Before the
Federal Communications Commission
Washington, DC

Unauthorized Disclosure and Sale of Customer Location Information by Wireless Carriers	))	__ - _____

Informal Complaint Against

AT&T Corporation
T-Mobile U.S.
Sprint Corporation
Verizon Wireless
for Unauthorized Disclosure and Sale of Customer Location Information

by

Georgetown Law Center on Privacy & Technology (CPT)
New America's Open Technology Institute (OTI)
Free Press

via ECFS, e-mail, and hand delivery
June 14, 2019

Open Technology Institute
New America Foundation
740 15th Street, NW—9th Floor
Washington, DC 20005

Eric Null, Senior Policy Counsel
null@opentechinstitute.org • 202.596-3493

Free Press
1025 Connecticut Avenue, NW, Suite 1110
Washington, DC 20036

Gaurav Laroia, Policy Counsel
glaroia@freepress.net • 202.265.1490

Center on Privacy & Technology at Georgetown Law
600 New Jersey Avenue NW
Washington DC 20001

Laura Moy, Executive Director
laura.moy@law.georgetown.edu
202.662.9547

Samuelson-Glushko Technology Law & Policy Clinic (TLPC) at Colorado Law
Robert and Laura Hill Clinical Suite
404 UCB, Boulder, CO 80309-0404

Counsel to Center on Privacy & Technology

Blake E. Reid, Director*
blake.reid@colorado.edu • 303.492.0548

* Nathan Bartell and Zachary DeFelice, Student Attorneys, provided substantial assistance.

Summary

Location information associated with wireless customers' cell phones is highly sensitive. Cell phones go nearly everywhere their owners go. In the words of the Supreme Court, they are "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[1] According to at least one widely cited national privacy survey, Americans consider location to be more sensitive than almost any other category of information apart from Social Security numbers.[2]

Nevertheless, customers who wish to receive wireless service have no choice but to share this information with their provider, because the very nature of wireless service is that it strives to connect customers no matter where they go. Accordingly, the Communications Act requires telecommunications providers—including wireless service providers—to observe heightened privacy obligations for location information.

But wireless service providers AT&T, Verizon, T-Mobile, and Sprint ("Carriers") have broadly violated those obligations and their customers' privacy expectations. The Carriers have disclosed customer location information to location aggregators, other location-based services companies, and unauthorized individuals without customer approval. That location information has in some circumstances found its way into the hands of bounty hunters and stalkers. In most cases, Carriers have not attempted to notify their customers of this information sharing, let alone to obtain consent.

These actions violate Sections 222 and 201(b) of the Communications Act. Carriers have failed their responsibilities under Section 222(c) to obtain customers' affirmative prior consent before using or sharing customer proprietary network information for purposes other than to provide service. Carriers have also failed their responsibilities under Section 222(a) to protect the confidentiality of customers' proprietary information. Finally, Carriers have violated Section 201(b)'s prohibition against unjust and unreasonable practices by failing to employ even the most basic consent mechanisms, creating an unreasonable risk of unauthorized access, and violating their own privacy policies.

The Carriers' actions have threatened public safety, contrary to Congress' directive that the Commission ensure communications networks promote safety of life and property. The Carriers' improper disclosure of location information enabled stalkers, people posing as police officers, debt collectors, and others to take advantage and find unwitting individuals. Furthermore, it is likely that abuses of location data have disproportionately impacted disadvantaged and marginalized communities.

We urge the Commission to investigate these practices and enforce against the Carriers Sections 201(b) and 222 of the Communications Act, and the Commission's rules implementing those statutes.

[1] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[2] *See infra* note 54 and accompanying text.

Table of Contents

Discussion

The Center on Privacy & Technology at Georgetown Law, New America's Open Technology Institute, and Free Press ("Complainants") file this informal complaint against Carriers for violations of the Communications Act and the Commission's rules. This complaint is filed pursuant to Section 208 of the Communications Act, in accordance with Section 1.716 of the Commission's rules.[3] Complainants urge the Commission to investigate allegations that the Carriers disclosed real-time customer location information to third parties without customer approval, and to take enforcement action against any statutory or regulatory violation.

Section I details the reported factual circumstances of the carriers' improper disclosures of location information. Section II explains why the Carriers' disclosure of customers' location information violates the protections for customer proprietary information ("PI") and customer proprietary network information ("CPNI") in Section 222 of the Communications Act and the Commission's implementing rules, as well as Section 201(b) of the Communications Act. Finally, Section III illustrates how the unauthorized disclosure of location information is harmful, particularly to disadvantaged and marginalized communities.

I. The Carriers have disclosed customer location information to unauthorized third parties without customer consent.

Carriers must collect location data from customer devices for the purposes of providing the wireless telecommunications services they offer and ensuring proper functioning of the wireless network. Several investigative reports have revealed, however, that AT&T, Verizon, T-Mobile, and Sprint disclosed their customers' device location data for purposes unrelated to the provision of those services and did so without first receiving express prior consent for such disclosures from those customers as required by law. In these cases, the Carriers have disclosed protected cell-site location information ("CSLI") and highly precise A-GPS data (described below) to third-party location aggregators and other unauthorized parties that use it for purposes wholly unrelated to the provision of wireless services. These cases include selling or otherwise disclosing location information to bounty hunters, stalkers, and debt collectors posing as law enforcement officers.

A. Wireless providers must collect location information from wireless devices to provide service.

Wireless providers collect location information from customer devices as a necessary and unavoidable part of providing wireless services.[4] Consumers have no ability to opt-out of this

[3] 47 U.S.C. § 208(a); 47 C.F.R. § 1.716.

