

August 16, 2022

**VIA EMAIL** (Jessica.Rosenworcel@fcc.gov)

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

Re: Geolocation Data

Dear Chairwoman Rosenworcel:

We are in receipt of your letter dated July 19, 2022 requesting that we respond to the questions below regarding our consumer data retention and sharing policies for geolocation data.

Following an email exchange with a member of your staff, it was clarified that the FCC is not requiring our responses to include any geolocation data collected on our website and mobile application (such as IP addresses) when consumers visit, use, create accounts and/or make purchases – just when they activate and use our wireless and data services. Within these limited parameters, our responses are as follows:

**(1) Data retention:**

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

As a mobile virtual network operator contracting with the mobile network operator (MNO) T-Mobile, we do not have the capability of obtaining geolocation data by virtue of our provision of wireless and data services to our users separate and apart from the data shared with us by our MNO. To assist us with the provision of our wireless calling service, T-Mobile provides us with our users' CID information. A GSM Cell ID (CID) is a generally unique number used to identify each base transceiver station (BTS) or sector of a BTS within a location area code (LAC) if not within a GSM network. The CID is received and stored by us in numerical format as part of call processing in our application. We cannot translate the numerical CID to pinpoint an actual user address without additional translation information of its network layout, which is not provided to us by our MNO.

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

As explained, we require the CID in order to properly transmit wireless calling service to our users. This data is retained along with the entire call detail record (CDR) for eighteen (18) months pursuant to our data retention policy. The reason we retain this data is because it is intertwined with all call data, which we are legally required to retain by federal regulations for this specific retention period (47 C.F.R. §42.6).

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

18 months.

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

We have a global security policy in place that complies with GDPR requirements as well as US privacy and security standards. This policy requires that all personally identifiable information be both protected and disposed of using appropriate security classification privacy markings. We note that, it is debatable whether CID is personally identifiable data since we do not have the necessary technical data regarding our MNO network layout to translate such numbers to a physical address.

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

United States, United Kingdom and India.

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

We have a Privacy Policy that is published on our website here:

<https://www.lycamobile.us/en/privacy-policy/>

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

As previously stated, we retain CDRs (containing CIDs) for 18 months from creation, as per our data retention policy. This policy applies regardless of whether subscribers are current or former. We dispose of such data with a regularly occurring monthly purge. The only exceptions to such automatic system purging that requires manual modifications are (i) when a consumer requests that we delete their data; and (ii) when we are obligated by legal process to retain specific data for longer retention periods (such as in the case of a litigation hold or court order).

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

Yes, consumers may request that we delete certain data that is not required for us to continue provision of services to them (or that we are not legally required to retain). We have contact information provided in our Privacy Policy for any such consumer requests.

**(2) Data sharing:**

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

As described in the CALEA System Security and Integrity (SSI) Plan we filed with the FCC, we have designated a Custodian of Records as the authorized person to accept requests and legal process (e.g., subpoenas, warrants, court orders, NSLs). Upon legal review of the requesting documentation, a response is provided within ten business days either explaining why the data is not being produced or including its production, often with a certification of records or other declaration.

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

As set forth in our Privacy Policy, we do not share personally identifiable information of our consumers with third parties that are unaffiliated with the Lyca Group for their own independent marketing purposes without obtaining prior consumer consent. We note that CDRs may be produced if we are served with a valid third-party subpoena in a civil action (not by law enforcement).

**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?**

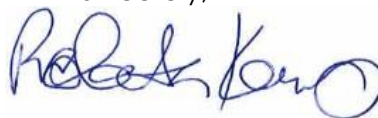
As previously explained, we require consumers to opt-in to third party marketing rather than opt-out (as required by CPNI rules). We will not share any consumer data outside of the Lyca Group absent a legal requirement, such as service of a civil subpoena.

**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?**

Again, we do not share subscriber geolocation information (CID) with third parties outside of the Lyca Group of companies unless we are required to do so by law. Often, such legal process also requires us not to disclose the service of such subpoena or court order or the existence of a legal investigation or action that may involve our subscriber.

We trust that the above adequately responds to the questions posed. Should you require any additional information, please do let me know.

Sincerely,



Roberta Kraus