Google North America Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

650-253-0000 main
fi.google.com

August 3, 2022

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

Dear Chairwoman Rosenworcel:

I write in response to your July 19, 2022 letter regarding Google Fi's practices concerning the collection, storage, and processing of subscribers' geolocation data.[1] Please see below for responses to each of your questions.

1. **Data retention**

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

Google Fi may collect and/or process location information about a current and/or former subscriber or their device, depending on the subscriber's device or account settings, as described in the Google Fi Privacy Policy, the Google Privacy Policy, and the Google Fi FAQ page.[2] For example, this may include location information about a subscriber or subscriber's device moving between and throughout mobile and Wi-Fi networks, in order to provide and improve Google Fi's services. We discuss specific types of information in more detail below.

First, Google Fi's U.S. carrier partners, T-Mobile and US Cellular, share charging data records (CDRs) with Google Fi, where available. These records may contain calling, messaging, and cellular data usage information, including Cell IDs (CIDs),[3] mobile country codes (MCCs), and IP addresses.

---

[1] Letter from Jessica Rosenworcel, Chairwoman, FCC, to Google, DOC-385452 (sent July 19, 2022). Google Fi is provided by Google North America Inc., a wholly owned subsidiary of Google LLC.
[2] In this response, for explanatory purposes, we have included certain types of data that Google Fi does not use to identify an individual subscriber's or a subscriber's device's location and that would not be considered subscribers' "geolocation data."
[3] A CID is a unique number used to identify a cellular base station transceiver.

With respect to CIDs, Google Fi receives CID information from carriers' CDRs and in the course of providing Google Fi's services. Although a carrier partner possesses the relevant cell tower data needed to correlate a CID value with a base station location, Google Fi does not possess the relevant cell tower data needed to identify a subscriber's or subscriber's device's location from the CID.

Similar to CIDs, Google Fi receives MCCs both in the course of providing Google Fi's services and from carriers' CDRs.

As for IP addresses, Google Fi only occasionally receives this information in CDRs from carrier partners. Google Fi also obtains IP addresses in the course of offering and providing Google Fi's services, e.g., by permitting users to sign up for the service online and providing online technical support. An IP address does not in and of itself identify the location of an individual or device at a specific period of time, but could, in some cases, be used to infer a general area (e.g., city).

Finally, Google Fi also receives service addresses from subscribers. The service address is the subscriber-provided permanent residence (i.e., what's on the subscriber's billing statement). The service address set at the beginning of each monthly cycle is the address used to calculate that cycle's state and local taxes. This address is also used to route emergency calls and services if the subscriber's location isn't immediately known.[4] In addition, a subscriber's Google Account address is used to bill and collect payments for Google Fi services.

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

The reasons Google Fi collects location information for current and/or former subscribers are described in the Google Fi Privacy Policy, the Google Privacy Policy, and the Google Fi FAQ page. CDRs are used to accurately bill subscribers for their Google Fi usage and to provide call history information in subscriber accounts. MCCs and IP addresses are used to provide the Google Fi services, as well as to prevent abuse of Google Fi services. Service addresses are used for billing and tax purposes, as well as to route emergency calls.

For Android devices, Google Fi's network-switching function, which ensures that the device uses the best available network based on the device's location, requires that the device process certain types of data–such as device location (GPS and other signals), Cell IDs, and

[4] The emergency call made on a carrier partner's cellular network is handled entirely by the carrier partner (e.g., connecting the caller to the local Public Safety Answering Point).

MCCs. However, this data, with the exception of Cell IDs, MCCs, and IP addresses, does not leave the subscriber's device.

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

Google Fi abides by the Google Privacy Policy, including with respect to data retention. The policy explains how Google Fi retains subscriber data, including location data. These disclosures describe why Google Fi holds onto different types of data for different periods of time. Consistent with Google's general approach to data retention, Google Fi automatically deletes subscriber data after a set period of time, when it is no longer needed for the purpose for which it was collected.

d. *Please provide a description of what safeguards Google Fi uses to protect current and former subscriber geolocation data.*

Google Fi builds security into its services to protect subscriber data.[5] We work hard to protect subscribers' information from unauthorized access, alteration, disclosure, or destruction, including by using several safeguards.

First, Google Fi requires that subscriber data (including data that can be used to identify a subscriber's or subscriber's device's location) be encrypted "at rest," and that subscriber data "in transit" be encrypted when transmitted over networks outside of Google's physical control, including traffic between data centers, and across the Google network. In particular, Google Fi encrypts certain data while it is stored "at rest"—stored on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing subscriber data, they will not be able to read it because they do not have the necessary encryption keys.

Second, consistent with the Google Fi Privacy Policy and the Google Privacy Policy, Google Fi implements safeguards, including technical access controls, that are designed to protect subscriber information. For example, Google Fi restricts access to subscriber information to only those employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be subject to disciplinary actions up to and including termination if they fail to meet these obligations.