[4] *E.g.*, AT&T Privacy Policy FAQ, https://about.att.com/sites/privacy_policy/terms#collect ("Location information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System.") (last visited June 5, 2019).

collection, which must take place so that wireless carriers are prepared to route calls and messages to the correct device at the correct location at any given time.[5]

Wireless devices connect regularly to, and send and receive calls and data through, wireless towers. Each wireless tower can house several antennae, which are directional and can estimate the distance of a wireless device from the device's signal strength. Based on those characteristics, towers can determine the approximate location of a wireless device, which is necessary to transmit to and receive information from that device. CSLI is registered by towers when a call or message is received or sent. In addition, in order to ensure that service is always operational, cell phones often "ping" nearby towers to register their location.[6]

Wireless providers may also have access to Global Positioning System ("GPS") and Assisted GPS ("A-GPS") data, especially for aiding emergency services. GPS data is generally highly accurate, but it has some flaws. For instance, identifying the location of a device may take a long time initially, and the GPS signal may experience interference from nearby buildings. Thus, GPS can be "assisted" with other data to more quickly and accurately determine location. Wi-Fi data and the cell-site location data described above both can assist GPS to make it more accurate.[7] With A-GPS and other location data, wireless providers have even more accurate location data on devices. This data is very useful for emergency services, but its accuracy also makes it highly valuable to other parties who may want to use it for non-emergency, and potentially nefarious, purposes.

B. The Carriers disclosed vast amounts of location information to third-party location aggregators without customer consent or a lawful order.

Several recent investigative reports have detailed improper sharing of location information by the Carriers, who are the four major wireless communications service providers (AT&T, T-Mobile, Sprint, and Verizon).[8] The Carriers shared this information

---

[5] Commissioner Geoffrey Starks, *Why It's So Easy for a Bounty Hunter to Find You,* NY Times (Apr. 2, 2019), https://www.nytimes.com/2019/04/02/opinion/fcc-wireless-regulation.html.

[6] *See T-Mobile Privacy Statement*, T-Mobile (Mar. 22, 2019), https://www.t-mobile.com/responsibility/privacy/privacy-policy (last visited June 7, 2019).

[7] *See generally* Ex Parte of CTIA, Wireless E9-1-1 Location Accuracy Requirements, PS Docket No. 07-114 (Jan. 14, 2015), https://ecfsapi.fcc.gov/file/60001013580.pdf.

[8] *See* Jennifer Valentino-DeVries, *Service Meant to Monitor Inmates' Calls Could Track You, Too*, New York Times (May 10, 2018), https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html ["New York Times, May 10, 2018"]; Joseph, Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile ["Motherboard, Jan. 8, 2019"]; Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, Motherboard (Feb. 6, 2019), https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years ["Motherboard, Feb. 6, 2019"]; Joseph, Cox, *Stalkers and Debt Collectors Impersonate Cops to Trick Big Telecom Into Giving*

without consent from the customers whose information was shared, and without a lawful order compelling disclosure of the information at issue.

In May 2018, the *New York Times* reported that the Carriers shared their customers' location information with Securus Technologies ("Securus"), a U.S.-based prison technology company that provides location-based services,[9] which then shared that information with additional third parties without authorization or consent.[10] As part of its suite of products for law enforcement and corrections agencies, Securus offers the "integrated proprietary software solution Location Based Services or LBS," which enables users to track cellular devices of interest.[11]

To facilitate LBS, Securus collects location information from major wireless carriers.[12] Some individuals located by LBS—those receiving calls from prisons—are informed via a prerecorded message that their location information will be collected, and they cannot receive the call until they press "1" to acknowledge this.[13] But when users of the LBS platform use LBS "Real-Time Location Services" to obtain the real-time location information of a phone not currently engaged in a call, Securus does not attempt to obtain consent.[14] Instead, Securus states that users of Real-Time Location Services are required to "upload the appropriate Search Warrant information and accept the associated terms and conditions."[15] However, Securus reportedly does not condition provision of location information to users of its LBS product upon receipt, review, and verification of any sort of information regarding warrants or other lawful orders. To the contrary, the company does not "conduct any review of surveillance requests," and as of May 10, 2018, wireless carriers did not receive forwarded

---

Them Cell Phone Location Data, Motherboard (Mar. 6, 2019), https://motherboard.vice.com/en_us/article/panvkz/stalkers-debt-collectors-bounty-hunters-impersonate-cops-phone-location-data ["Motherboard, Mar. 6, 2019"].

[9] *See generally* Securus Technologies, https://securustech.net/ (last visited June 5, 2019).

[10] *See* New York Times, May 10, 2018, *supra* note 8.

[11] Securus, *GDP Inmate Telephone Service RFP: Additional Scored Response Document* 26, https://ssl.doas.state.ga.us/PRSapp/bid-documents/164670046700-GDC0000669198904.pdf [Securus Georgia Response Document]; *see* Securus, *Location-Based Services White Paper* (Feb. 21, 2018), *available at* https://www.eff.org/files/2018/05/03/securus_white_paper_-_location_based_services_lbs_copy.pdf.

[12] Neema Singh Guliani & Nathan Freed Wessler, *Company That Handles Prison Phone Calls Is Surveilling People Who Aren't in Prison*, ACLU (May 11, 2018), https://www.aclu.org/blog/privacy-technology/location-tracking/company-handles-prison-phone-calls-surveilling-people-who.

