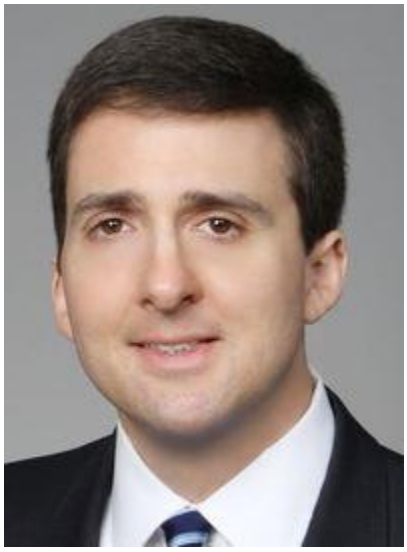
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FCC's 1st Data Security Action Raises Concerns

Law360, New York (October 29, 2014, 10:14 AM ET) --



Howard Waltzman

The Federal Communications Commission is asserting unprecedented authority to regulate data security matters with its recent action against two telecommunications carriers for failing to protect customers' personal information from unauthorized disclosure. The FCC issued a notice of apparent liability for forfeiture (NAL) against TerraCom Inc. and its affiliate, YourTel America Inc. for failing to adequately protect consumers' information from disclosure, and fined the companies a record $10 million.

The action is the FCC's first major case involving data security, a subject matter typically overseen by the Federal Trade Commission. More importantly, the case involves the data security of noncall-related information, which introduces a potential overlap with the FTC's jurisdiction and the risk of dual, and even conflicting, regulation.

Background

The companies are common carriers that provide telecommunications services to low-income customers as part of the Universal Service Fund's Lifeline program. In order to demonstrate customers' eligibility for the Lifeline program, the companies collected sensitive personal information, such as name and address, date of birth, Social Security number and driver's license or state ID number. The companies then allegedly stored the information on unprotected Internet servers in publicly accessible folders without password protection or encryption.

Scripps Howard News Service discovered the breach when it found that the customers' sensitive data files could be located with a simple Google search and basic URL manipulation. The FCC claims that the personal data of up to 305,000 consumers was potentially breached between September 2012 and April 2013.

In the NAL, the FCC charged the companies with various violations of the Communications Act of 1934. Specifically, the FCC alleged that the companies violated: (1) Section 222(a) of the act for failing to protect the confidentiality of consumers' proprietary information; (2) Section 201(b) of the act by failing to employ reasonable data security practices to protect consumers' proprietary information; (3) Section 201(b) of the act by falsely representing in their privacy policies that they protected such information;

and (4) Section 201(b) of the act by failing to notify all customers whose information could have been breached.[1]

Section 222(a) Violation

While the FCC has rules governing data breaches, they are limited to breaches of customer proprietary network information (CPNI). Section 222 of the act, which also governs a carrier's use and disclosure of CPNI, defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and … information contained in the bills pertaining to … service received by a customer of a carrier."

Typically, the subsections of Section 222 have been read in conjunction with each other to describe a carrier's obligations with respect to CPNI — with subsection (a) setting forth the entities to which Section 222 applies, and the subsequent subsections providing more specificity on how carriers may use or disclose CPNI. The FCC has not previously promulgated rules interpreting the definition of "proprietary information" in subsection (a) differently than the definition of CPNI.

In the NAL, however, the FCC expanded the scope of subsection (a) to go beyond CPNI and encompass any proprietary information. Section 222(a) of the act states that carriers have a duty "to protect the confidentiality of proprietary information of, and relating to … customers." In the NAL, the FCC argued that the reference to "proprietary information" in Section 222(a) covered "all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy." The term proprietary information, according to the FCC, "broadly encompasses such confidential information as privileged information, trade secrets, and personally identifiable information."

As part of its reasoning for this interpretation, the FCC relied on the inclusion of the word "privacy" in two section headings as a source of authority — first in the section heading for Section 222 and again in the heading for Section 222(c)(1). In addition, the FCC pointed out that, although Section 222(c)(1) refers to CPNI specifically, it is titled "Privacy requirements for telecommunications carriers," therefore, the term "clearly encompass[s] private information that customers have an interest in protecting from public exposure."

