Published on *The National Law Review* https://natlawreview.com

FCC Proposes Over $200 Million in Fines to AT&T, Verizon, T-Mobile and Sprint for Not Protecting Customers' Location Data

Article By:

Womble Bond Dickinson Communications, Technology and Media

On February 28, 2020, the Federal Communications Commission proposed fines amounting to over $200 million dollars against the four largest wireless carriers in the U.S., alleging that the companies broke the law by not taking reasonable measures to protect customers' private location information and allowing third parties to have unauthorized access to it.

The Communications Act requires telecommunications carriers to protect the confidentiality of certain customer data known as CPNI (Customer Proprietary Network Information), which is related to the provision of telecommunications service and includes the customer location information. The FCC's CPNI rules make clear that carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to this data. The rules also require that carriers or those acting on their behalf generally must obtain affirmative, express consent from a customer before using, disclosing, or allowing access to this data. And carriers are liable for the actions of those acting on their behalf.

The FCC's Enforcement Bureau, who started these investigations into the four carriers in May 2018, adopted the Notices of Apparent Liability for Forfeiture and Admonishment, or NALs, finding that all four carriers sold access to their customers' location information to "aggregators," who then resold access to such information to third-party location-based service providers. Under these NALs, T-Mobile faces a proposed fine of $91 million; AT&T of $57 million; Verizon of $48 million; and Sprint of $12 million.

Specifically, the FCC mentions the case of the company Securus Technologies, Inc., a provider of telecommunications services to correctional facilities throughout the United States, that also operated a "location-finding service" that enabled law enforcement and corrections officials to access the location of a mobile device belonging to customers of the major wireless carriers without the device owner's knowledge or consent. Securus had authorization from the carriers to receive their customer location information to confirm that recipients of collect calls from prisons were "not within a certain distance of the prison from which a collect call was placed." But Securus then used that information for its "location-finding service." And although Securus required users to certify that they had the authority to perform location searches and to upload an appropriate document that provided legal authorization for the location request, such as a court order or warrant, the FCC found that such

efforts were insufficient to comply with applicable rules.

The FCC used as an example an incident that was reported by The New York Times in 2018. Then-Missouri Sheriff Cory Hutcheson used the Securus service, without legal authorization, to access location information about anyone he pleased. Hutcheson submitted thousands of unauthorized location requests via the Securus service between 2014 and 2017, in some cases "upload[ing] entirely irrelevant documents including his health insurance policy, his auto insurance policy, and pages selected from Sheriff training manuals" in lieu of genuine legal process or court orders. Among those apparently tracked by Hutcheson in this manner were his predecessor as Sheriff, a Missouri Circuit Judge, and at least five highway patrol officers.

The FCC found that even after these incidents were highly publicized by the reports from the New York Times and other sources, which put the companies on notice that their safeguards for protecting customer location information were inadequate, the carriers apparently continued to sell access to its customers' location information for nearly a year without putting in place reasonable safeguards—leaving its customers' data at unreasonable risk of unauthorized disclosure. And although the carriers had several commonsense options to impose reasonable safeguards, such as verifying consent directly with customers via text message or app, the carriers apparently failed to take the reasonable steps needed to protect customers' data.

So what's next? The NALs contain allegations from the FCC that advise the parties on how they have apparently violated the law and set forth a proposed monetary penalty. The size of the proposed fines for the four wireless carriers differs based on the length of time each carrier apparently continued to sell access to its customer location information without reasonable safeguards and the number of entities to which each carrier continued to sell such access. Neither the allegations nor the proposed sanctions in the NALs are final Commission actions. The carriers now have 30 calendar days to either pay the full amount of the proposed forfeiture or file a written statement seeking reduction or cancellation of the proposed amount. In the latter case, the Commission will consider the parties' evidence and legal arguments before taking further action to resolve these matters. The carriers also have the option of filing a petition for reconsideration. Almost certainly all of the carriers will challenge these findings by the FCC.

As the Supreme Court has observed, location data associated with wireless service "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." With these actions, the Commission has advised carriers that this duty requires them to take "every reasonable precaution" to safeguard their customers' information, and failure to do it may cost them millions of dollars.

National Law Review, Volume X, Number 70