[13] *Id.*

[14] Securus Georgia Response Document, *supra* note 11, at 29 ("The user then inputs the cellular number that is to be tracked and within seconds, the approximate location of the cell phone will be displayed on a graphical map of the area.").

[15] *Id.*; *see* Guliani & Wessler, *supra* note 12.

copies of surveillance requests from Securus that Securus in turn has received from its LBS users.[16]

Not only does Securus fail to require or obtain proof of lawful orders or customer consent as part of its LBS product, but this service has been abused in ways that both Securus and the carriers knew about for some time. According to the *New York Times*, between 2014 and 2017, Cory Hutcheson, a former sheriff of Mississippi County, Missouri, used Securus' LBS platform to track multiple wireless customers' location without consent or a court order.[17] Hutcheson was arrested in 2017 and was subsequently convicted on state and federal charges.[18]

Then, in January 2019, reporting by *Motherboard* exposed the Carriers' sale of location information to a host of other individuals and entities not affiliated with law enforcement.[19] Indeed, *Motherboard*'s reporting suggests that any individual could easily obtain location information from third parties, which receive that data directly from the Carriers.[20] In one example, a *Motherboard* reporter gave a bounty hunter a T-Mobile cell phone number, and the bounty hunter used the number to determine the phone's location within a couple of blocks.[21] The *Motherboard* investigation found product documentation suggesting that the service used by the bounty hunter was able to locate phones using location information made available by multiple wireless carriers, including AT&T, T-Mobile, and Sprint.[22] At no time was the owner of the located phone notified that the phone was being tracked or asked for consent to be tracked.[23]

Furthermore, the *Motherboard* reporting detailed how inexpensive it is for third parties to purchase location verification and monitoring of wireless customers' mobile devices without

---

[16] New York Times, May 10, 2018, *supra* note 8.

[17] *Id.*

[18] *Id.*; Jim Salter, Missouri sheriff pleads guilty to cellphone tracking charges, Associated Press (Nov. 20, 2018), https://www.apnews.com/c0901d36b9fe4edca4fa4c951dd3dea1.

[19] Motherboard, Jan. 8, 2019, *supra* note 8 (It is assumed that carriers are using cell-site location information); *see* Motherboard, Feb. 6, 2019, *supra* note 8 ("A LocationSmart spokesperson told Motherboard in an email 'Carrier location services available through LocationSmart are based on a variety of technologies depending on each carrier's particular location infrastructure implementation. That could include AGPS, cell tower, cell sector, or cell site trilateration. While there is no explicit indicator as to the technology used to provide a specific location response from a carrier, each response includes an accuracy estimate that can be used to infer the technology used.'").

[20] Motherboard, Jan. 8, 2019, *supra* note 8.

[21] *Id.*

[22] *Id.* The middleman who used a commercially available phone location service to locate the phone referenced in the *Motherboard* investigation was unable or unwilling to conduct a search for a Verizon device. *Id.*

[23] *Id.* ("[W]hen Motherboard tested the geolocation service, the target phone received no warning it was being tracked.").

consent.[24] For example, for $12.95 per device, one location aggregator service offers "mobile device account and location verification monitoring," which verifies billing account information from carriers and actively monitors the mobile device's physical location over time. The cost falls to $8.42 per device when a purchaser tracks 20,001 or more mobile devices.[25]

C. The Carriers disclosed location information directly to unauthorized individuals without customer consent or a lawful order.

The Carriers have shared their customers' location information without customer consent or a lawful order not only with third-party location aggregators, but with individuals as well. Recent investigative reporting revealed that fraudsters have tricked the Carriers into releasing real-time location data by posing as law enforcement officers.[26] The Carriers have handed over customer location information to these fraudsters without taking meaningful steps to verify their identities.

The scam typically works in the following way: a person who wants to access the location of a cellular device creates an email account that appears to belong to law enforcement. The scammer then sends an email to a carrier describing a circumstance in which there is imminent threat of physical harm. The scammer includes a request for the immediate release of the location of a customer whom the scammer falsely characterizes as a "suspect." The carrier then delivers the location to the scammer as requested.[27]

One scammer**,** John Letcher Edens, used the scam many times to gain unauthorized access to location information.[28] Edens "made up several stories of fictitious kidnappings to convince T-Mobile to hand over the location information**.**"[29] Edens used the email domain "gafugitivetaskforce1.net" to bolster his fake identity as a member of law enforcement.[30] After receiving the requested location information, Edens used this information not only to find victims, but also to harass and threaten at least one victim.[31]

The conduct of Edens is not an isolated case. Sources indicate that other similar scams have elicited location information from Verizon, T-Mobile, and AT&T.[32] One source

---

[24] *Id.*

[25] *Id.*

[26] Motherboard, Mar. 6, 2019, *supra* note 8.

[27] *Id.*

[28] *Id.*

[29] United States v. John Letcher Edens (N.D. Ga. Feb. 5, 2016) Criminal Action No. 1:15-CR158-ELRJFK, *available at* https://www.documentcloud.org/documents/5760568-Government-Response-in-Edens-Phone-Location-Case.html ["U.S. v. Edens"].

[30] *Id.* at 5.

