United States Senate
WASHINGTON, DC 20510

May 21, 2015

Randall L. Stephenson
Chairman and Chief Executive Officer
AT&T Inc.
208 S. Akard St.
Dallas, TX 75202

Dear Mr. Stephenson:

As mobile device usage continues to increase in our country, we have seen how cell phone information serves an important role in assisting law enforcement's efforts to protect Americans and bring wrongdoers to justice. We have also learned how wireless carriers play a critical role in helping law enforcement with their investigations, and I continue to appreciate your continued commitment to serving the public.

I have previously sent to your company and the country's other major wireless carriers questions asking about your policies for sharing customers' mobile phone information with law enforcement agencies. Your responses proved invaluable in understanding these practices. In a first-ever accounting of its kind, the carriers reported over one million federal, state, and local law enforcement requests for cell phone records were made in both 2011 and 2012. According to the responses I received from your company and the others, information shared with law enforcement includes a wide range of data including geolocation information, content of text messages, and wiretaps.

Your company has also taken the important step of publishing regular transparency reports that help inform Americans about the nature and extent of wireless surveillance. I commend your company for making these disclosures and have urged other companies to do the same.

I respectfully request that you submit records for the years 2013 and 2014. I ask that you provide answers to the following questions:

1. In 2013 and 2014, respectively, how many total requests did your company receive from law enforcement to provide information about your customers' phone usage? Please include *separate* information for each of the two calendar years. While I appreciate your company publishing regular transparency reports, I am requesting this information in this form so I can best understand and compare all participants in the marketplace.

    a. Within that total, please list the amount of requests your company received for <u>each</u> type of usage, including but not limited to the following: 1) Geolocation of device (please distinguish between historical and real-time); 2) Call detail records (please distinguish between historical and real-time) (i.e., pen register and trap and trace); 3) Text message content; 4) Voicemail; 5) Cell tower dumps; 6)

Wiretapping; 7) Subscriber information; 8) Data requests (e.g., information on URLs visited).

b. Within that total, how many of the requests were made in emergency circumstances, and how many were in non-emergency situations?

c. Within that total, how many of the requests did your company fulfill and how many did it deny? If it denied any requests, for what reasons did it issue those denials?

d. Within that total, please breakdown how many of the requests were made by Federal authorities, how many by state authorities, and how many by local authorities.

e. Within that total, please break down how many of the requests were civil and how many were criminal.

2. For each type of usage in 1(a), how long does your company retain the records?

3. What is the average amount of time law enforcement requests for one cell tower dump (e.g., one hour, 90 minutes, two hours, etc.)? For each hour of a cell tower dump that your company provides, on average, how many mobile device numbers are turned over to law enforcement?

4. What protocol or procedure does your company employ when receiving these requests?

   a. What legal standard do you require law enforcement to meet for each type of usage in 1(a)?

   b. After the Sixth Circuit Court of Appeals held in *United States v. Warshak* that stored content, such as email messages, is protected by the 4th Amendment, many major email and cloud computing providers established policies insisting on warrants before disclosing such communications to law enforcement. Does your company require a warrant before disclosing content, such as stored emails, text messages or voicemail messages? If no, why not and what legal standard do you require?

   c. The State Supreme Courts of Massachusetts, New Jersey, and Florida have ruled that cellular location data (either real-time, historical, or both) are subject to warrant-based protections under the laws. At the same time, some states have also passed laws protecting location data. How does your company address the variety of different state and federal rules regarding access to location data? Specifically:

i. Does your company require a warrant before disclosing location records generated by phones in states that have legislative or judicial location data protections?

ii. What form of legal process does your company require before disclosing location records generated by devices outside the states that have location data protections?

iii. Do you require a warrant for cell tower dumps in states that have location data protections?

d. Does your company distinguish between emergency cell phone tracking requests from law enforcement and non-emergency tracking requests? If yes, what are the distinctions?

e. Have any of these practices changed since your 2013 correspondence with my office?

5. Has your company seen a recent rise in requests for emergency circumstances? If yes, do you attribute that rise to an actual increase in emergencies or a changed definition of what qualifies as an emergency, or some other reason?

6. Does your company notify subscribers about government requests for their information? If yes, please explain how. If no, why not? If no, is your company considering changing this policy?

7. Did your company encounter misuse of cell phone tracking by law enforcement authorities during 2013 or 2014? If yes, in what ways has tracking been misused? And if yes, how has your company responded?

8. Does your company have knowledge of law enforcement authorities that use their own tracking equipment (e.g., Stingray phone trackers)? If yes, please explain.

a. Does your company cooperate with law enforcement that uses its own tracking equipment? If yes, how?

b. Does your company have knowledge of whether law enforcement uses information obtained by carriers in conjunction with information gathered from law enforcement's own tracking equipment?

9. Did your company receive requests or demands from law enforcement for assistance installing surveillance software on the mobile devices or computers of a target? If yes, what assistance, if any, did your company provide?

10. Did your company receive requests or demands from law enforcement for assistance remotely activating the microphone in a target's phone? If yes, what assistance, if any, did you provide?

11. Did your company receive requests or demands from law enforcement for encryption keys, including the unique encryption keys stored on customer SIM cards which would enable the decryption of customer communications? If yes, what assistance, if any, did your company provide?

12. Did your company receive "community of interest" (e.g., information about the person with whom the target communicates) requests or demands from law enforcement? If yes, did your company provide those records? If yes, how many times in each calendar year was community of interest records provided?

13. In 2013 and 2014, respectively, did your company receive money or other forms of compensation in exchange for providing information to law enforcement? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?

    a. Does your company charge different amounts depending upon whether the request is for emergency or non-emergency purposes? Does your company charge fees for emergency cell phone tracking requests by law enforcement authorities?

    b. Please include any written schedule of any fees that your company charges law enforcement for these services.

Thank you for your attention to this important matter. Please provide written responses to these questions no later than June 11, 2015. If you have any questions, please have a member of your staff contact Joseph Wender at 202-224-2742.

Sincerely,

Edward J. Markey

Edward J. Markey
United States Senator