STATEMENT OF COMMISSIONER GEOFFREY STARKS
APPROVING IN PART AND DISSENTING IN PART

Re: *AT&T Inc.*, File No.: EB-TCD-18-00027704.

Taking control of our personal information is one of the defining civil rights issues of our generation. Practically every day, we learn about new data harms: algorithmic and facial recognition bias; companies failing to protect our most sensitive information from hackers and thieves; and "pay to track" schemes that sell location information to third parties. These practices put all Americans at risk, and they are especially insidious because they replicate and deepen existing inequalities in our society.

In recent months, consumers have become increasingly aware of how much private information trails behind them as they go about their days. In December 2019, the New York Times opinion series *One Nation, Tracked* brought renewed focus to the issue of smartphone tracking.[1] Their stories illustrated, sometimes in frightening detail, how much can be learned about a person from the location of their smartphone. Using supposedly anonymous location data, the Times was able to follow the movements of identifiable Americans, from a singer who performed at President Trump's inauguration to President Trump himself.

The findings by journalists at the New York Times, Motherboard, and many other outlets unsettle us for good reason. Your location at any time goes to the heart of personhood—where you live, who you see, where you go, and where you worship. And tracking over time can build a picture of a life in intimate detail. Disclosure of those coordinates and patterns isn't just creepy; it can leave us vulnerable to safety threats and intrusions never before possible on such a comprehensive scale. And because people of color rely more heavily on smartphones for internet access than other Americans, they bear these harms disproportionately.

For those "freaked out" by their reporting, the Times offered a number of steps consumers can take to limit access to the location data, including blocking location sharing and disabling mobile advertising IDs. Those can be good steps, but they are no defense against your wireless carrier. Your carrier needs to know where you are to complete your calls. Because it is simply impossible to use a mobile phone—an important part of participation in our modern economy—without giving location data to one of the carriers, our rules about how that they can use customer location data must be strict and strictly enforced.

For that reason, I am pleased that the Notices of Apparent Liability we vote on today confirm that misuse of customer location data by AT&T, Verizon, Sprint, and T-Mobile violate the Commission's rules. These serious violations damaged Americans' faith in our telephone system, and I am pleased that we have reached bipartisan agreement that enforcement is appropriate here. I cannot fully approve these Notices, however, because in conducting these investigations and determining the appropriate penalty, we lost track of the most important part of our case—the very consumers we are charged with protecting. Because I strongly believe we should have determined the number of customers impacted by the abuses and based our forfeiture calculations on that data—calculations that would have been possible if we had investigated more aggressively—I must dissent in all remaining parts of the item.

[1] Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times (Dec. 19, 2019).

Enforcement Authority

Congress has clearly directed carriers to protect our location information, and these Notices confirm that this protection exists even when no call is in progress. Going forward, there should be no dispute about this basic legal conclusion.

This is a responsibility that can't be delegated away. Carriers are responsible for the actions of their agents and sub-contractors. This is a well-established principle, and it recognizes the special nature of the customer-carrier relationship. We trust our wireless carrier to provide high-quality service, and we don't expect that our carrier is going to monetize that relationship.

None of these carriers should be surprised that we take the protection of customer data so seriously. In 2007, the Commission addressed the problem of "pretexting," where data brokers would impersonate customers to fool carriers into disclosing confidential customer information. We revamped our rules and, for the first time, required that carriers obtain "opt-in" consent to the disclosure of customer information, rather than presenting it as an "opt-out."

Regrettably, these investigations show that carriers did not heed that warning. Despite the clear message from the FCC, these carriers did not treat the protection of their customers' data as a key responsibility. Instead, they delegated responsibility for protecting this sensitive information to aggregators and third-party location service providers. They subjected these arrangements to varying degrees of oversight, but all were ineffective and failed to prevent the problem. Significant penalties are more than justified.[2]

Delays

Today's action has been too long delayed. As the Notices point out, the Commission has been investigating these matters for nearly two years. And the investigations show that, even after the problems with their location data sharing programs became readily apparent, the carriers took months to shut them down. Indeed, nearly one year ago, I published an op-ed in the NY Times about the slow pace of this investigation, and the need for the FCC to "act swiftly and decisively to stop illegal and dangerous pay-to-track practices."[3] I had no idea it would be another 11 months before we finally acted.

