The US Federal Communications Commission steps up data privacy expectations with record $10 million fines

On 24 November 2014, the FCC announced plans to fine two telecommunications carriers - TerraCom, Inc. and YourTel America, Inc. - a total of $10 million for failing to protect certain customer data.

In the US, data privacy enforcement actions at the federal level typically have been the domain of the Federal Trade Commission ('FTC'), which has brought more than 30 legal actions against organisations under its general authority to police unfair and deceptive acts and practices. However, the Federal Communications Commission ('FCC'), the nation's telecommunications regulator, recently jumped into the data privacy fray, expanding the data privacy requirements applicable to telecoms carriers in the process. In November, the FCC announced plans to fine two telecoms carriers - TerraCom, Inc. and YourTel America, Inc. - a total of $10 million for failing to protect certain customer data[1].

The FCC alleged that the two carriers, which provide discount phone services to low income individuals, stored customer 'proprietary information' on unprotected servers accessible to the public. The fine, approved by a 3-2 vote of the FCC, represents the largest privacy action in FCC history, eclipsing a $7.4 million fine handed down to Verizon for failing to provide customers with required notices about Verizon's use of Customer Proprietary Network Information ('CPNI').

TerraCom and YourTel America provide discounted phone services to low income customers through Lifeline, a US government program administered as part of the Universal Service Fund. In order to verify eligibility for the program, both companies gathered information, including Social Security numbers, names, and addresses, from applicants and customers. Applicants submitted this information by uploading scanned documents and completing online forms. Both carriers' privacy policies stated that they utilised 'technology and security features to safeguard the privacy of your customer specific information from unauthorized access or improper use,' and pledged to 'continue to enhance [their] security measures as technology becomes available.'

Both carriers' stored applicants' completed forms and scanned documents in dedicated space on a third party's servers from September 2012 until April 2013. According to the FCC's later findings, the servers were publicly accessible via the internet and no form of password protection or enhanced security measures were utilised. In early 2013, a reporter from Scripps Howard News Service inadvertently discovered the online records through an internet search while researching the carriers. After discovering that over 120,000 records were easily accessible, Scripps notified the carriers in April 2013. The carriers responded by sending a 'cease and desist' letter accusing Scripps of illegally accessing the information and notified the FCC's Enforcement Bureau of the alleged unauthorised access the following month.

In its enforcement action, the FCC found that information regarding 305,000 customers was stored on publicly accessible servers between September 2012 and April 2013. The FCC determined that the failure to protect this information, combined with the carriers' privacy policies, violated Section 222 and Section 201 of the Communications Act. The FCC also found that the carriers' failure to promptly notify customers of the breach violated Section 201 and had prevented them from taking steps to avoid identify theft.

The FCC's action in this case is notable because it appears to mark the first time the FCC has applied Section 222 rules designed to protect a specific category of customer data - CPNI - to activity that resulted in the public exposure of a broader range of data, which the FCC referred to as 'proprietary data.' Under Section 222(c), the use or disclosure of CPNI, or customer proprietary network information, is strictly limited. CPNI includes information related to the 'quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service' by a customer, which the telecoms provider receives through its relationship with the customer. A telecoms carrier who receives CPNI cannot use, disclose, or permit access to it outside of its provision of services from which the information is derived unless such use or disclosure is approved by the customer or required by law. Section 222 contains a series of exceptions to the prohibition on CPNI use and disclosure, including billing for telecoms services or use in an emergency.

However, according to the FCC's enforcement action, both companies violated Section 222(a), which requires telecoms carriers to 'protect the confidentiality of [customers'] proprietary information.' Proprietary information is not defined in Section 222, but the FCC's notice regarding the proposed fine describes the information that customers provided to demonstrate eligibility for Lifeline services as proprietary information. The FCC acknowledged that this interpretation of proprietary information is broader than the category of CPNI defined in the statute, but stated that its interpretation of the term is consistent with its previous actions and Congressional intent. According to the FCC, Congress used the term 'proprietary

information' in Section 222 to encompass 'all types of information that should not be exposed widely to the public.'

In its notice, the FCC stated that Section 222(a)'s protection of proprietary information should be read to include 'privileged information, trade secrets, and personally identifiable information (PII).' Although the FCC did not adopt a formal definition of PII, they cited the definition used by the National Institute of Standards and Technology ('NIST') as 'informative.' The NIST definition of PII includes '(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.' Under this definition, all of the information submitted by applicants to TerraCom and YourTel America constituted proprietary information. This reading of Section 222, and the enforcement power it grants to the FCC, represents a noteworthy expansion when compared to previous FCC actions focusing on CPNI under Section 222.

In addition, the FCC rejected the carriers' argument that information provided by rejected applicants was not information 'relating to […] customers' under Section 222(a). In doing so, the FCC noted that potential customers place their trust in telecoms carriers to safeguard information the customer discloses prior to subscribing to the service. According to the FCC, a customer relationship is established for the purposes of Section 222(a) when a consumer divulges proprietary information to the carrier, not when the consumer actually subscribes. However, the FCC noted that this definition of 'customer' should not apply uniformly throughout Section 222. While Section 222(a) protects 'proprietary information' provided by applicants as well as current subscribers, Section 222(c), which protects CPNI, is limited to protection of current subscribers.

The FCC's action is also notable because it marks the first time the FCC has determined that a failure to adequately protect customer data amounts to an 'unjust and unreasonable' practice in violation of Section 201(b) of the Communications Act. In this respect, the FCC's action appears to create a standard similar to the FTC's 'Safeguards Rule,' which requires that companies take industry appropriate steps to protect certain types of data. The FCC found that the carriers 'failed to employ even the most basic and readily available technologies and security features' to protect customers' proprietary information. Although the FCC cautioned that encryption, without more, would not satisfy a carrier's duty to protect proprietary information under Sections 222 and 201, the carriers' failure to use encryption and password protection amounted to an unjust and unreasonable practice.

Finally, the FCC's action also marked the first time that the agency has issued a proposed fine for a carrier's failure to notify subscribers of a breach. The carriers, relying on state-specific data breach notification requirements, informed over 35,000 customers that their information had been exposed. However, the FCC determined that the 'notification of anything less than all potentially affected consumers' constituted an unjust and unreasonable practice in violation of Section 201(b) in light of the identity theft risks posed by the carriers' actions. The FCC also focused on the carriers' inability to conclusively determine the scope of the breach. Although the carriers estimated that only 128,066 records were actually accessed by unauthorised third parties, the FCC found that Section 201(b) required notification of all customers whose information was stored in an unsafe manner and could have been subject to access.

Telecoms carriers may find important clues about the FCC's data privacy expectations in TerraCom and YourTel America. By including Social Security numbers and other personal information within the reach of Section 222, the FTC has expanded Section 222 beyond CPNI to any information considered 'proprietary,' including PII and information supplied by applicants who have not yet entered into a consumer relationship with the carrier. In addition, the fine demonstrates that the FCC is paying close attention to the measures that carriers use to safeguard proprietary information, as well as the speed and scope of post breach notifications. Although the FCC did not offer specific security recommendations, carriers should be aware that encryption of proprietary information, without additional safeguards, does not satisfy the requirements of Sections 201 and 222. Carriers should consider the adoption of additional data security measures and develop a plan to notify all potentially affected consumers in the event of a data breach.

Kurt Wimmer Co-Chair, Privacy and Data Security Practice
Covington & Burling, Washington DC
kwimmer@cov.com

1. Summary available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-330136A1.pdf