FCC NEWS from the Federal Communications Commission

Media Contact:
MediaRelations@fcc.gov

For Immediate Release

FCC FINES AT&T, SPRINT, T-MOBILE, AND VERIZON NEARLY $200 MILLION FOR ILLEGALLY SHARING ACCESS TO CUSTOMERS' LOCATION DATA

Carriers Sold Access to Location Data to Third Parties Without Customer Consent and Continued to Do So Without Reasonable Safeguards

WASHINGTON, April 29, 2024—Today, the Federal Communications Commission fined the nation's largest wireless carriers for illegally sharing access to customers' location information without consent and without taking reasonable measures to protect that information against unauthorized disclosure. Sprint and T-Mobile – which have merged since the investigation began – face fines of more than $12 million and $80 million, respectively. AT&T is fined more than $57 million, and Verizon is fined almost $47 million.

"Our communications providers have access to some of the most sensitive information about us. These carriers failed to protect the information entrusted to them. Here, we are talking about some of the most sensitive data in their possession: customers' real-time location information, revealing where they go and who they are," **said FCC Chairwoman Jessica Rosenworcel**. "As we resolve these cases – which were first proposed by the last Administration – the Commission remains committed to holding all carriers accountable and making sure they fulfill their obligations to their customers as stewards of this most private data."

In 2018, U.S. Senator Ron Wyden first highlighted the use case which launched the agency's investigation and the legal concerns stemming from it in a public letter to its leadership. The FCC Enforcement Bureau investigations of the four carriers found that each carrier sold access to its customers' location information to "aggregators," who then resold access to such information to third-party location-based service providers. In doing so, each carrier attempted to offload its obligations to obtain customer consent onto downstream recipients of location information, which in many instances meant that no valid customer consent was obtained. This initial failure was compounded when, after becoming aware that their safeguards were ineffective, the carriers continued to sell access to location information without taking reasonable measures to protect it from unauthorized access.

Under the law, including section 222 of the Communications Act, carriers are required to take reasonable measures to protect certain customer information, including location information. Carriers are also required to maintain the confidentiality of such customer information and to obtain affirmative, express customer consent before using, disclosing, or allowing access to such information. These obligations apply equally when carriers share customer information with third parties.

"The protection and use of sensitive personal data such as location information is sacrosanct," **said Loyaan A. Egal, Chief of the FCC Enforcement Bureau and Chair of its Privacy and**

Data Protection Task Force. "When placed in the wrong hands or used for nefarious purposes, it puts all of us at risk. Foreign adversaries and cybercriminals have prioritized getting their hands on this information, and that is why ensuring service providers have reasonable protections in place to safeguard customer location data and valid consent for its use is of the highest priority for the Enforcement Bureau."

The investigations that led to today's fines started following public reports that customers' location information was being disclosed by the largest American wireless carriers without customer consent or other legal authorization to a Missouri Sheriff through a "location-finding service" operated by Securus, a provider of communications services to correctional facilities, to track the location of numerous individuals. Yet, even after being made aware of this unauthorized access, all four carriers continued to operate their programs without putting in place reasonable safeguards to ensure that the dozens of location-based service providers with access to their customers' location information were actually obtaining customer consent.

The Forfeiture Orders announced today finalize Notices of Apparent Liability (NAL) issued against these carriers in February 2020. The fine amount for AT&T and Sprint are unchanged since the NAL stage. Both the T-Mobile and Verizon fines were reduced following further review of the parties' submissions in response to the NALs. The law does not permit forfeiture amounts for specified violations to escalate after issuance of an NAL.

The Forfeiture Orders are available here:

- AT&T, Inc. Forfeiture Order: https://www.fcc.gov/document/fcc-fines-att-57m-location-data-violations
- Sprint Corporation Forfeiture Order: https://www.fcc.gov/document/fcc-fines-sprint-12m-location-data-violations
- T-Mobile USA, Inc. Forfeiture Order: https://www.fcc.gov/document/fcc-fines-t-mobile-80m-location-data-violations
- Verizon Communications Forfeiture Order: https://www.fcc.gov/document/fcc-fines-verizon-46m-location-data-violations

In 2023, the Chairwoman established the Privacy and Data Protection Task Force, an FCC staff working group focused on coordinating across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors, including data breaches (such as those involving telecommunications providers) and vulnerabilities involving third-party vendors that service regulated communications providers. More information on the Task Force is available at: https://www.fcc.gov/privacy-and-data-protection-task-force.

###