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

The FCC Takes a Seat at the Cyber-Regulation Table

Article By:

Alexander W. Major

Brian D. Weimer

The FCC recently slid up its chair to the fiscal feast that is cyber security and data breach regulation and took a hefty piece of the pie. In late October the FCC announced that it charged a record $10 million fine against two telecommunication companies after the telecoms reportedly posted the private information of nearly 300,000 people in a manner making the people eligible for identity theft. Taking a cue from the Federal Trade Commission ("FTC"), the FCC action was not based on any new set of concrete regulations or laws established to give organizations a minimum bar for data protection, but rather on existing FCC powers established under the Communications Act of 1934. The action serves as good warning not only to communications providers that the FCC will be examining data breaches and, more expressly, data storage issues, but also that in the absence of clear cybersecurity regulations, federal agencies will take an expansive view of their existing authority to address cybersecurity-related incidents involving companies subject to their jurisdiction.

For those unfamiliar with similar FTC actions, over the course of the past several years the FTC has asserted its authority to regulate the handling of consumers' sensitive personal information under the "unfair or deceptive acts or practices" prong of Section 5 of the Federal Trade Commission Act, the basic consumer protection statute enforced by the Commission.. Under Section 5, an act or practice is unfair if "it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." With over fifty of such actions under its belt, the FTC has taken the *de facto* lead on addressing cybersecurity data breaches. That authority has even been confirmed by the U.S. District Court of New Jersey in an action against Wyndham Hotels, a decision that is currently on appeal to the Third Circuit.

Similar to the FTC's response, the FCC's first foray into data beach regulation was born from its interpretation of its existing authority under the Communications Act of 1934 (the "Act"). Under the Act, the FCC is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable throughout the United States and its territories. Moreover, under § 503(b)(1) of the Act, the FCC is authorized to impose a forfeiture penalty against "any person who willfully or repeatedly fails to comply with any provision of the Act." As the FCC described in its Notice of Forfeiture, that is exactly what two companies did, YourTel America and TerraCom Inc., when they collected the data of up to 300,000 customers to determine eligibility for the FCC's low-income discount phone program, "Lifeline." In order to enroll, potential participants had to

demonstrate eligibility by submitting personal information to the Companies, including the applicant's name, address, date of birth, social security number, and driver's license information. Between September 2012 and April 2013, the FCC alleges that applicants' information was stored on data servers that were publicly accessible via the Internet, a fact made known to the FCC after reporters from the Scripps Howard News Service advised the FCC that they were able to access at least 128,066 confidential records by using a simple Google search.

Acting under the authority provided by the Communications Act, as amended by the Telecommunications Act of 1996 , the FCC charged the Companies with violations of Sections 222(a) and 201(b) Under § 222(a), a carrier has a duty "to protect the confidentiality of proprietary information of, and relating to . . . customers." Similarly, § 201(b) makes it unlawful for a carrier to employ "unjust or unreasonable" data security practices related to its "practices," such as, in this case, holding customers' "proprietary information." Relying on the statutorily-inferred breadth Congress included as part of the Telecommunications Act of 1996, the Commission reasoned that "proprietary information" was to be interpreted "broadly to encompass 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." After concluding that that the information gathered by the Companies fell within the statutory protections of § 222(a), the FCC charged that the Companies violated:

- § 222(a) for failing to protect the confidentiality of proprietary information that consumers provided for Lifeline enrollment;
- § 201(b) for failing to employ reasonable data security methods to protect consumers' proprietary information;
- § 201(b) for misrepresenting in their privacy policies that they employed reasonable security measures to protect customers' proprietary information; and
- § 201(b) for failing to notify all affected customers.

The $10 million fine levied against the two companies as a result of these alleged violations is worth noting for several reasons:

(1) The FCC has adopted a broader interpretation of "customer" that would include protection of proprietary information even before an applicant becomes a subscriber. Now applicants, like subscribers, "have a reasonable expectation that the carrier will protect the confidentiality of the PI they provide as part of that transaction."

(2) Telecommunication providers could very well be subject to regulation by both the FCC and the FTC for data security breaches that may occur. Therefore, it is extremely important that they ensure that their cybersecurity efforts in protecting a customer's proprietary information are "just and reasonable" under the Act. In the absence of clear guidelines or regulations telling companies what exactly "reasonable" means, this is a challenge that will require providers to adopt and implement a clear data and information security (DAIS) program that enables them to defend the reasonableness of their security measures should a breach occur.

(3) When a breach does occur, providers must ensure that their incident response plans provide for timely notice to all consumers affected by a data breach and be responsive not only to federal

requirements but to all individual state requirements, as appropriate.

(4) Telecommunication companies must ensure that their representations about security measures to protect customer proprietary information accurately reflect the security measures the provider has in place.

The FCC's foray into the world of cybersecurity regulation, along with a host of other federal regulatory agencies (the Federal Trade Commission, Securities and Exchange Commission, and Department of Justice), further underscores the lack of established regulations or laws capable of providing organizations a minimum bar for data protection. In that vacuum, agencies are scrambling to figure out what to do about cybersecurity and how to do it – a messy proposition. So, while industry regulators belly-up and find room at the data breach table, companies should take a solid look at their cybersecurity efforts and make sure their data and information security plans leave nothing on the table whetting those appetites.

National Law Review, Volume IV, Number 335