COMCAST

1701 John F. Kennedy Boulevard
Philadelphia, PA 19103-2838
www.comcastcorporation.com

Christin McMeley
SVP, Sr Deputy General Counsel
Chief Privacy and Legal Information
Security Officer

August 3, 2022

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

Dear Chairwoman Rosenworcel:

I am responding to your letter of July 19, 2022 regarding Comcast's data retention practices for geolocation data that Xfinity Mobile collects regarding current and/or former customers and our policies regarding sharing of that data with third parties.

Protecting our customers' privacy and the data they entrust to us is fundamental to how we run our business. We firmly believe that a relationship built on earned trust – in particular, trust that we will respect our customers' privacy – is essential to maintaining long-term customer relationships and our continued success in the marketplace. These values led to the launch of the Xfinity Privacy Center in 2019 and a set of privacy commitments, https://www.xfinity.com/privacy/our-commitment, including our commitment not to sell location data when consumers use our Xfinity Mobile service. We are very proud of both our work related to privacy and our affirmative privacy commitments.

We appreciate the sensitivity of our customers' location data and the importance of safeguarding it. As always, we will continue to review our practices to identify opportunities to enhance aspects of our privacy program in ways that benefit consumers.

Our responses to your specific questions are set forth in the Attachment. Thank you for the opportunity to provide this information, and kindly direct any follow-up questions to the undersigned.

Sincerely,

Christin McMeley
Senior Vice President, Chief Privacy and Legal Information Security Officer
Comcast Corporation

ATTACHMENT – RESPONSES TO INDIVIDUAL QUESTIONS

(1) Data retention:

(a) Please describe in detail the geolocation data that Xfinity Mobile collects and/or retains regarding current and/or former subscribers. How is that data collected?

Comcast (d/b/a "Xfinity") offers its Xfinity Mobile ("XM") service as a mobile virtual network operator ("MVNO") in partnership with the wireless network operator Verizon Communications Inc. ("Verizon"). As such, XM does not have access to nor does it obtain precise geolocation data – i.e., longitude/latitude coordinates – about XM subscribers from Verizon. Any such data about XM subscribers that may be collected by Verizon are not shared with XM.

XM receives very limited location data from Verizon. Specifically:

- **Phone Calls.** When a customer makes a phone call, XM receives information necessary to provide the service: the city and state from which the call originates and terminates, along with a base station identification code, comprised of a number that corresponds to a tower serving the subscriber. XM does not receive any information related to the location of the tower, nor does XM derive a location from the base station identification codes. XM does not receive the precise geolocation of devices used to make calls. For international roaming calls, XM receives the country of origination and termination.

- **Internet Access.** The information that XM receives from Verizon about XM subscribers' Internet access is even more limited and does not include location information.

Comcast collects certain location data when consumers, including XM customers, use Comcast's Xfinity WiFi hotspots to access Internet services. Comcast's Xfinity WiFi hotspots also may carry Wi-Fi calling for customers who have enabled the feature and are in-range of an Xfinity WiFi hotspot. When any device, including an XM customer's device, connects to an Xfinity WiFi hotspot, Comcast has access to certain device identifiers and the corresponding location of the hotspot to which the device connects. As described further below, this information is used for network optimization by enabling Comcast to understand where Xfinity WiFi hotspot demand is concentrated, so it can allocate additional resources and invest in network deployment and enhancements to improve network performance.

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

Comcast retains the records provided by Verizon (described in Response 1(a) above) to: (1) assess total customer usage and total number of devices running on the Verizon network, as well as the usage consumption on Wi-Fi and cellular networks; (2) understand geographic

clustering of cellular usage, which is essential for network planning, deployment, and management; and (3) bill for and evaluate consumer offerings.

Comcast retains information about the location of Xfinity WiFi hotspots to which Xfinity Internet subscribers' devices, including devices of XM subscribers, connect, to ensure that we are allocating additional investments and resources to build and enhance our network infrastructure in the optimal locations where subscriber use is concentrated, in order to improve network performance. Wi-Fi offloading from the Verizon network assists Comcast in providing the most cost-effective, highest-performing XM service to its subscribers and in planning for broader network upgrades. While the usage data we receive from Verizon is helpful, it is not sufficient for optimizing network planning, deployment, and management. But when supplemented by our Wi-Fi data, we have sufficient information for such network analyses and planning purposes.

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

Currently, we retain data provided by Verizon that reflects the city and state from which a customer's call originates and terminates: (1) for 45 days in our billing system before it is archived for 30 more days, and then deleted; and (2) for up to two years for network planning, deployment, and management. We retain the Xfinity WiFi hotspot data for up to two years to better understand seasonal and long-term trends in usage and to optimize our future network investments. All of our retention is subject to applicable legal holds and preservation requests.

(d) Please provide a description of what safeguards Xfinity Mobile uses to protect current and former subscriber geolocation data.

As described above, XM has access to and collects only limited location data. XM restricts access to such data to personnel for which access has been specifically authorized pursuant to a formal user access provisioning process, which includes periodic user access review. Access rights are automatically removed upon termination of employment, contract, or engagement. When de-identification of data is conducted, such de-identification must occur in conformance with the standards prescribed by Comcast's national De-Identification Center of Excellence, which meets or exceeds industry standards. These policies also apply to any location data obtained via the Xfinity WiFi network, whether from XM customers or other consumers using an Xfinity WiFi hotspot.

