Joan Marsh
Executive Vice President
Federal Regulatory Relations

AT&T Services, Inc.
1120 20th Street, NW
Suite 1000
Washington, DC 20036

T: 202.457.3120
C: 202.262.7479
jm3489@att.com
att.com

August 3, 2022

VIA EMAIL

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

Re: Location Data Retention and Sharing Policies of AT&T Mobility

Dear Chairwoman Rosenworcel:

I am writing in response to your July 19, 2022 letter to AT&T CEO John Stankey seeking information on our policies and practices regarding the retention and sharing of consumer location information. Thank you for your attention to the important issue of consumer data privacy, particularly as it relates to location information. We welcome the opportunity to highlight the robust privacy protections, safeguards, and choices that our customers enjoy when it comes to their personal information.

As you know, consumer location information is collected by many companies other than mobile wireless providers using a variety of technologies that go well beyond customer proprietary network information ("CPNI"), including, for example, device operating systems, GPS or other sensors, applications, and proximity/connection to WiFi hotspots or Bluetooth-enabled devices.

For convenience, this letter will refer to AT&T's postpaid and prepaid wireless affiliates, AT&T Mobility and Cricket Wireless, as "AT&T Mobility." As explained in our easy-to-read privacy policies, accessible at att.com/privacy and cricketwireless.com/privacy, AT&T Mobility is committed to protecting our customers' privacy and securing their information.[1] To that end, our global privacy program is based on four simple principles:

- **Transparency**. We're open and honest about how we use your data.
- **Choices and control**. We give you choices about how we use your data.
- **Security**. We use strong safeguards to keep your data confidential and secure.
- **Integrity**. We do what we say.

[1] The privacy policies of AT&T Mobility and Cricket Wireless extend the same substantive protections and, in this letter, will be referred to collectively as our "Privacy Policy."

We therefore agree that practices governing the retention and sharing of customers' location information are "of utmost importance to consumer safety and privacy," and we are pleased to provide the information below in response to your questions.

* * * * *

To serve its customers, AT&T Mobility collects CPNI location information that is the subject of this letter in two primary ways:[2]

> *Cell Towers*. AT&T Mobility collects network location information from the cellular towers used to power AT&T Mobility's wireless network. This information identifies which cell sites are used by the devices on AT&T Mobility's network and thus enables AT&T to provide wireless connectivity using those devices.
>
> *IQI Software*. IQI software, developed and owned by AT&T, is embedded in the firmware of Android devices by original equipment manufacturers ("OEMs"). It collects device diagnostic and location data on a passive basis (*e.g.*, when a device powers on or contacts a new cell tower), including latitude/longitude information. AT&T Mobility uses IQI software to improve network performance and for customer service purposes. For example, AT&T Mobility uses data derived from IQI software to identify areas where it needs to enhance network coverage. AT&T Mobility does not share IQI data except where legally required, nor do we use it for advertising purposes.

As explained in our Privacy Policy, we use information collected from customers, including location data, together with the information from testing and running our network, to power our services and to improve customers' experiences.[3] This includes:

> *Provisioning Service*. To serve our customers, AT&T Mobility must and does collect location information. For example, AT&T Mobility collects the location of a person's device to direct a cell tower to provide telecommunications, as well as emergency 911 support.
>
> *Network Security and Anti-Fraud Efforts*. AT&T Mobility uses location information to prevent fraud and ensure the security of customer devices connected to AT&T Mobility's networks. For example, AT&T Mobility uses such information to ensure that users on AT&T Mobility's networks are legitimate AT&T subscribers and not malicious actors and to notify affected customers if it detects network-security threats.

---

[2] *See* 47 U.S.C. § 222(h)(1) (defining "customer proprietary network information").

[3] For these reasons, as detailed below, AT&T Mobility's retention policies and practices apply to customers without exception.

Strengthen Network and Improve Services. AT&T Mobility uses location information to ensure that AT&T's mobile telecommunications and other networks are operating effectively, to troubleshoot networks, and to improve products and services. For example, AT&T Mobility uses device location information to determine whether network signal strength is low in specific geographic locations or the network has insufficient bandwidth to serve all customers in an area.

Advertising. In addition to first-party marketing of AT&T Mobility's own products and services, AT&T Mobility postpaid customers can choose to participate in Relevant Advertising ("RA"), which is an opt-out advertising program, and Enhanced Relevant Advertising ("ERA"), which is an opt-in advertising program. Customers are free to change their RA and ERA preferences at any time.

Each AT&T Mobility customer receives the AT&T Privacy Policy, which informs the customer of the criteria used to determine our practices governing retention and data destruction. The AT&T Privacy Policy is also available on our website.

The AT&T Mobility systems of record that house customer geolocation information are electronically stored in the United States. In addition, AT&T Mobility applies robust protections to all customer data, including location information. These protections are detailed in our Network and Data Security Issue Brief and include, among others:

AT&T Code of Business Conduct, which requires all AT&T personnel to protect the privacy of our customers' communications and to comply with the law and AT&T's internal policies and procedures regarding the collection, retention, and use of personal information.

