



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

July 19, 2022

Deborah DiSanzo
President
Best Buy Health
7601 Penn Avenue South
Richfield, MN 55423

VIA EMAIL

Dear Ms. DiSanzo:

Mobile internet service providers are uniquely situated to capture a trove of data about their own subscribers, including the subscriber's actual identity and personal characteristics, geolocation data, app usage, and web browsing data and habits.

In February 2020, the Federal Communications Commission held the nation's four largest wireless carriers responsible for more than \$200 million in fines for selling access to their customers' location information without taking reasonable measures to protect against unauthorized access to that information.¹ These carriers voluntarily determined to end the sale of real-time location information to location aggregation services.² However, last year, a report by the Federal Trade Commission that studied ISPs representing 98 percent of the mobile internet market observed that ISPs collect more data than is necessary to provide services and more data than consumers expect.³

Accordingly, given the highly sensitive nature of this data—especially when location data is combined with other types of data, the ways in which this data is stored and shared with third parties is of utmost importance to consumer safety and privacy. I kindly ask that Best Buy Health respond to the following questions regarding Lively's consumer data retention policies for geolocation data and its policies regarding sharing of that data with third parties.

¹ *FCC Proposes Over \$200 Million in Fines for Wireless Location Data Violations*, at <https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations>.

² *See, e.g.* Brian Fung, "Verizon, AT&T, T-Mobile and Sprint suspend selling of customer location data after prison officials were caught misusing it," *The Washington Post*, Jun. 19, 2018 at <https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/>.

³ "A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers, An FTC Staff Report" Federal Trade Commission, Oct. 21, 2021, at https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

(1) Data retention:

- a. Please describe in detail the geolocation data that Lively collects and/or retains regarding current and/or former subscribers. How is that data collected?
- b. Please explain the reasons geolocation data is retained for both current and former subscribers.
- c. How long is geolocation data retained for both current and former subscribers.
- d. Please provide a description of what safeguards Lively uses to protect current and former subscriber geolocation data.
- e. In what country (or countries) is geolocation data stored?
- f. Please share whether and how you disclose your data retention policies to subscribers.
- g. What is your data deletion policy for current or former subscribers, and how do you dispose of subscriber geolocation data?
- h. Do your subscribers have any opportunity to opt-out of your data retention policies and if not, why not?

(2) Data sharing

- a. Please provide Lively's process and policies for sharing subscriber geolocation data with law enforcement?
- b. Describe the arrangements, agreements, and circumstances in which Lively shares subscriber geolocation data with third parties that are not 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?
- 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?

Please send your responses to the undersigned via email (Jessica.Rosenworcel@fcc.gov) by August 3, 2022.

Sincerely,



Jessica Rosenworcel