Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

May 1, 2019

John Donovan, CEO
AT&T Communications
208 S. Akard Street, Suite 2954
Dallas, TX 75202

Dear Mr. Donovan:

In January of this year, a reporter was able to identify the exact location of a smartphone using only the phone number and a $300 payment to a bounty hunter. The ensuing journalistic investigation revealed that a wireless carrier sold an individual's real-time location data to a data aggregator, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to an independent bounty hunter. The investigation further revealed that every major wireless carrier in the United States may have sold location data to aggregators, making consumers' real-time location information available to hundreds of bounty hunters.

Then in February of this year, press reports revealed that wireless carriers may also have sold assisted or augmented global positioning system location data. A-GPS data is more precise location data that is collected for use with enhanced 911 services to allow first responders to pinpoint an individual's location with greater accuracy. Under federal law, A-GPS data included in the National Emergency Address Database for enhanced 911 services may not be used for any other purpose.

Real-time location information is sensitive data deserving the highest level of privacy protection. But it is evident from press reports that this data may have been sold without the explicit consent of consumers and without appropriate safeguards in place.

Accordingly, I appreciate your decision to end these location aggregation services by March of this year. To that end, I kindly request that you provide an update on your efforts and confirm by what date AT&T ended its arrangements to sell the location data of its customers. Please also confirm whether and by what date the company ended arrangements to sell assisted or augmented GPS data.

Finally, the public still has very little detail about how much geolocation data is being saved and stored—including in ways that may be far too accessible to others. Even de-anonymized location data may be combined with other information in ways that could make it personally identifiable again. Accordingly, please explain whether AT&T's agreements permitted aggregators or others to save and store location data they received from your company. If so, please confirm what steps your company is taking to ensure that these companies delete or destroy previously shared data and any derivative data. Alternatively, please explain what steps

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

AT&T is taking to safeguard such data from use or onward sale that is inconsistent with consumers' original consent.

Please send your response to the undersigned via email (Jessica.Rosenworcel@fcc.gov) by May 15, 2019.

Sincerely,

Jessica Rosenworcel

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

May 1, 2019

Michel Combes, CEO
Sprint
6200 Sprint Parkway
Overland Park, KS 66251

Dear Mr. Combes:

In January of this year, a reporter was able to identify the exact location of a smartphone using only the phone number and a $300 payment to a bounty hunter. The ensuing journalistic investigation revealed that a wireless carrier sold an individual's real-time location data to a data aggregator, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to an independent bounty hunter. The investigation further revealed that every major wireless carrier in the United States may have sold location data to aggregators, making consumers' real-time location information available to hundreds of bounty hunters.

Then in February of this year, press reports revealed that wireless carriers may also have sold assisted or augmented global positioning system location data. A-GPS data is more precise location data that is collected for use with enhanced 911 services to allow first responders to pinpoint an individual's location with greater accuracy. Under federal law, A-GPS data included in the National Emergency Address Database for enhanced 911 services may not be used for any other purpose.

Real-time location information is sensitive data deserving the highest level of privacy protection. But it is evident from press reports that this data may have been sold without the explicit consent of consumers and without appropriate safeguards in place.

Accordingly, I appreciate your decision to end these location aggregation services by May 31. To that end, I kindly request that you provide an update on your efforts to meet this timeline. Please also confirm whether the company will end arrangements to sell assisted or augmented GPS data by that date.

Finally, the public still has very little detail about how much geolocation data is being saved and stored—including in ways that may be far too accessible to others. Even de-anonymized location data may be combined with other information in ways that could make it personally identifiable again. Accordingly, please explain whether Sprint's agreements permitted or currently permit aggregators or others to save and store location data they received from your company. If so, please confirm what steps your company is taking to ensure that these companies delete or destroy previously shared data and any derivative data. Alternatively,

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

please explain what steps Sprint is taking to safeguard such data from use or onward sale that is inconsistent with consumers' original consent.

Please send your response to the undersigned via email (Jessica.Rosenworcel@fcc.gov) by May 15, 2019.