From the beginning, it has been difficult to get the facts straight. The carriers repeatedly told the public that they were stopping their location sharing program while hiding behind evasive language and contractual terms. For example, on June 15, 2018, Verizon told Senator Ron Wyden, "[w]e are initiating a process to terminate our existing agreements for the location aggregator program."[4] But Verizon didn't terminate its aggregator agreements until November 2018, and didn't end all of its location data sharing

[2] In fact, just a few years ago, the Enforcement Bureau entered into multi-million-dollar consent decrees with these same carriers involving a similar problem— the unauthorized billing of customers by third-party vendors where the carriers sought to delegate their consumer protection responsibility via contract. As in the cases at issue here, the carriers claimed that they weren't responsible for unlawful billing because their contracts had requirements placing any responsibility on the downstream companies. The carriers we find liable today did a fundamental disservice to their customers when they simply "passed the buck" to these location data aggregators and service providers. Failure to supervise their agents is no defense. *See Cellco Partnership d/b/a Verizon Wireless,* Order and Consent Decree, 30 FCC Rcd 4590 (Enf. Bur. 2015) (requiring $90 million in payments and restitution to consumers to settle allegations that Verizon charged consumers for third-party products and services that the consumers did not authorize; *Sprint Corp.,* Order and Consent Decree, 30 FCC Rcd 4575 (Enf. Bur. 2015) ($68 million); *AT&T Mobility LLC,* Order and Consent Decree, 29 FCC Rcd 11803 (Enf. Bur. 2014) (($105 million); *T-Mobile USA, Inc.*, Order and Consent Decree, 29 FCC Rcd 15111 (Enf. Bur. 2014) ($90 million).

[3] Geoffrey Starks, "Why It's So Easy for a Bounty Hunter to Find You," New York Times (April 19, 2019).

[4] Letter from Karen Zacharia, Chief Privacy Officer, Verizon, to Senator Ron Wyden, dated June 15, 2018.

programs until April 2019. With respect to the other carriers, on June 19, 2018, the Washington Post reported:

> AT&T then said in a statement Tuesday that it also will be ending its relationship with location data aggregators "as soon as practical" while ensuring that location-based services that depend on data sharing, such as emergency roadside assistance, can continue to function. Sprint said in a statement that it cut ties with LocationSmart on May 25, and has begun cutting ties with the data brokers who received its customers' location data.
>
> T-Mobile chief executive John Legere tweeted: "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."[5]

Despite these statements, each of these carriers continued to sell their customers' location data for *months* afterwards. Americans deserve better.

For its part, the FCC also failed to act with sufficient urgency. As a former enforcement official, I recognize the challenges of reviewing the tens of thousands of pages of documents produced in these investigations, but we have conducted similarly extensive investigations much faster. Indeed, we took less time to resolve the highly complex merger between T-Mobile and Sprint, which involved mountains of pages of materials. Given the seriousness of the violations here, the Commission should have invested the resources necessary to get a draft to the Commission faster. By allowing this investigation to drag on when we knew that important public safety and public policy issues were at stake, we failed to meet our responsibilities to the American people.

Consumer Harms

I am concerned that the penalties proposed today are not properly proportioned to the consumer harms suffered because we did not conduct an adequate investigation of those harms. The Notices make clear that, after all these months of investigation, the Commission still has no idea how many consumers' data was mishandled by each of the carriers. I recognize that uncovering this data would have required gathering information from the third parties on which the carriers' relied. But we should have done that via subpoenas if necessary. We had the power—and, given the length of this investigation, the time—to compel disclosures that would help us understand the true scope of the harm done to consumers. Instead, the Notices calculate the forfeiture based on the number of contracts between the carriers and location aggregators, as well as the number of contracts between those aggregators and third-party location-based service providers. That is a poor and unnecessary proxy for the privacy harm caused by each carrier, each of which has tens of millions of customers that likely had their personal data abused. Under the approach adopted today, a carrier with millions more customers, but fewer operative contracts, would get an unfairly and disproportionately lessened penalty. That is inconsistent with our approach in other consumer protection matters and cannot stand.[6] More importantly, basing our forfeiture on a carrier's

[5] Brian Fung, "Verizon, AT&T, T-Mobile and Sprint Suspended Selling of Customer Location Data After Prison Officials Were Caught Misusing It," Washington Post (June 19, 2018).

