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 Data Security Powers Likely To See FTC-Like Challenges

By **Allison Grande**

Law360, New York (October 29, 2014, 10:24 PM ET) -- The Federal Communications Commission last week added its name to the growing number of regulators intent on bringing enforcement actions over allegedly lax data security practices, but attorneys say the agency's efforts are likely to face corporate challenges similar to the ones plaguing the Federal Trade Commission.

On Friday, the FCC hit TerraCom Inc. and YourTel America Inc. with a $10 million fine for allegedly placing the personal data of up to 300,000 consumers at risk by storing Social Security numbers, names, addresses, driver's licenses and other sensitive customer information on unprotected Internet servers that "anyone in the world" could access.

"For a first entry into this area of enforcement, it is a particularly aggressive action," Kirk Nahra, Wiley Rein LLP's privacy practice chair, said. "Obviously, the FCC does not have the jurisdictional reach of other enforcement agencies in this area, but its ability to issue fines gives it some additional clout in this area that the FTC typically does not have."

In addition to its novelty, the FCC's action also quickly attracted widespread attention for its similarities to recently contested efforts by the FTC to hold private companies liable for alleged data security shortcomings.

“Like the FTC, the FCC has drawn on statutory provisions that were not written with data security in mind,” said Lisa Sotto, head of Hunton & Williams LLP's global privacy and data security practice. “The FCC clearly is drawing from the FTC’s bag of tricks in moving into unchartered territory.”

During the past decade, the FTC has brought more than 50 data security actions using its authority under Section 5 of the FTC Act to police unfair and deceptive trade practices.

While most of the cases have settled, Wyndham Worldwide Corp. and LabMD Inc. within the past two years have become the first companies to challenge the commission's allegations. They both assert that Section 5 does not give the FTC the authority to set data security standards for private companies and, even if it did, the regulator has failed to give companies proper notice of its data security expectations.

To support its venture into data security enforcement, the FCC is relying on the Communications Act, a statute that, like Section 5, was drafted decades ago and does not explicitly mention data security.

The FCC alleged in its notice Friday that the carriers' failure to reasonably secure their customers' personal information violated their duty under the act to protect "customer proprietary network information" and constituted an "unjust and unreasonable practice" in violation of the act.

Given that the FCC had not previously applied the "proprietary network information" to personal data or used the "unjust and unreasonable practice" provisions to force companies to employ reasonable security practices, the stage is set for a showdown similar to the one over the FTC's purportedly vague "unfairness" authority.

"The FCC is very likely to face similar challenges to this decision that the FTC has faced in matters such as LabMD and FTC v. Wyndham," said Christopher Nucifora, the chair of the technology practice group at Kaufman Dolowich & Voluck LLP. "The dissenters are clearly following the same playbook."

Opponents of the FCC's approach are likely to find support from at least two commissioners, the Republicans Ajit Pai and Michael O'Rielly, who filed scathing dissents to their colleagues' decision to issue the proposed fine.

Pai criticized his colleagues for sanctioning the companies without providing notice of "what the law is," saying an agency "cannot at once invent and enforce a legal obligation," while O'Reilly wrote that he was not convinced the FCC had the authority to act due to his "firm belief" that the Communications Act "was never intended to address the security of data on the Internet."

"Commissioner Pai's statement that the 'government cannot sanction you for violating the law unless it has told you what the law is' and Commissioner O'Rielly's statement questioning the FCC's authority to act under the stated sections of the law are directly in line with the protestations we are hearing about the FTC's authority to act in data security cases," Sotto said.

Attorneys say the strongest argument available to challengers hinges on the way the regulator has interpreted two sections of the Communications Act to justify its enforcement decision.

"It appears that the commission has taken a very broad view of the Communications Act and stretched the scope to allow for the claims they wanted to make," Cynthia Augello of Cullen and Dykman LLP said.

Traditionally, the commission has used Section 222 of the Communications Act to ensure companies are protecting customer proprietary network information, or CPNI, which generally encompasses call-related data such as the duration and length of a call.

But in bringing its latest enforcement action, the FCC is claiming that CPNI can be defined more broadly to include "information that should not be exposed widely to the public," drawing personal data that "customers expect their carriers to keep private" within the statute's reach.

"The broad interpretation of what constitutes proprietary information creates a lot of ambiguity," Mayer Brown LLP partner Howard Waltzman said. "For example, does that mean I would expect my carriers to keep my grandma's cookie recipe private? The definition can include almost anything."

Challengers are likely to argue that Congress did not intend for personal information to be included in the definition of proprietary data when it added the provision to the statute in 1996. Foley Hoag LLP privacy and data security practice co-chair Colin Zick noted that the argument might be aided greatly by

another statute enacted that year, the Health Insurance Portability and Accountability Act, which protects personal health information.

“Lawmakers knew how to call something personal information in HIPAA, but they used a different term in another statute passed in the same year,” Zick said. “To me, that means something different.”

The FCC is also likely to face backlash from its declaration Friday that the “unjust and unreasonable practice” provision of Section 201(b) applies to data security, even though the provision has traditionally applied to subjects like pricing and classifications, attorneys say.

“If the FCC continues on this path, a wide variety of practices might suddenly become the subject of enforcement even without FCC rules having been adopted,” Kelley Drye & Warren LLP partner Steven Augustino said. “That truly would be a challenge, as carriers would have to exercise predictive judgments about what the FCC might construe the statute to mean.”

Looking ahead, companies are likely to push for the FCC to issue notice and rulemaking to provide them with insight into not only what it is expecting to do, but also how its plans coincide with those of the FTC.

“As a regulated entity, the worst thing that can happen is to have two different agencies trying to regulate in different ways and you don’t know what rules to follow,” Zick said. “The FTC thinks it has very broad jurisdiction, and the question is: Have they now bumped up against some other legitimate regulator, and who is going to draw those lines? The turf war is on.”

--Editing by Kat Laskowski and Chris Yates.
