Jeffrey H. Blum
Executive Vice President,
External & Legislative Affairs
Jeffrey.Blum@dish.com
(202) 463-3703

VIA ELECTRONIC MAIL

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

Re: July 19, 2022 Letter to DISH Network Corporation Requesting Geolocation Information

Dear Chairwoman Rosenworcel:

DISH Wireless L.L.C. ("DISH")[1] submits this response to your letter requesting information about "Boost Mobile's consumer data retention policies for geolocation data and its policies regarding sharing of that data with third parties."[2]

To aid the Commission's inquiry, DISH provides information about the mobile wireless entities that it owns and operates, which are mobile virtual network operators Boost Mobile, Republic Wireless, Ting Mobile, and Gen Mobile (collectively, the "DISH MVNOs"), as well as Project Genesis, a facilities-based commercial service offered in more than 120 cities nationwide ("DISH MNO" or "Project Genesis").[3]

DISH does not currently collect and retain geolocation data that would identify individual customers, except for purposes of network performance and optimization as described below.[4] Nor does DISH at this time collect information in a manner that would require any DISH entity to obtain opt-in consent under the Commission's Customer Proprietary Network Information ("CPNI") regulations.[5]

As you know, DISH has made a number of commitments to the Commission to facilitate and expedite its entry into the wireless market as a nationwide facilities-based competitor with a "first-of-its-kind 5G network built from the ground up with an architecture that can take full advantage of expected

[1] DISH Wireless L.L.C. is a wholly owned subsidiary of DISH Network Corporation and submits this response as the relevant corporate entity for its wireless operations.

[2] Letter from FCC Chairwoman Jessica Rosenworcel to DISH Network Corporation President and CEO W. Erik Carlson at 1 (July 19, 2022).

[3] DISH was the first provider to launch VoNR in the U.S. (in its Las Vegas deployment) and we plan to expand VoNR functionality and the sale of VoNR devices to additional markets in the coming months as we optimize the VoNR experience. More information about DISH's Project Genesis offering and facilities-based deployment can be found at 5G Buildout Status Report, Filed by DISH Network Corp., WT Dkt. 22-212 (July 14, 2022) *available at* https://files.fcc.gov/ecfs/download/ca31afd7-0ea5-4d8e-988e-9e0e3c56eb1e?orig=true&pk=cb77b2ec-1a58-dbc6-139b-ad192cfd5d9b.

[4] We interpret your reference to "geolocation data" to refer to data about the location of a device that is determined by technological means, such as tower-location data or devices-based hybrid location methodologies like Assisted GPS ("A-GPS").

[5] *See* 47 C.F.R. § 64.2007(b); 47 C.F.R. § 64.2005(a).

5G functionality."[6] In addition, DISH acquired Boost Mobile in 2020 and has complemented that purchase with acquisitions of several other wireless brands in the two years since. Today, DISH provides a variety of consumer offerings and continues to integrate its various brands into its systems and policies.

Below, DISH provides its responses to the questions raised in your letter. These responses capture DISH's practices as of the date of this letter, but DISH may update its policies consistent with applicable law as its business and operations evolve.

Data Collection, Retention, and Security

Your letter asks a number of questions about DISH's collection and retention of geolocation data. Below we provide information about DISH MVNOs, the DISH MNO, and general practices that cover all DISH consumer wireless offerings.

DISH MVNOs

Like other MVNOs, the DISH MVNOs do not currently use DISH network infrastructure to provide consumer service. Instead, DISH's network partners carry the traffic of DISH's MVNO customers across their respective networks. Because of this architecture, DISH is not able to generate the geolocation data of its MVNO customers from partner networks, and does not otherwise collect such data. Further, DISH neither receives nor obtains geolocation data from the underlying facilities-based carriers that host its MVNO customers. Similarly, compliance with the Commission's Enhanced 911 ("E911") location collection and retention requirements for DISH MVNO customers is the responsibility of the underlying facilities-based carrier that handles DISH MVNO customer traffic. Thus, because DISH MVNOs do not collect and retain geolocation data of their customers,[7] DISH MVNOs do not have a need for policies to retain, share, or destroy such data, nor a need to obtain any customer consent for the above-described purposes.

DISH MNO

DISH collects geolocation data of Project Genesis customers, alongside other device telemetry data, to improve our MNO network performance (*i.e.* for internal network and customer experience optimization). Tower-location data is collected for specific devices at both the network and device-based application levels in the normal course of Project Genesis' network operations, as location information is required to identify and route calls and other traffic. This information is not sold to third parties or otherwise made available to third parties for any use other than improving our MNO network performance.

Project Genesis also collects or will collect information about the location of devices used to make 911 emergency calls, as necessary to comply with E911 location accuracy requirements.[8]

---

[6] Applications of American H Block Wireless L.L.C., DBSD Corporation, Gamma Acquisition L.L.C., and Manifest Wireless L.L.C. for Extension of Time, Order of Modification and Extension of Time to Construct, WT Docket No. 18-197, 35 FCC Rcd 9580, 9585 (WTB 2020).

[7] Boost customers can download the Boost One app, which allows them to opt in to notifications for deals from nearby businesses, such as restaurants. Boost does not cache, store, or retain the location data used to find these deals, and does not share any associated location information with third parties.

[8] *See* 47 C.F.R. § 9.10(i)(2)(i)(A)(4) (horizontal location requirement of 50 meter radius); 47 C.F.R. § 9.10(i)(2)(ii)(H)(I) (vertical location accuracy of ± 3 meters).

Project Genesis shares or will share such information with Public Safety Answering Points (or other answering point that a state or locality has designated to receive 911 calls and route them to emergency services personnel), as required by Commission rules.