[6] *See, e.g., Scott Rhodes A.K.A. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek,* Notice of Apparent Liability for Forfeiture, FCC 20-9, 2020 WL 553616 (rel. Jan. 31, 2020) (spoofed robocall violations; calculates the proposed forfeiture of $12,910,000 by assessing a base forfeiture of $1,000 per each of 6,455 verified unlawful spoofed robocalls with a 100% upward adjustment); *Kenneth Moser dba Marketing Support Systems*, Notice of Apparent Liability for Forfeiture, FCC 19-135, 2019 WL 6837865 (rel. Dec. 13, 2019) (spoofed robocall violations; calculates the proposed forfeiture of $9,997,750 by assessing a base forfeiture of $1,000 per each of 5,713 analyzed/verified calls with a 75% upward adjustment); *Long Distance Consolidated Billing Company*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 8664 (2015) (slamming and cramming violations; calculates $2.3 million forfeiture by assessing a $40,000 forfeiture for each unlawful bill plus an upward adjustment for misrepresentation) (subsequent history omitted); *Neon Phone Service,* Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 7964 (2017) (slamming and cramming violations; proposing a $3.9 million forfeiture by assessing a base forfeiture of $40,000 for each unlawful bill plus an upward adjustment for egregiousness). *See also TerraCom,*

number of aggregator contracts cannot be squared with our core mission today – to vindicate harmed consumers first and foremost.

Make no mistake – there are real victims who've had their privacy and security placed in harm's way. Each of them has a story. As discussed in the Notices, in May 2018, the *New York Times* reported that then-Missouri Sheriff Cory Hutcheson had used Securus technologies, a vendor that all of these wireless carriers allowed to access their customer location data, to conduct thousands of unauthorized location requests, accessing the locations of multiple individuals, including his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.[7] But I've personally spoken at length with one of those officers, retired Missouri State Highway Patrol Master Sergeant William "Bud" Cooper.

MSgt. Cooper told me that, while leading a homicide unit with the State Highway Patrol, he would investigate cases in the Missouri county where Cory Hutcheson was Sheriff. As they worked together on investigations, M.Sgt. Cooper noticed Hutcheson following up on leads and locating witnesses and suspects very quickly. M.Sgt. Cooper initially thought Hutcheson just had a particularly effective network of informants, but then grew suspicious and asked Hutcheson about his methods. Hutcheson eventually told him that he was using a Securus program to "ping" phone numbers from the investigations to uncover people's locations.

M.Sgt. Cooper suspected "something dirty" was going on. M.Sgt. Cooper began to wonder, based on Hutcheson's behavior towards him and his state trooper colleagues, if Hutcheson was targeting their phones too.

When M.Sgt. Cooper's worst fears were confirmed—that he had been targeted, along with his colleagues and a narcotics investigator—he was "shocked and angry." "I felt violated." This was personal information, akin to "going into someone's home." M.Sgt. Cooper found it "appalling" when it turned out that Hutcheson was obtaining this information based solely on woefully insufficient supporting documentation, including parts of an instruction manual, his vehicle maintenance records, and even an insurance policy. Hutcheson had personally "pinged" phones without authorization "over 2,000 times, and nobody checked."

M.Sgt. Cooper related that the revelations of Hutcheson's spying have threatened the safety of officers in the community and their informants. He reported that it has become harder to convince witnesses to trust police and talk to them, particularly in communities where witnesses fear retaliation. He has devoted his career to upholding the honor and integrity of law enforcement, but with the Hutcheson scandal "we all took a black eye."

M.Sgt. Cooper's story is but one single account of the harm done by the carriers; but we know there are many—perhaps millions—of additional victims, each with their own harms. Unfortunately, based on the investigation the FCC conducted, we don't even know how many there were, and the penalties we propose today do not reflect that impact.

This ignorance not only highlights a problem with today's decisions but a gap in our policymaking. The Commission needs to consider policy changes to protect the rights of consumers. Specifically, we should initiate a rulemaking to require carriers to inform consumers when there has been a breach of their confidential data, so that individual can take steps to protect themselves.