[31] *Id.*

[32] Motherboard, Feb. 6, 2019, *supra* note 8.

suggested that this is an ongoing technique that can be performed on any carrier, by any imposter.[33]

D. The Carriers reportedly disclosed CSLI as well as other, more highly precise location information.

The Carriers have disclosed multiple types of location information regarding their customers. It is not clear, based on reporting and on what the Carriers have made public about their practices, what types of location information the Carriers disclosed in all instances. But the Carriers reportedly disclosed at least real-time CSLI, as well as highly precise A-GPS data, to bounty hunters, data aggregators, and firms that provide location-based services.[34]

The Carriers disclosed CSLI to Securus and users of Securus' LBS platform. As discussed above, CSLI derives from wireless network towers.[35] According to *The New York Times*, "In an email, Securus said the service was based on cell tower information, not on phone GPS."[36]

In addition to CSLI, the Carriers reportedly disclosed more precise location information pertaining to their customers, including tower triangulation data as well as A-GPS data. In a document describing location aggregator Microbilt's "Mobile Device Verify" service, the company states that the location information it provides will be accompanied by "[e]stimated location accuracy given available towers for triangulation."[37]

Motherboard confirmed that at least two location aggregation firms, CerCareOne and LocateUrCell, used even more precise A-GPS location tracking services. CerCareOne had access to A-GPS information from AT&T, T-Mobile, and Sprint, then provided location services to over 250 bail bond companies in secrecy, as customers agreed to "keep the existence of CerCareOne.com confidential."[38] CerCareOne operated for five years with little public visibility before closing in 2017.[39]

Another firm implicated in the use of A-GPS, LocateUrCell, was less secretive. Circumstantial evidence, such as a shared IP address with CerCareOne, indicates that LocateUrCell might have been affiliated with CerCareOne.[40] Although the website is now

---

[33] *Id.*

[34] *Id.*

[35] See discussion *supra*, Section I.A.

[36] New York Times, May 10, 2018, *supra* note 8.

[37] Microbilt, *Mobile Device Verify*, https://www.microbilt.com/Cms_Data/Contents/Microbilt/Media/Docs/ProductSheets/Mobile-Device-Verify-2018.pdf; *see* Motherboard, Jan. 8, 2019, *supra* note 8.

[38] Motherboard, Feb. 6, 2019, *supra* note 8.

[39] *Id.*

[40] *Id.*

defunct, LocateUrCell worked with AT&T, T-Mobile, and Sprint to use what appeared to be A-GPS technology to track cell phones within a few feet of their location.[41]

Finally, another firm, Captira, claimed to provide location data to bail bondsmen to within an accuracy of two meters for as little as $7.50.[42] Captira's service purportedly worked on all the major wireless carriers' networks, including Verizon, AT&T, Sprint, and T-Mobile.[43]

II. The Carriers' reported disclosure of customers' location information violates Sections 222 and 201(b) of the Communications Act and the Commission's implementing rules.

By selling or disclosing customers' location information without customer consent or lawful order, the carriers have violated Sections 222 and 201(b) of the Communications Act as well as the Commission's rules implementing those statutes. Location information collected by wireless carriers constitutes CPNI under Section 222 and associated rules, and Carriers therefore may not disclose it without first obtaining customers' affirmative consent or pursuant to lawful order. Wireless customers' location information also constitutes PI under Section 222(a), and Carriers therefore must protect its confidentiality. Yet the Carriers have broadly disclosed their customers' location information in direct violation of these obligations. The Carriers' widespread and reckless unauthorized disclosure of customers' location information further constitutes an unjust and unreasonable practice in violation of Section 201(b) of the Communications Act.

A. Wireless customers' location information constitutes CPNI under Section 222 and the Commission's rules, and the Carriers therefore may not disclose it without obtaining customers' affirmative prior consent.

Location information collected by wireless carriers is CPNI because "location" is specifically named in the statutory definition of CPNI, and because carriers collect this information for the purpose of providing telecommunications service. Because wireless customers' location information is CPNI, carriers are required by Section 222(c) and the Commission's rules to obtain affirmative consent from customers before using or sharing it for purposes other than to provide service.

Wireless customers' location information meets the definition of CPNI under Section 222(h)(1) and the Commission's implementing rules. Those provisions define CPNI as customer information that "relates to the quantity, technical configuration, type, destination,

---

[41] Johanna Somers, *Cell Phone Tracking Importance Not Lost on Naples Man,* Naples Daily News (Sept. 11, 2011), https://web.archive.org/web/20190202233943/http://archive.naplesnews.com/business/cell-phone-tracking-importance-not-lost-on-naples-man-ep-391057527-330865721.html.

[42] Joseph Cox, *Bail Bond Company Let Bounty Hunters Track Verizon, T-Mobile, Sprint, and AT&T Phones for $7.50*, Motherboard (June 22, 2018), https://www.vice.com/en_us/article/9k873e/captira-phone-tracking-verizon-tmobile-sprint-securus-locationsmart-bounty-hunters.

[43] *Id.*

location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier."[44] Customers are "using" this service merely by subscribing and connecting to the network and being capable of receiving calls or messages on a mobile handset or other device, and information about where their device is physically located while connected to the network therefore is information about the location of their use of the service.

To be considered CPNI, customer information also must be "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[45] Wireless customers' location information meets this test as well. Customers provide their location to their carriers solely for the purpose of being able to use the wireless services to which they have subscribed. As noted above, wireless carriers must stay apprised of connected devices to be able to connect calls and deliver messages. Even at times when no such message is being transmitted, cell towers are constantly "pinging" devices nearby and noting location to remain prepared to connect a call or send a message should one be sent over the network.[46] This location information is collected solely by virtue of the provision of wireless services because it is provided directly to the wireless provider from the customer's device and is collected to ensure the proper functioning of the service.