[5] *See, e.g.*, Google Fi Privacy Policy, Google Privacy Policy, Google Safety Center, and May 11, 2022 Keyword blog post.

Third, Google has strong incident response procedures. Potential privacy issues are addressed through our robust incident response program for privacy- and security-related events. Employees are required to report any suspected security or privacy incidents to our dedicated 24x7x365 worldwide incident response teams so that we can respond, including by securing and protecting users' data and handling user notifications.

Finally, Google Fi regularly reviews its information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to its systems.

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

Google Fi processes data at Google data centers, which are decentralized and located in many countries around the world. A Google Fi subscriber's data may be processed (and stored securely) at any of these data centers.

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

Google Fi's data retention policies are disclosed in the "Retaining Your Information" section of the Google Privacy Policy.

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

When a user deletes data in their Google Fi-associated account, Google Fi starts the process of removing it from the product and Google systems. First, Google Fi aims to immediately remove the data from a subscriber's view. Google Fi then begins a process designed to safely and completely delete the data from storage systems. This process generally takes around two months from the time of the deletion request (or may take longer for certain data types that require longer retention periods, e.g., billing data). This often includes up to a month-long recovery period in case the data was removed unintentionally.

Each storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted, or brief delays to allow for recovery from potential mistakes. As a result, deletion could sometimes take longer when extra time is needed to safely and completely delete the data.

Google Fi uses encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to 6 months.

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

Users can delete some types of data whenever they like, some data is deleted automatically after a certain period of time, and some data is retained for longer periods when necessary (as noted in response to 1(g) above).[6] However, when retention of the data as described above is necessary to provide the Google Fi services, it is not possible for subscribers to opt out while using the Google Fi services.

2. Data sharing

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

A variety of laws, including the Electronic Communications Privacy Act, allow federal, state, and local government agencies to compel the disclosure of user information in connection with criminal investigations. As set forth in the Google Privacy Policy and the Google Fi Privacy Notice, Google may produce Fi subscriber data in response to valid requests made consistent with those laws.

Google has a robust process for evaluating legal demands for user data. When Google reviews such demands, it carefully reviews each request to make sure it satisfies applicable laws. If a request asks for too much information, Google tries to narrow it, and in some cases, it objects to producing any information at all. In every instance, Google takes into account the privacy and security expectations of its users.

Google's Transparency Report Help Center and Frequently Asked Questions provide additional details regarding (1) the common types of legal requests it receives and (2) examples of what Google discloses in response to requests.

Where permissible, Google also provides users notice when a government agency seeks production of their information. In those instances where permissible, Google sends an email to the subscriber before disclosing information. If the account is managed by an organization, Google gives notice to the account administrator. While Google cannot give notice when legally prohibited, we will provide notice after a legal prohibition is lifted, such as when a

[6] *See, e.g.*, How Google retains data we collect.

statutory or court-ordered gag period has expired. Google also may not give notice if the account has been disabled or hijacked, or in the case of emergencies, in which case it will provide notice if it learns that the emergency has passed.

More generally, Google has long advocated for transparency and due process. Google was the first major company to create a Transparency Report on government requests for user data, and was a founding member of the Global Network Initiative and the Reform Government Surveillance coalition, both of which recommend establishing limits on government access to user data and serve as accountability mechanisms for technology companies.

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

Google Fi does not share data with third parties that are not law enforcement without subscriber consent, unless necessary to provide Google Fi services or required by law. In accordance with the Google Privacy Policy, Google Fi may share limited data with its carrier partners to provide Google Fi services to its subscribers. This sharing is necessary to provide the Google Fi services, and carrier partners are prohibited from sharing Fi subscriber data with third parties except where legally required (e.g., emergency calling).

Google Fi also shares limited types of data with Google affiliates as needed to: provide Google Fi services; process device purchases; bill and collect payments for Google Fi services and devices; troubleshoot potential issues with Google Fi services, devices, or the Google Fi account; verify identity; and protect from fraud, phishing, or other misconduct.

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?*

Google Fi shares data with third parties that are not law enforcement only when it is necessary to provide and improve Google Fi services or required by law, and for this reason, it is not possible for subscribers to opt out of such sharing while using Google Fi services.

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?*

As mentioned above, Google Fi shares limited subscriber data with its carrier partners to provide the Google Fi services (including for compliance with carrier obligations like E911). We provide notice of this sharing in the Google Fi Privacy Notice. The Privacy Notice contains a "Sharing with third parties" section that addresses how we may share subscriber information with individuals or companies outside of Google Fi and our affiliates. Specifically, this section notifies subscribers that, "We may provide personal information to our trusted businesses or persons to provide you the Services based on our instructions and in compliance with the Google Fi Privacy Notice and any other appropriate confidentiality and security measures."

***

We appreciate your attention to these issues and we hope our response has provided insights into Google Fi's data practices.

Sincerely,

Darah Franklin
Counsel to Google North America Inc.