Even setting aside my concerns that our forfeitures are not pegged to the number of consumers harmed, I would still object to the amount of the proposed forfeiture to T-Mobile. It should be higher. As discussed in the Notice, T-Mobile had clear notice back in July 2017 that its contractual protections were

(Continued from previous page)
Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) (in proposing a forfeiture for Section 222 violations, citing the number of personal data records exposed by a carrier as the key factor, ultimately resulting in a penalty figure of $8.5 million) (subsequent history omitted).

[7] *See, e.g., T-Mobile NAL* at para. 28; *AT&T NAL* at para. 21; *Verizon NAL* at para. 26; *Sprint NAL* at para. 21.

failing to prevent location-based service providers from misusing customer location information. T-Mobile knew that one of these service providers was taking customer information and selling it to "bail bonding and similar companies"—aka, bounty hunters. Despite T-Mobile's knowledge of the problem, it took *two months* for the carrier to contact the aggregator company about this issue, and even then, T-Mobile only inquired of the aggregator and reminded it of its contractual obligations. It was the *aggregator* that terminated the service provider's access to T-Mobile customer information soon after hearing from T-Mobile. I believe that T-Mobile was on notice about the problems with its location data protections back in July 2017 and that the proposed forfeiture amount should reflect that fact – the punishment should fit the crime. Unfortunately, although their legal justification for doing so remains a mystery, a majority of my colleagues disagreed.

Transparency

Our slow response has also impacted our ability to discuss the facts of this case and the Commission's credibility for future investigations. Like other federal agencies, the Commission has a process that allows parties to protect the confidentiality of certain materials submitted to the agency. In their responses to the Bureau's investigation, however, the four carriers named in today's decisions bent that process so far that it is broken. Each of them adopted such an overbroad interpretation of our confidentiality protections that the Enforcement Bureau initially circulated heavily redacted draft decisions that would have made it impossible for the public to understand the key facts in each case.

Sadly, this is not a new phenomenon. The Enforcement Bureau has long struggled with parties asserting overbroad designations of confidentiality. Some parties, including some in these cases, have claimed confidential treatment for nearly the entirety of their responses to the Bureau's Letters of Inquiry, including legal arguments, publicly available facts, and even references to Commission's rules. Both as a former Enforcement Bureau official and as a Commissioner, I have seen such tactics hamstring our ability to vindicate the public interest and deter wrongdoing.

We should have rejected these confidentiality requests—some of which are frankly laughable—as soon as the Bureau reviewed the documents. Instead, many of those assertions were taken at face value, and the original drafts had heavy redactions. It is critical that Americans, particularly the hundreds of millions who use the services of these carriers, understand what happened here. If we let unreasonable and self-serving confidentiality assertions stand, those customers will never have the full picture.

Only after Commissioner Rosenworcel and I objected did the Bureau go back to the parties to challenge the confidentiality requests and negotiate the disclosure of more information. While I am glad that some of the parties reduced their requests, much of this information still remains confidential for now. Some even designated as confidential the number of agreements they had entered with aggregators and location-based service providers. That is frivolous.

The Commission does not have not to tolerate this. Section 0.459 of the Commission's rules establishes a process for resolving confidentiality requests. That process takes time, so we must begin resolving such requests immediately upon receipt. Here, despite the extraordinary length of our investigation, we let this problem fester for too long. Now, because we waited until the orders were before the Commission and then rushed to negotiate with the parties, there is insufficient time for the Section 0.459 process to play out. Even with the reduced redactions, Americans who read these Notices and the news coverage of them today will not have all the facts to which they are entitled. So while I am glad that we are ordering the parties to explain why we should not deny their requests completely, I worry that the carriers will have succeeded in hiding key facts until the spotlight has moved on. The FCC must do better.

* * *

Finally, while today's actions underscore and confirm the power of Section 222, they also highlight the need for additional actions. For example, our action today is limited to the major wireless carriers. But we know from this investigation that they are not the only wrongdoers. Securus, for one

example, behaved outrageously. Though Securus holds multiple FCC authorizations, I recognize that there may be legal limitations on the Commission's ability to take enforcement against the company for its misuse of customer location data. But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.

Going forward, Americans must be able to place trust in their wireless carriers. I understand that operating businesses at the enormous scale of these companies means relying on third parties for certain services. But these carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just few. Carriers must take responsibility for those people they allow into their operations.

I thank the staff of the Enforcement Bureau for their hard work on these important investigations.