Because wireless customers' location information is CPNI, wireless service providers may not disclose it without obtaining their customers' express prior consent to do so. Section 222, which places the burden of obtaining customers' consent to use CPNI squarely on telecommunications carriers, extends to wireless carriers.[47] Section 222(c)(1) provides, with limited exceptions,[48] that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law; (2) with customer approval; or (3) in its provision of the telecommunications service from which such information is derived, or in provision of other services necessary to or used in the underlying provision of such telecommunications service.[49]

The Commission has determined that for most uses of CPNI that are unrelated to the provision of service, carriers not only must obtain their customers' approval, but the requisite approval must be affirmative and obtained in advance of the proposed unrelated use. More

---

[44] 47 U.S.C. § 222(h)(1); 47 C.F.R. § 64.2003(g) (emphasis added).

[45] 47 U.S.C. § 222(h)(1).

[46] *See, e.g.*, *T-Mobile Privacy Statement*, T-Mobile (March 22, 2019), https://www.t-mobile.com/responsibility/privacy/privacy-policy (last visited April 15, 2019).

[47] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, CC Docket No. 96-115, 28 FCC Rcd 9609, 9611, ¶ 7 (June 27, 2013), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0628/FCC-13-89A1.pdf.

[48] *See* 47 U.S.C. § 222(c)(1). Customers' CPNI can also be disclosed to a carrier's agents or affiliates without express prior permission if those agents or affiliates provide communications-related services. 47 C.F.R. § 64.2007.

[49] 47 U.S.C. § 222(c)(1).

specifically, Section 64.2007(b) of the Commission's rules requires carriers to obtain the opt-in approval of their customers before disclosing CPNI.[50] Opt-in approval requires "that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request . . . ."[51]

B. Wireless customers' location data also constitutes customer proprietary information under Section 222(a), and the Carriers therefore must protect its confidentiality.

Wireless customers' location information is also proprietary information under Section 222(a), both because customers expect it to be kept private and because it is personally identifiable information. Therefore, in addition to having an obligation to obtain their customers' consent before disclosing location information, carriers have a general "duty to protect the confidentiality of" location information.[52]

Location information is PI because customers expect their wireless carriers to maintain the privacy and confidentiality of this type of information. As the Commission stated in 2014, "we should interpret the term 'proprietary information' [PI] in the commonly understood sense of information that should not be exposed widely to the public, so when applied to information about individuals, the term must include personal data that customers expect their carriers to keep private."[53]

There can be no question that customers expect carriers to maintain the privacy and confidentiality of location data—especially this highly precise, real-time, on-demand CSLI and A-GPS data that the carriers are known to have shared with third parties without their customers' consent. A 2014 survey conducted by Pew Research Center found that approximately 82% of Americans consider details of their physical location over time to be either "very sensitive" or "somewhat sensitive"—a greater total percentage than for any other type of information included in the survey apart from Social Security numbers.[54]

Further, location information is PI because it constitutes personally identifiable information. The Commission concluded in 2014 that Section 222(a) "broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information (PII). In general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an

---

[50] 47 C.F.R. § 64.2007(b).

[51] *Id.* § 64.2003(k).

[52] 47 U.S.C. § 222(a) (imposing a "duty to protect the confidentiality of proprietary information of, and relating to . . . customers.").

[53] *TerraCom and YourTel America*, Notice of Apparent Liability, 29 FCC Rcd 13325, 13331, ¶ 16 (2014) ["*TerraCom/YourTel NAL*"].

[54] Mary Madden, Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Research Center (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

individual in context."[55] Location information—especially precise real-time location—plainly can be used "to locate a single person," and location information collected over time can easily be used to identify a single person. For example, in 2013, four researchers found that they were able to uniquely identify 95% of individuals in a dataset of location points using only four data points for each person.[56]

Because location information is PI under Section 222(a), carriers have a duty to protect its confidentiality.

C. The Carriers' unauthorized disclosure of customers' location data violates Section 222 of the Communications Act and the Commission's implementing rules.

By failing to meet the requirements attaching to CPNI and PI, the Carriers have violated Section 222 of the Communications Act and the Commission's CPNI rules.[57] The Carriers have violated Section 222(c) by failing to obtain affirmative prior consent from their customers (or other lawful order) before disclosing location information to third parties. In addition, the Carriers have violated Section 222(a) by failing to protect the confidentiality of their customers' location information.

The Carriers have violated Section 222(c) and the Commission's implementing regulations. As detailed above, the Carriers are required to obtain affirmative prior consent or a lawful court order before disclosing their customers' location information, which is a type of CPNI. Yet the Carriers have failed to comply with those requirements.

In responses to letters from Senator Ron Wyden, the Carriers admitted they relied on location aggregators or the aggregators' customers to obtain consent from tracked customers in many circumstances, and often did not seek to obtain customer consent themselves.[58] But

---

[55] *TerraCom/YourTel NAL*, ¶ 17.

[56] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports, Mar. 25, 2013, https://www.nature.com/articles/srep01376. The dataset used by the researchers contained location information collected from individuals in an unspecified western country from 2006–2007. In the dataset, the location of individuals was specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, *i.e.* equal to that of cell-site location information.

[57] *See* 47 U.S.C. § 222; 47 C.F.R. § 64.2007(b).

