Timothy P. McKone
Executive Vice President
Federal Relations

AT&T Services, Inc.
1120 20th Street, NW
Suite 800
Washington, DC 20036

T 202.463.4144
tm3703@att.com
att.com

June 15, 2018

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter dated May 8, 2018 regarding a real-time location service that another company, Securus Technologies, Inc. ("Securus"), was apparently providing to law enforcement officials. AT&T takes the concerns you raise in your letter seriously and I can assure you that AT&T values and respects its customers' privacy.

AT&T has never authorized the use of its customer data for the Securus web portal service described in your letter. We are actively investigating the extent to which Securus may have obtained unauthorized access to AT&T customer location data, and we are pressing Securus to provide greater cooperation than they have to this point. Our top priority is to protect our customers' information, and, to that end, we have suspended all access by Securus to AT&T customer location data.

We provide below a summary of the facts based on AT&T's continuing investigation.

Background

AT&T permits authorized third parties to access customer location data for location-based services ("LBS") only where a customer consents to such disclosure except in limited cases where a specific provision of law or regulation requires or authorizes access.[1] For instance, AT&T permits roadside assistance companies to access customer location data to find stranded motorists. Other examples include bank-fraud prevention by ensuring the customer is present when making financial transactions, shipment tracking to provide estimated arrival times, and services that help emergency responders locate victims.[2]

To facilitate these services, an intermediary company known as an "aggregator" typically manages requests for customer data across multiple carriers. For example, when customers request emergency roadside assistance and consent to the disclosure of their location data, the roadside assistance company sends the request to an aggregator to identify the carrier from which

[1] The CTIA LBS Guidelines provide examples of where provisions of law do not require consent under its discussion of "Scope of Coverage." See CTIA "Best Practices and Guidelines for Location Based Services," *available at* https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.

[2] *See* CTIA LBS Guidelines.

location data needs to be requested. Without an aggregator, there would be no practical and efficient method to facilitate requests across different carriers.

Such practices are common among all major carriers. Under the CTIA LBS Guidelines, which AT&T contractually requires all aggregators to follow, LBS providers (such as Securus) are required to give customers notice and obtain consent to use location information.[3] As we describe below, AT&T did not authorize Securus's collection of customer data for its self-service web portal.

The Approved Inmate Calling Service

In October 2012, an aggregator named LocationSmart (then called Locaid) sought AT&T's approval for a prison inmate calling service. Under the use case, LocationSmart's customer, 3Cinteractive, a provider of mobile collect calling service, would share location information with prison officials through prison telecommunications provider Securus (the "Inmate Calling Service"). When a wireless customer receives a call from an inmate, the customer hears an IVR message requesting affirmative consent to share phone location information for investigative purposes. We understand the correctional facility uses the location information for security purposes, such as to counter schemes involving prisoner escapes or contraband deliveries. AT&T imposed contractual requirements on LocationSmart requiring it to collect consent for each location request; comply with data security requirements; comply with all applicable laws; and maintain a record of consent for each location request.

The Unapproved Securus On-Demand Service

The Securus service discussed in your letter relates to a different – and unapproved – use of AT&T location information. We understand that this program involves the provision of location information to certain law enforcement officials, namely correctional officers at prison facilities, in response to warrants or other lawful demands (the "On Demand Service"). AT&T was not informed of the On-Demand Service and never approved it. Based on our preliminary assessment, it appears that the On-Demand location requests comprised a tiny fraction – less than two tenths of one percent – of the total requests Securus submitted for the approved Inmate Calling Service.

We now understand that, despite AT&T's requirements to obtain customer consent, Securus did not in fact obtain customer consent before collecting customers' location information for its On-Demand Service. Instead, Securus evidently relied upon law enforcement's representation that it had appropriate legal authority to obtain customer location data, such as a warrant, court order, or other authorizing document as a proxy for customer

[3] See CTIA LBS Guidelines.

consent. Despite this fundamental departure from the approved Inmate Calling Service, and without ever informing AT&T of the new service, Securus apparently used the process established for the Inmate Calling Service to provide its On-Demand Service. Consequently, AT&T received confirmation that Securus had obtained consent for each request for location information, which AT&T understood were all related to the approved Inmate Calling Service. Indeed, even if the incoming request for location information to Securus was duly authorized by law, AT&T did not authorize Securus to access AT&T customer location information except in connection with the Inmate Calling Service.

After learning about the Securus On-Demand Service, AT&T took prompt steps to protect customer data and shut down 3Cinteractive and Securus's access to AT&T customer location data. On May 10, 2018, within two days of receiving your letter, AT&T terminated Securus's access to customer information in connection with the On-Demand Service. And on May 16, 2018, after learning that Securus may have suffered a data breach that compromised the log-in credentials of its corrections and law enforcement customers, AT&T suspended the provision of all customer location information to Securus for any purpose, including the Inmate Calling Service.

AT&T has no reason to believe that there are other instances of unauthorized access to AT&T customer location data. Nonetheless, we are reviewing these issues carefully to ensure the proper handling of all AT&T customer information.

Thank you again for raising with us this important area of shared concern.

Sincerely,