(1) Data retention:

a. Please describe in detail the geolocation data that US Cellular collects and/or retains regarding current and/or former subscribers. How is that data collected?

UScellular collects mobile device location information from subscribers using its network by estimating the latitude and longitude of a mobile device within a given radius. Only when required by law enforcement or court order does UScellular collect real-time mobile device location by locating the tower with the associated sector and azimuth that the subscriber's device is connected to. The data is retained in storage systems located in the United States. UScellular manages access and use to such systems on a strict need-to-know basis.

b. Please explain the reasons geolocation data is retained for both current and former subscribers.

The systems retain geolocation data to ensure the effective management of the network and continually improve the subscriber experience. For example, the data is used to detect and prevent security incidents and fraud; to identify and repair network errors; to monitor and adjust the network's performance; to maintain the quality, safety and integrity of the wireless service; to audit digital interactions; to perform services such as customer care activities; and to efficiently manage our workforce.

c. How long is geolocation data retained for both current and former subscribers.

UScellular's systems regularly purge subscriber geolocation data on a specified schedule. Unless otherwise required by law or court order, the longest this information is stored is 18 months.

d. Please provide a description of what safeguards US Cellular uses to protect current and former subscriber geolocation data.

UScellular protects subscriber geolocation data through a security approach that is based on the critical security controls best practices guidelines published by the Center for Internet Security and is designed to protect information against loss, unauthorized access, destruction, use, modification, or disclosure.

e. In what country (or countries) is geolocation data stored?

The United States.

f. Please share whether and how you disclose your data retention policies to subscribers.

UScellular discloses its collection, use and sharing policies through its privacy center, which can be accessed at: <https://www.uscellular.com/privacy>. As stated in UScellular's privacy policy (available within the privacy center at: <https://www.uscellular.com/privacy/privacy-policy>), UScellular conducts periodic updates to its privacy policy that may, as required, include information on its data retention practices.

g. What is your data deletion policy for current or former subscribers, and how do you dispose of subscriber geolocation data?

UScellular's systems regularly purge subscriber geolocation data on a specified schedule. Unless otherwise required by law or court order, the longest this information is stored is 18 months.

h. Do your subscribers have any opportunity to opt-out of your data retention policies and if not, why not?

UScellular subscribers in California may opt out of data retention in compliance with the requirements of the California Consumer Privacy Act. UScellular subscribers may not otherwise opt out of retention policies because the retention of such data is important for network management and other business purposes, as described in answer to question (1)(b) above.

(2) Data sharing

a. Please provide US Cellular's process and policies for sharing subscriber geolocation data with law enforcement?

UScellular has a publicly available Law Enforcement and Legal Compliance Resource site <https://www.uscellular.com/legal/LEA>. That site provides a Law Enforcement Resource Guide <https://www.uscellular.com/content/dam/uscc-static/assets/pdfs/LERGv2.pdf>.

We note that UScellular only collects real-time mobile device location information (or Ping) in response to exigent circumstance emergency affidavits submitted by law enforcement. Ping is collected by locating the tower with the associated sector and azimuth that the subscriber's device is connected to. When a Ping is not available, UScellular may share time-limited historical geolocation data with law enforcement. Emergency requests are stored and tracked.

Further, UScellular notes that a subscriber's historical geolocation data is otherwise only shared pursuant to a lawful search warrant or court order.

b. Describe the arrangements, agreements, and circumstances in which US Cellular shares subscriber geolocation data with third parties that are not law enforcement.

There are no such arrangements or agreements. The information is only shared with law enforcement pursuant to the above or when required to do so by a court order.

c. Describe in detail the process by which a subscriber may opt out of the sharing of their geolocation data. Under this opt-out process is that subscriber's data still shared with third parties? In particular, does the opt-out process allow a subscriber to opt out of the sharing of their geolocation data with all third parties that are not law enforcement?

There is no opt-out process because the information is only shared with law enforcement pursuant to the above or when required to do so by a court order.

d. Are subscribers notified of the sharing of their geolocation information with third parties that are not law enforcement? And if so, how are they notified?

There is no notification process because the information is only shared with law enforcement pursuant to the above or when required to do so by a court order.