[58] Letter from Anthony Russo, T-Mobile to Sen. Ron Wyden at 3 (Feb. 15, 2019) ("**[L]ocation aggregators** were required to ensure verifiable informed customer consent was obtained . . ." (emphasis added)), *available at* https://www.documentcloud.org/documents/5767086-T-Mobile-Response-to-Wyden-on-Phone-Location.html; Letter from Tim McKone, AT&T to Sen. Wyden at 1 (Feb. 15, 2019) ("**[T]he aggregator or service provider** must . . . obtain the customer's consent to [the use of location information]" (emphasis added)), *available at* https://www.documentcloud.org/documents/5767087-AT-T-Response-to-Wyden-on-Phone-Location-Data.html; Letter from Karen Zacharia, Verizon to Sen. Wyden at 2 (Feb. 15,

location aggregators and other downstream users apparently did not seek consent or structure their services in a way that made seeking consent even possible, and it is not clear that the Carriers consistently undertook meaningful efforts to verify that consent had been obtained.[59] For instance, Verizon claims that Securus Technologies misrepresented that it had obtained consent from Verizon's customers, and Verizon admits that its own audit process did not reveal this fact.[60] Given that an LBS provider was able to conceal a feature that plainly did not contemplate customer consent, the Carriers' auditing procedures appear to have been insufficient to reliably ensure customer consent has been obtained by aggregators and other downstream users.

The Carriers have also violated Section 222(a). As explained above, location information is PI, and the Carriers therefore are required to respect and protect its privacy and confidentiality. The Carriers have failed to uphold this obligation. The unauthorized disclosure of customers' location information not only violates expectations and basic privacy principles, but also exposes customers to additional harm.

The Commission noted the relevance of potential for substantial injury in its 2014 case against TerraCom and YourTel.[61] In that case, two carriers needlessly exposed the Social Security numbers and other financial information of customers and potential customers, "invit[ing] identity theft and other serious consumer harms."[62]

Here, the Carriers' behavior has invited physical and predatory harms.[63] Carriers have exposed customers' location information to a number of parties—the vast majority of whom cannot be identified and perhaps will never be known—including stalkers, bounty hunters, and at least one rogue law enforcement official.

2019) ("Verizon authorized . . . location aggregators to facilitate access to Verizon subscriber location information . . . after the **corporate customer had obtained the affirmative opt-in consent of the wireless subscriber.**" (emphasis added)), https://www.documentcloud.org/documents/5767089-Verizon-Response-to-Wyden-on-Phone-Location-Data.html#search/p1/verizon; Letter from Maureen Cooney, Sprint to Sen. Wyden at 3 (Feb. 15, 2019) ("**Aggregators and developers** must clearly and completely document the presentation of . . . consent." (emphasis added)), https://www.documentcloud.org/documents/5767088-Sprint-Response-to-Wyden-on-Phone-Location-Data.html.

[59] Motherboard, Jan. 8, 2019 *supra* note 8. ("[W]hen Motherboard tested the geolocation service, the target phone received no warning it was being tracked.").

[60] Verizon Letter, *supra* note 58 at 4.

[61] *TerraCom/YourTel NAL*, ¶ 30.

[62] *Id.* ("By not employing appropriate security measures, TerraCom and YourTel exposed their customers to potentially substantial injury. The exposed PI—in particular, financial information and Social Security numbers—invites identify theft and other serious consumer harms.").

[63] See discussion *infra* at Part III.

D. The Carriers' unauthorized disclosure of customers' location data violates Section 201(b) of the Communications Act

The Carriers' sharing of customers' location information also violates Section 201(b) of the Communications Act, which states that "[a]ll charges, practices, classifications, and regulations for and in connection with [telecommunications] service, shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[64] The Carriers have violated Section 201(b) by failing to employ even the most basic consent mechanisms, creating an unreasonable risk of unauthorized access, and violating their own privacy policies.

In the case against TerraCom and YourTel, the Commission found that two carriers' insufficient data security practices were unjust and unreasonable because the carriers "failed to employ even the most basic and readily available technologies and security features for protecting consumers' PI."[65] Here, the Carriers have failed to employ even the most basic consent mechanisms to protect their customers' CPNI and PI. Instead, the Carriers recklessly facilitated aggregators' widespread access to their customers' highly detailed and real-time location information without consent, permitted aggregators to share that information with additional third parties downstream without consent, and apparently did not practice any meaningful or effective oversight or monitoring to see whether aggregators themselves ever obtained customers' consent.

The Commission has also found violations of Section 201(b) where carriers' data security practices "created an unreasonable risk of unauthorized access."[66] Here, the Carriers' routinely careless behavior facilitated widespread unauthorized access to customers' location information.

Finally, the Carriers have violated Section 201(b) because they have either violated their own privacy policies or omitted critical information from the policies. The Commission has found violations of 201(b) where "representations in [carriers'] privacy policies were false, deceptive, and misleading."[67] Here, the Carriers did not disclose in their privacy policies that they sold real-time location data to third parties, including third parties of which customers were unaware and thus unable to provide consent.

AT&T. AT&T's privacy policy states that it "do[es] not sell, trade or share your CPNI with anyone outside of the AT&T family of companies or our authorized agents, unless required by law (example: a court order)."[68] It further states that it "do[es] use your CPNI internally, however. We may share information about our customers among the AT&T

---

[64] 47 U.S.C. § 201(b).

[65] *TerraCom/YourTel NAL*, ¶ 32.

[66] *Id.,* ¶ 33–34 (The Commission further noted that as a result of the two carriers' practices, a third party accessed and downloaded over 100,000 proprietary records.).

[67] *Id.*, ¶ 38 (TerraCom and YourTel had represented that they employed reasonable security measures to protect customers' private information, when in fact they did not).