Sincerely,

Jessica Rosenworcel

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

May 1, 2019

John Legere, CEO
T-Mobile US. Inc.
12920 SE 38th Street
Bellevue, WA 98006

Dear Mr. Legere:

In January of this year, a reporter was able to identify the exact location of a smartphone using only the phone number and a $300 payment to a bounty hunter. The ensuing journalistic investigation revealed that a wireless carrier sold an individual's real-time location data to a data aggregator, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to an independent bounty hunter. The investigation further revealed that every major wireless carrier in the United States may have sold location data to aggregators, making consumers' real-time location information available to hundreds of bounty hunters.

Then in February of this year, press reports revealed that wireless carriers may also have sold assisted or augmented global positioning system location data. A-GPS data is more precise location data that is collected for use with enhanced 911 services to allow first responders to pinpoint an individual's location with greater accuracy. Under federal law, A-GPS data included in the National Emergency Address Database for enhanced 911 services may not be used for any other purpose.

Real-time location information is sensitive data deserving the highest level of privacy protection. But it is evident from press reports that this data may have been sold without the explicit consent of consumers and without appropriate safeguards in place.

Accordingly, I appreciate your decision to end these location aggregation services by March of this year. To that end, I kindly request that you provide an update on your efforts and confirm by what date T-Mobile ended its arrangements to sell the location data of its customers. Please also confirm whether and by what date the company ended arrangements to sell assisted or augmented GPS data.

Finally, the public still has very little detail about how much geolocation data is being saved and stored—including in ways that may be far too accessible to others. Even de-anonymized location data may be combined with other information in ways that could make it personally identifiable again. Accordingly, please explain whether T-Mobile's agreements permitted aggregators or others to save and store location data they received from your company. If so, please confirm what steps your company is taking to ensure that these companies delete or destroy previously shared data and any derivative data. Alternatively, please explain what steps

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

T-Mobile is taking to safeguard such data from use or onward sale that is inconsistent with consumers' original consent.

Please send your response to the undersigned via email (Jessica.Rosenworcel@fcc.gov) by May 15, 2019.

Sincerely,

Jessica Rosenworcel

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

May 1, 2019

Hans Vestberg, CEO
Verizon
1095 Avenue of the Americas
New York, NY 10013

Dear Mr. Vestberg:

In January of this year, a reporter was able to identify the exact location of a smartphone using only the phone number and a $300 payment to a bounty hunter. The ensuing journalistic investigation revealed that a wireless carrier sold an individual's real-time location data to a data aggregator, who then sold it to a skip-tracing firm, who then sold it to a bail-bond company, who then sold it to an independent bounty hunter. The investigation further revealed that every major wireless carrier in the United States may have sold location data to aggregators, making consumers' real-time location information available to hundreds of bounty hunters.

Then in February of this year, press reports revealed that wireless carriers may also have sold assisted or augmented global positioning system location data. A-GPS data is more precise location data that is collected for use with enhanced 911 services to allow first responders to pinpoint an individual's location with greater accuracy. Under federal law, A-GPS data included in the National Emergency Address Database for enhanced 911 services may not be used for any other purpose.

Real-time location information is sensitive data deserving the highest level of privacy protection. But it is evident from press reports that this data may have been sold without the explicit consent of consumers and without appropriate safeguards in place.

Accordingly, I appreciate your decision to end these location aggregation services this year. To that end, I kindly request that you provide an update on your efforts and confirm by what date Verizon ended its arrangements to sell the location data of its customers. Please also confirm whether and by what date the company ended arrangements to sell assisted or augmented GPS data.

Finally, the public still has very little detail about how much geolocation data is being saved and stored—including in ways that may be far too accessible to others. Even de-anonymized location data may be combined with other information in ways that could make it personally identifiable again. Accordingly, please explain whether Verizon's agreements permitted aggregators or others to save and store location data they received from your company. If so, please confirm what steps your company is taking to ensure that these companies delete or destroy previously shared data and any derivative data. Alternatively,

Federal Communications Commission
Washington, D.C. 20554

Jessica Rosenworcel
Commissioner

please explain what steps Verizon is taking to safeguard such data from use or onward sale that is inconsistent with consumers' original consent.

Please send your response to the undersigned via email (Jessica.Rosenworcel@fcc.gov) by May 15, 2019.

Sincerely,

Jessica Rosenworcel