Further, Project Genesis follows applicable rules requiring CMRS providers to retain certain information about 911 positioning methods and confidence-and-uncertainty data for a period of two years.[9] Project Genesis also will collect a Registered Location from each VoWiFi customer before activating that service for the customer.[10] Project Genesis plans to retain Registered Locations for as long as a person remains a customer and for at least one year after service is discontinued as proof of compliance and in case a commercial relationship is re-established after, for example, termination for non-payment.

Presently, DISH MNO customers do not have the ability to opt out of DISH retention policies for geolocation data because DISH collects certain geolocation data exclusively for internal network and customer experience optimization, including proper routing of call traffic, or as necessary to comply with applicable laws and regulations. DISH plans to conduct periodic reviews of DISH MNO retention practices to determine whether an opt-out option is appropriate, and to ensure doing so will not negatively impact operations, service quality, or compliance with applicable laws.

General DISH Practices

DISH customers may sometimes decide to use third-party, location-sensitive apps that are available through their devices. Customers may also decide to share device location data via such third-party apps. DISH has no direct involvement in those relationships, and a customer's use of such a third-party app is subject to that app's terms, conditions and policies, including any applicable privacy policies.

DISH's data-deletion policies, which apply to all records (including any records that contain geolocation data) have been established based on the business, billing, and legal needs for the information. As a general matter, when there is no longer any business, billing, or legal need to retain geolocation data, DISH will destroy such information in the normal course, according to its records retention policies. DISH has established a policy that customer information will be destroyed on a rolling basis in a manner that reflects billing and contractual needs, and regulatory record-retention requirements.[11] DISH discloses its data retention policies to subscribers via terms and conditions posted online.

DISH maintains a variety of physical, electronic and procedural safeguards for customer data, which apply to any geolocation data that DISH may obtain. These safeguards help protect personal information from misuse, disclosure, alteration, and destruction. These safeguards include both technical and procedural solutions to ensure consistent attention to movement and storage of sensitive data, including any geolocation data.

---

[9] *See* 47 C.F.R. § 9.10(k). Any geolocation information collected for E911 compliance is retained in accordance with Commission requirements, and is stored separately from other customer records.

[10] *See* 47 C.F.R. § 9.11.

[11] *See*, *e.g.*, 47 C.F.R. § 9.10(k) (requiring CMRS providers to maintain certain information about 911 positioning methods and confidence and uncertainty data for a period of two years); 47 C.F.R. § 9.11 (requiring providers of interconnected VoIP services to obtain a registered location of a user prior to activation of service); 47 C.F.R. § 42.6 (requiring common carriers to retain any telephone toll records for 18 months).

To the extent DISH retains any geolocation data, it is electronically stored within DISH IT systems that are exclusively located in the United States, with industry-standard cybersecurity protocols, policies, and procedures in place. DISH IT systems are subject to comprehensive, industry-standard information security protections including, but not limited to, Intrusion Detection Systems ("IDS"), an Intrusion Prevention Systems ("IPS"), and a Data Loss Prevention ("DLP") system.

To the degree that DISH transmits geolocation information, we would follow DISH's standard process to encrypt the transmission of sensitive information using secure socket layer technology ("SSL"). DISH has also implemented a comprehensive CPNI-compliance program, including regular employee training on acceptable and unacceptable uses of CPNI, consistent with Commission CPNI requirements.

Data Sharing and Consent

Your letter asked a number of questions about process and policies for sharing geolocation information with law enforcement and third parties, as well as customer consent and notice practices.

Pursuant to 47 U.S.C. § 1004 and 47 C.F.R. § 1.20005, DISH has filed a Confidential Systems Security and Integrity report ("SSI Report") at the FCC on behalf of the DISH MNO and DISH MVNOs. DISH incorporates by reference its policies and procedures set forth in that SSI Report. As indicated in the SSI Report, DISH has retained the services of a limited agent to serve as law enforcement agencies' primary point of contact for lawful access to data and records of DISH MVNOs and the DISH MNO, consistent with the Commission's prior approval of the use of this type of agent for lawful-access compliance as a "Trusted Third Party."[12]

Below, we provide information about DISH MVNOs, followed by information about the DISH MNO, and a general practice that covers all DISH consumer wireless offerings.

DISH MVNOs

DISH does not possess any geolocation information for DISH MVNO customers that would be subject to a lawful intercept or a legal demand for historical records because MVNOs by definition are not facilities-based providers. In instances where law enforcement contacts DISH's Trusted Third Party to request the location of a DISH MVNO customer, DISH's Trusted Third Party will refer law enforcement to the underlying facilities-based provider that carries the communications of DISH MVNO customers. It is then up to the facilities-based carrier to validate the lawfulness of the law-enforcement demand and to comply with any required production of information.

DISH MNO

DISH's Trusted Third Party must receive an Appropriate Legal Authorization (as defined in its SSI Report) before providing location information to law enforcement, whether that location information is sought in the context of a lawful intercept under the Electronic Communications

[12] *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360, para. 26 (2006).

Privacy Act of 1986, or whether the lawful demand seeks historical records that may contain geolocation information.[13]

To the extent geolocation data is retained as a record of production of information to law enforcement pursuant to a lawful demand for historical tower information, DISH's policy is to store the data for only two years.

General DISH Practice

There is no need for subscribers to opt out of the sharing of geolocation data specific to a customer because DISH does not share customer-identifying geolocation data with third parties except as required to comply with a valid and lawful legal process or for network optimization. Project Genesis will notify customers of any future sharing of their geolocation information with third parties, consistent with applicable law.

DISH takes the privacy of its customers seriously and is available to answer any additional questions you may have.

/s/ Jeffrey H. Blum
Jeffrey H. Blum

[13] For security reasons, DISH again refers to its SSI Report on file with the Commission for DISH's definition of Appropriate Legal Authorization.