[68] AT&T, *Your Rights and Choices*, *Network Information (CPNI)*, https://about.att.com/sites/privacy_policy/rights_choices#cpni (last visited June 7, 2019).

companies and our agents in order to offer you new or enhanced services. For example, we might offer a discount or promotion for Internet or TV services based on your CPNI."[69] In another part of its privacy policy dealing specifically with location data, AT&T does suggest broadly that it collects and uses location data in "all kinds of ways," and lists as examples (1) providing and improving its wireless service, (2) enabling location-based services installed on the device, (3) enabling location-based services from third parties, and (4) advertising.[70] AT&T also notes that it may share location data without consent to, among other things, "[n]otify, respond or provide information (including location information) to a responsible governmental entity in emergency or exigent circumstances or in situations involving immediate danger of death or serious physical injury."[71]

Nowhere in AT&T's privacy policy is there any specific reference to the sale of CPNI, including location data, to the types of entities to which AT&T reportedly sold real-time location data. Moreover, AT&T's purported consent for "enabling location-based services from third parties" is insufficient to cover the sale of real-time location data to bounty hunters and essentially any willing purchaser, especially when the AT&T customer has no awareness of or relationship with that third party. The intrusiveness of such privacy violations requires much more detailed disclosures and cannot be left to such euphemistic language. Importantly, AT&T itself conceded that these uses of real-time location data violate its policies. Indeed, "AT&T . . . told Motherboard the use of its customers' data by bounty hunters goes explicitly against the company's policies."[72]

Sprint. Sprint's sparse privacy policy states that it shares personal data (including location data) with, for instance, affiliates, third-party service providers, reward programs, and emergency services.[73] Sprint also may share data for the "[p]rotection of Sprint and others," including responding to emergencies. However, Sprint's privacy policy does not expressly mention the sale of location data to the relevant categories of third parties at issue here.

T-Mobile. T-Mobile's policy statements similarly do not expressly cover the sale of location data to the relevant categories of third parties. T-Mobile's CPNI policy states that "T-Mobile is committed to protecting the privacy and security of our customers' personal information and, as set forth in our Privacy Statement, we strive to be a leader in protecting all such personal information," and acknowledges that "federal law has long-required

---

[69] *Id.*

[70] AT&T, *Privacy Policy FAQ, (Questions About Location Information)*, https://about.att.com/sites/privacy_policy/terms#location (last visited June 7, 2019).

[71] AT&T, *About Our Privacy Policy*, https://about.att.com/sites/privacy_policy/full_privacy_policy (last visited June 7, 2019).

[72] Motherboard, Jan. 8, 2019, *supra* note 8.

[73] Sprint, *Sprint Corporation Privacy Policy* (April 24, 2019), *INFORMATION WE SHARE*, https://www.sprint.com/en/legal/sprint-corporation-privacy-policy?ECID=vanity:privacypolicy#infoshare (last visited June 7, 2019).

telecommunications carriers to protect CPNI."[74] Regarding location-based services, T-Mobile simply states that it "may provide LBS services. Where we do so, we will request your permission before we access precise location data to support the service."[75]

Like the other Carriers, T-Mobile does not explicitly identify the location aggregators identified by the investigative reports. And if T-Mobile adheres to its own privacy policy, the company should have required these third parties to comply with privacy and security protections consistent with that policy. It appears, however, that the third parties and subsequent parties obtaining this kind of data from T-Mobile and the other Carriers were not subject to any such obligations, likely because T-Mobile did not know about these practices and did not exercise proper care to investigate or prevent such practices.

Verizon. Verizon was implicated only in the *New York Times* reporting about the sale of data to Securus, and not Motherboard's reporting about the broader sale of location information. However, Verizon states that "Location information may . . . be used for emergency purposes (such as E911) and with your consent at other times."[76] Thus, like the other carriers, Verizon too did not provide notice of its location sharing practices.

III. The Carriers' practices exposed customers to risk of physical harm, disproportionately visited upon disadvantaged and marginalized communities.

Continuing to allow access to real-time location data of cell phones is a safety concern that the Commission must take seriously. The Commission has a duty to "promot[e] safety of life and property through the use of wire and radio communications."[77] The sharing of real-time location data of potentially all wireless customers served by the Carriers raises significant concerns about public safety. Some bounty hunters allegedly use the data to track individuals they know personally.[78] Stalkers, harassers, and other people meaning to do harm to others often turn to tracking wireless devices where they can.[79] The Commission should not condone this behavior, and must stamp it out where it can.

To make matters worse, abuses of location data have real-life consequences that not only directly affect the Carriers' paying customers, but are likely to have a disproportionately

---

[74] T-Mobile, *About T-Mobile*, *More Information: CPNI*, https://www.t-mobile.com/responsibility/privacy/resources/cpni (last visited June 7, 2019).

[75] T-Mobile, *T-Mobile Privacy Statement* (Mar. 22, 2019), *HOW WE USE INFORMATION WE COLLECT ABOUT YOU*, https://www.t-mobile.com/responsibility/privacy/privacy-policy#howuseinfo.

[76] Verizon, *Full Privacy Policy*, https://www.verizon.com/about/privacy/full-privacy-policy (last visited June 7, 2019).

[77] 47 U.S.C. § 151.

[78] Motherboard, Jan. 8, 2019, *supra* note 8.

[79] *See, e.g.*, Kristin Houser, *Stalkers Are Pretending to be Cops to Steal Your Phone's Location* (Mar. 8, 2019), https://futurism.com/stalkers-location-data-telcos-cops/.

negative effect on people in disadvantaged and marginalized communities.[80] These potentially include victims of domestic violence and low-income people and their families.

A. Victims of domestic violence and stalking are put at greater risk when perpetrators have access to sensitive location data.