AT&T Security Policy and Requirements ("ASPR"), which establish information security requirements for treatment of data, including location information. ASPR generally requires the encryption of location data and establishes baseline control standards that apply to specific operating systems, databases, platforms, and other technical areas to, among other things, limit access to such systems to authorized individuals.[4]

AT&T Information Security Policy, which applies to all forms of information, infrastructure, and services ("AT&T's Information Resources") that are created, used,

[4] ASPR is a comprehensive set of security control standards based, in part, on leading industry standards such as ISO/IEC 27001:2013. ASPR also aligns with laws and standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST 800-53, as well as the European Union's General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS) Security Policy, and the California Consumer Privacy Act (CCPA).

or maintained by or on behalf of AT&T or its customers unless specifically superseded by customer contract. AT&T personnel may access AT&T information, including location information, only as authorized by AT&T and only for those purposes that are required to perform assigned job duties. AT&T personnel must immediately report any unauthorized access or suspicious activity to the AT&T Chief Security Office. Further, all AT&T infrastructure and services must be designed and administered in compliance with ASPR to ensure AT&T's Information Resources apply security controls, commensurate with the classification of the information, to prevent accidental or malicious exposure. AT&T Information Resources must positively and uniquely identify and authenticate individual users prior to granting access. All AT&T Information Resources (*e.g.*, servers, personal computers, routers, databases, smartphones, and websites) must register for threat notifications and have antivirus software installed and running.

AT&T Supplier Information Security Requirements, which are a detailed set of data security requirements that AT&T applies to suppliers and includes, among others, requirements for encryption, physical and network security, access authentication, monitoring, and data access management.

AT&T Record Information Management ("RIM") Policy, which sets standards on the creation, storage, retention, and destruction of records, including records containing personal data. Subject to requirements of legal holds, AT&T personnel are responsible for retaining and disposing of records according to AT&T's retention schedules, as well as protecting records from unauthorized access, use, or disclosure. All AT&T personnel who create and retain records containing personal information are responsible for maintaining the records' security at all stages of the records' life cycle, including using secure disposal methods at the disposition stage. Our RIM Policy establishes a retention period of no more than 13 months for information that identifies the current or past location of a specific individual's device and five years for historical call detail records, which include cell site location information.

Like all companies, we are required by law to provide information to law enforcement and other government entities by complying with court orders, subpoenas, and lawful discovery requests. In all cases, we review requests to determine whether they are valid. We require a search warrant based on the probable cause standard for all law enforcement demands for real-time or historical location information, except for exigent requests, such as emergency requests related to kidnappings, missing person cases, and attempted suicides. AT&T's Global Legal Demand Center includes a team dedicated to reviewing and responding to exigent requests from law enforcement.

AT&T Mobility may share real-time location data with public service answering points ("PSAPs"), other emergency service providers, and/or the customer's legal guardian or

immediate family when the exigent services exceptions of Section 222 apply.[5] In addition, unless a state law prohibits such disclosure, AT&T Mobility is required to respond to valid subpoena demands from civil litigants or criminal defendants for call detail records, which in the case of AT&T Mobility may include location information.[6] AT&T Mobility customers may not opt out of sharing location information with law enforcement, emergency services providers, or when a valid subpoena compels such disclosure. AT&T Mobility's practice is to provide notice to customers and an opportunity to object when a customer's records are the target of a civil or criminal defense subpoena to the extent such notice is legally permissible. We do not share location data with location aggregators and location-based service providers,[7] and we would not share such data with other third parties without our customer's consent.[8]

* * * * *

We value our customers' trust. Our commitment to customers' privacy and the security of their personal information—including location information—is unwavering. We accordingly note our strong disagreement with the unfair characterizations made in the Federal Trade Commission's Staff Report on the privacy practices of internet service providers ("ISPs")[9] and vigorously contest the factually and legally flawed—and, as yet, unresolved—determinations made in the Notice of Apparent Liability regarding location-based services.[10]

---

[5] 47 U.S.C. §§ 222(d)(4), (f). When a customer calls 911, AT&T Mobility transmits OEM-supplied device-based hybrid location information to the PSAP when such information is available and valid. If not, AT&T Mobility provides cell tower location information from its network.

[6] *See* 47 C.F.R. § 64.2003(d).

[7] *See* Letter from Joan Marsh, AT&T, to the Honorable Jessica Rosenworcel (May 15, 2019), https://docs.fcc.gov/public/attachments/DOC-357494A2.pdf.

[8] In addition to the CPNI location information discussed above, AT&T may collect other location information—*e.g.*, through applications it offers or in connection with its role as a WiFi service provider.

[9] Federal Trade Commission, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, An FTC Staff Report (Oct. 21, 2021), https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers.

[10] *See AT&T Inc.*, Brief of AT&T in Response to Notice of Apparent Liability Concerning Location-Based Services (filed May 7, 2020); *AT&T Inc.*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743 (2020).

We appreciate the opportunity of this response to set the record straight. Should you have further questions, please do not hesitate to contact me.

Respectfully submitted,

Joan Marsh
Executive Vice President
Federal Regulatory Relations
AT&T Services, Inc.