ENFORCEMENT ACTION SIGNALS EXPANSION OF FCC OVERSIGHT OVER CONSUMER DATA SECURITY

Brita Strandberg and Adrienne E. Fowler[1]

On October 24, 2014, the Federal Communications Commission released a Notice of Apparent Liability for Forfeiture against two telecommunications companies, TerraCom, Inc. and YourTel America, Inc., for alleged data-security related violations of the Communications Act. The Notice calls for a $10 million forfeiture and represents the FCC's first foray into a new realm of data security regulation. It may also portend more aggressive FCC action on data security going forward.

I. Background

TerraCom and YourTel America are affiliated telephone companies that offer services to low-income Americans through the Lifeline program. The FCC alleges that the companies' call center, which was operated by a sub-contractor, collected information from consumers trying to sign up for Lifeline, including name, address, social security number, address, and date of birth. According to the FCC, the sub-contractor stored all of this information online in an unencrypted format that could be accessed from any internet-connected computer without a password. As a result, consumers who had given their personal information to TerraCom and YourTel American could be at high risk for identity theft.

II. New theories of liability for data security failures at the FCC

The Commission asserts that TerraCom and YourTel are liable for their subcontractor's lack of data security on several different theories. Each of these theories represents a significant new policy direction for the FCC.

A. Failure to take reasonable precautions to protect "proprietary information" belonging to customers and applicants violates the Communications Act

The FCC has a long history of (and a detailed set of rules about) protecting the privacy of one particular kind of personal information: customer proprietary network information, or "CPNI." CPNI is a relatively narrow category of information that includes information about a customer's use of telecommunications services, such as the numbers the customer called, how long each conversation lasted, and certain billing information. Importantly, a customer's name, address, social security number, birth date, and many other types of personal information is *not* CPNI, and had previously been unregulated by the FCC.

In the TerraCom Notice, however, the Commission announces that telecommunications providers have a duty under the Communications Act to protect an entirely different type of personal information: "proprietary information" that has nothing to do with a customer's use of a network. The Commission takes the position that a consumer's name, address, social security

[1] Admitted only in NY; supervised by Brita Strandberg, member of the D.C. Bar, pending D.C. admission.

number, and birth date are proprietary information – and that a telecommunications provider's failure to adequately protect that information can result in an enforcement action.

Moreover, in the TerraCom Notice, the Commission interprets "proprietary information" to include information submitted by a consumer who is applying for service, regardless of whether the consumer ultimately purchases services from a telecommunications provider.

B. Liability for "unjust" or "unreasonable" data security practices

The Commission has brought a variety of enforcement actions over the years, charging telecommunications providers with engaging in unjust or unreasonable practices. In the TerraCom Notice, the Commission for the first time takes the position that data security failures can constitute unjust and unreasonable practices. It takes the position that it is unjust and unreasonable for a telecommunications provider to:

1. Lack basic data security to protect customer proprietary information;
2. Misrepresent the level of data security provided, either implicitly or explicitly; or
3. Fail to notify *all* customers potentially affected by a data security breach.

The breach notification requirement is especially noteworthy. In most instances, state law dictates whether a company must notify a particular consumer that his or her data may have been compromised in a data breach. Under the TerraCom Notice, however, a telecommunications provider that experiences a data breach may be required to notify all consumers potentially affected by the breach, regardless of where they live.

* * * * *

For more information regarding FCC regulation of data security or Harris, Wiltshire & Grannis's privacy practice, please contact **Brita Strandberg** at (202) 437-4066 or bstrandberg@hwglaw.com, or **Adrienne Fowler** at 202-730-1343 or afowler@hwglaw.com.