Victims of domestic violence and abuse are particularly vulnerable with respect to the sharing of location data. In domestic abuse situations, abusers will engage in systematic and repeated surveillance of victims as a means of asserting control over them.[81] An abuser with access to their victim's location information is able to engage in this sort of undesired surveillance with far more ease than without it.

Stalking victims, specifically, are especially at risk because location tracking technology enables perpetrators to follow and harm their targets more easily. Stalkers tend to use the internet as an "easy, low-cost method of communicating with [their] victims."[82] Similarly to bounty hunters, according to *Motherboard*'s reporting, a stalker given easy access to their victim's location information could amplify their harassment both online and in the real-world.[83]

An article originally published in Domestic Violence Report warns victims of stalking or abuse about the dangers of sharing location information:

> Sharing one's location can be quite dangerous, however, when a stalker or abuser uses this information to stalk, harass, and threaten. For victims of domestic violence, assault or stalking, knowing how much information may be inadvertently shared about them is key to planning for privacy and safety. For service providers, there is often a concern that abusers may be able to track victims to the shelter or program. Some programs have questioned if the solution is to ban cell phones in shelter. In reality, however, this response will not eliminate the feared risk. Additionally, it is not feasible for survivors to give up their cell phones, which for many is a life line to safety, help, and support. The better solution is to understand how location gets shared, minimize the amount of information that is being

---

[80] *Cf.* Scott Skinner-Thompson, *Privacy's Double Standards*, 93 Wash. L. Rev. 2051 (2018) (discussing disparate impacts in the context of tort law), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3134500.

[81] *E.g.*, Ryan Calo, *Boundaries of Privacy Harm*, 86 Ind. L. J. 1, 15 (2011) (internal citations omitted), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1641487.

[82] Joseph C. Merschman, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 Harv. Women's L.J. 255, 275-76 (2001), *available at* https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hwlj24&id=282&men_tab=srchresults.

[83] *See* Motherboard, Feb. 6, 2019, *supra* note 8.

> shared, and help survivors take back control by creating thorough safety planning and changing privacy settings.[84]

When location information is shared without consent, the opportunity for abusers to leverage this information for menacing purposes becomes even more acute. Without control over their information, victims of domestic abuse may experience physical harm and perpetual fear.

Victims of domestic violence have been harmed by sharing of location data. For instance, as mentioned above, John Letcher Edens was convicted of aggravated stalking and harassing phone calls after violating a temporary protective order to contact his ex-wife for the purpose of harassing and intimidating her.[85] Edens' "victimization of others extended beyond fraudulently obtaining individuals private location information and using that information to find those individuals."[86] Edens called another victim three or four times a day, "came to [her] home [at] all hours of the night[,] and showed up at [her] place of employment."[87]

B. Low-income people and their families are particularly vulnerable to abuse of their location data.

Low-income people, particularly those in the penal system and their families, are particularly vulnerable to abuses of location sharing and surveillance more generally.[88] "[S]urveillance of the poor is broader, more invasive, and more difficult to redress than surveillance of other groups."[89] It is reasonable to believe that the sharing of location information would likewise have a disproportionate effect.

Additionally, correctional officers have the capability to track the location of an inmate's friends and family.[90] Family and friends who decide to communicate with inmates in an effort

---

[84] Kaofeng Lee & Erica Olsen, *Cell Phone Location, Privacy and Intimate Partner Violence*, 18 Domestic Violence Report 6 (Aug./Sept. 2013), https://www.acesdv.org/wp-content/uploads/2014/06/NNEDV_CellPhoneLocationPrivacy_DVRarticle_2013.pdf.

[85] See discussion *supra*, Part I.C; Motherboard, Mar. 6, 2019, *supra* note 8; U.S. v. Edens, *supra* note 29.

[86] *U.S. v. Edens, supra* note 29 at 5.

[87] *Id.*

[88] *See* Mary Madden, *et al.*, *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash. L. Rev. 53, 58-60 (2017), *available at* https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/walq95&id=60&men_tab=srchresults. A study by the Prison Policy Initiative shows that in 2014, incarcerated people had a median annual income of $19,185 prior to their incarceration, which is 41% less than non-incarcerated people of similar ages. Bernadette Rabuy & Daniel Kopf, *Prisons of Poverty: Uncovering the pre-incarceration incomes of the imprisoned*, Prison Policy Initiative (July 9, 2015), https://www.prisonpolicy.org/reports/income.html.

[89] Madden, *supra* note 88 at 63.

[90] *See* Securus Georgia Response Document, *supra* note 11, at 26 (LBS will "[p]rovide the called party's true location at the time of an inmate's call via a link in the call detail record (CDR).").

to expedite their rehabilitation will be subject to monitoring by law enforcement. It is crucial that these family and friends are afforded the protection of the law. Preventing the unlawful abuse of location information is crucial to protecting the rights of those marginalized in society because of their economic disadvantage. To compound this concern, low-income individuals often lack the necessary resources to assert their rights.[91]

* * *

For the foregoing reasons, we respectfully request that the Commission investigate the improper disclosure by the Carriers of customer location information to unauthorized third parties, enjoin the practice, fine the Carriers as appropriate, and seek any further relief as is just and proper.

[91] Leonard Wills, *Access to Justice: Mitigating the Justice Gap,* American Bar Association (2017), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2017/access-to-justice-mitigating-justice-gap/ ("A recent study shows that approximately 80 percent of low-income individuals cannot afford legal assistance. The middle class struggles, too: a study shows that 'forty to sixty percent of their legal needs go unmet.'").