Commissioner Michael O'Reilly disagreed with the FCC drawing authority from the headings, and, in his dissent, commented "If the Commission can invent new authority based on the 'Privacy of Customer Information' heading of section 222, I can only imagine what it could do with the heading of section 215: 'Transactions Relating to Services, Equipment, And So Forth.'"

Section 201(b) Violations

Section 201(b) of the act generally requires telecommunication carriers' practices to be "just and reasonable." Specifically, Section 201(b) states that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."

In the NAL, the FCC broadly interpreted its authority to regulate "unjust and unreasonable" practices to

cover a telecommunication carrier's data security practices. It alleged that the companies violated Section 201(b) and engaged in "unjust and unreasonable" practices by: (1) failing to employ reasonable data security practices to protect their customers' personal information, (2) misrepresenting in their privacy policies that they protected customers' personal information, and (3) failing to notify all customers whose personal information could have been breached by the companies' lax security practices.

The FCC cited the failure to implement certain data security practices as an example of the companies' "unjust and unreasonable" practices. For example, the FCC pointed to the companies' lack of encryption for their customers' personal information. The FCC argued that, because carriers have an existing statutory obligation to use reasonable steps to protect their customers' CPNI, which could include the use of encryption, the lack of encryption "clearly evidences the unjust and unreasonable nature of the Companies' data security practices." The companies also used random URLs to protect their customers' personal information, which the FCC argued the companies "knew or should have known" provide inadequate security.

In addition, the companies' privacy policies either expressly represented or implied that they employed reasonable security measures to protect consumers' private information. For example, TerraCom's privacy policy stated "TerraCom Wireless has implemented technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use and will continue to enhance its security measures as technology becomes available."

The FCC found these misrepresentations to be a "deceptive practice" that was "unjust and unreasonable" in violation of Section 201(b). The FCC's assertion of authority over "deceptive" data security practices is strikingly similar to the FTC's authority over "unfair or deceptive acts or practices" under Section 5 of the FTC Act.

Moreover, the FCC found that, because the companies only notified 35,000 of the more than 300,000 people whose data was possibly compromised by the breach, this notification "of anything less than all potentially affected consumers" was unjust and unreasonable in violation of Section 201(b).

Conclusion

The FCC's action raises several concerns. First, its expansive interpretation of what constitutes "proprietary information" under Section 222(a) is being adopted as part of an enforcement action, rather than in the context of an industry-wide rulemaking subject to notice and comment. Such a seismic shift in the scope of Section 222 raises many issues that warrant consideration in a open, public proceeding. As Commissioner Ajit Pai noted, "an agency cannot at once invent and enforce a legal obligation."

Second, the FCC is interpreting "proprietary information" to far exceed the scope of CPNI. By including Social Security and driver's license numbers, in addition to other information, within the bounds of its authority, the FCC is asserting authority over information that has no bearing upon the call-specific information that served as the genesis of Section 222. The FTC has focused for quite some time on protecting Social Security numbers and other information the disclosure of which could result in identity theft, and it is not clear why the FCC would claim expertise over such information just because such information is possessed by a telecommunications carrier.

While issues related to the FTC's common carrier exemption would need to be addressed, the FTC

would seem to be the more logical agency to protect such information. In the interim, the FCC's action could create a compliance nightmare if the FCC interprets data security and breach notification obligations in a manner that conflicts with FTC-related requirements.

Third, if the FCC is able to claim that its authority over "unjust and unreasonable" practices includes data security breaches, then there appear to be few limiting factors as to what constitutes a practice "for and in connection with" a communications service under Section 201(b). Commissioner O'Reilly commented in his dissent that "I am noticing a disturbing trend at the Commission where, in the absence of clear statutory authority, the Commission suddenly imbues an innocuous provision of the Act with tremendous significance in order to meet its policy outcome."

—By Howard W. Waltzman and Lei Shen, Mayer Brown LLP

Howard Waltzman is a partner in Mayer Brown's Washington, D.C., office where he focuses his practice on communications and Internet law and privacy compliance. Lei Shen is a senior associate in the firm's Chicago office in the privacy and security and business and technology sourcing practice groups.

[1] See Federal Communications Commission, Notice of Apparent Liability for Forfeiture, In the Matter of TerraCom, Inc. and YourTel America, Inc., Oct. 24, 2014, at page 5.