Additionally, to the extent XM uses service providers to assist in the processing of sensitive personal information as is necessary to deliver the service, those service providers undergo a robust initial vetting and periodic monitoring process under Comcast's Third-Party Security Assurance ("TPSA") Program. This Program is designed to ensure that our service providers meet or exceed our expectations and can satisfy any contractual or other obligations to employ sufficiently robust administrative, physical, and technical controls that meet or exceed XM's standards to protect the security, integrity, and confidentiality of the information.

These risk assessments are managed through a scalable, risk-based approach by the Governance, Risk & Compliance organization within the Comcast Cybersecurity department. The TPSA policy requires that applicable TPSA risk assessments be completed before an agreement is signed with any third party. Additionally, service providers are monitored on an ongoing basis throughout the entire lifecycle relationship including, as appropriate, through audits and subsequent remediation actions as defined by the TPSA Group. Independent third-party attestation reports are required annually from service providers with higher risk (as identified through the TPSA assessments) and reviewed by the TPSA Group. All Comcast information is destroyed or returned to Comcast (at Comcast's sole election) on completion of the services or termination of the related agreement.

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

All the location data described above is stored in the United States.

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

Comcast provides consumers with notice of our retention practices through our Privacy Policy, which currently states:

> We keep your personal information for different lengths of time depending on the type of information and the business and legal requirements. For example, if you are a customer, we keep information that personally identifies you as long as you subscribe to one or more of our Services. If you no longer subscribe to a Service, we still may need that information for business and legal requirements, such as to protect against fraud, calculate taxes, or respond to legal requests. Other information is deleted automatically after a set period of time, often set by law, unless we are legally required to hold it longer, such as for pending litigation. We destroy, de-identify, or anonymize the information when it is no longer needed in identifiable form.[1]

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

Comcast retains consumer information in accordance with our Records and Information Management Policy. After the specified retention period has elapsed, Comcast's policy is to proactively delete or de-identify the information automatically, except as otherwise needed to comply with legal processes. Certain data categories may be deleted upon a consumer's request.

[1] *Xfinity Privacy Policy*, XFINITY (Oct. 12, 2021), https://www.xfinity.com/privacy/policy?pc=1.

XM customers can visit the Xfinity Privacy Center to learn more about our data collection, use, and sharing practices, to manage their privacy settings, and to make information rights requests, including the deletion of personal information, in accordance with law.[2]

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

Subscribers cannot opt out of XM's retention policies because XM retains a limited set of location data for as long as is necessary to provide services and perform the operational functions identified above; it is not used for marketing or advertising, and we do not share any XM location data or Xfinity WiFi location data with third parties for their own purposes as further explained below.

(2) Data sharing:

(a) Please provide Xfinity Mobile's process and policies for sharing subscriber geolocation data with law enforcement?

Comcast maintains a Legal Response Center that is dedicated to receiving and processing requests from law enforcement and other government entities and ensuring legal compliance with all relevant privacy laws when we disclose customer information in response to such requests. As explained in our Guidance for Law Enforcement,[3] our wireless network operator carrier Verizon maintains responsibility for CALEA surveillance, pen register/trap and trace, SMS content, video, images, and geolocation services for XM customers. Were law enforcement to request the specific location from which an XM subscriber placed a call or accessed the Internet, XM would not possess that information and would refer the request to Verizon.

Additionally, emergency calls by XM subscribers to 911 over the cellular network are handled by Verizon, and Verizon generates the geolocation data that is shared with public safety authorities. Emergency calls by XM subscribers over Wi-Fi are also sent to Verizon for routing. In that case, rather than sharing coordinates, Verizon shares the registered location that the customer entered into their phone when they activated/updated the Wi-Fi calling feature. Customers are given notice that the address they enter will be shared with public safety.[4]

---

[2] *Xfinity Privacy Center*, XFINITY, https://www.xfinity.com/privacy (last accessed Aug. 2, 2022).
[3] *Guidance for Law Enforcement*, COMCAST LEGAL RESPONSE CENTER (July 2022), https://lea.comcast.com/register?id=leaguide.
[4] *How do I use WiFi calling on my iPhone?*, XFINITY (Mar. 24, 2022). https://www.xfinity.com/mobile/support/article/wifi-calling-on-iphone (last accessed Aug. 2, 2022).

(b) Describe the arrangements, agreements, and circumstances in which Xfinity Mobile shares subscriber geolocation data with third parties that are not law enforcement.

XM does not sell or share any consumer geolocation data with third parties for their own purposes. In certain instances, Comcast may need to share data with service providers who process that data on Comcast's behalf to enable us to provide our services. Our service providers are required to go through the TPSA process described above, which would include ongoing monitoring and audits if they receive location data, and they are contractually restricted to process the data for the limited purposes of serving Comcast. Further, Comcast's policies require the service providers with which the company shares personal information to: treat the information as confidential; use commercially reasonable physical, administrative, and technical security controls to safeguard the data, including requiring multi-factor authentication for any access to systems with sensitive personal information; and to use the data only for the purpose of providing the services for which they have been engaged, including a restriction on disclosing the data to any unauthorized third parties.

(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?

Because Comcast does not sell or otherwise share any geolocation data with third parties, a process for opting out of such sharing is not necessary.

(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?

Because Comcast does not sell or otherwise share any geolocation data with third parties, such notification is not necessary.