ROPES & GRAY

ALERT

Privacy & Data Security

November 12, 2015

FCC Expands Its Claim of Data Security Authority with Recent Enforcement Action Against Cox Communications

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
David T. Cohen
Sunil Shenoi

Last week, the Federal Communications Commission ("FCC") reached a settlement with Cox Communications, Inc. ("Cox") regarding a 2014 data security breach that allegedly exposed the personal information of at least 54 current customers and seven former customers. The settlement requires Cox to pay $595,000 and undertake enhancements to its data security compliance program. The FCC's action against Cox is its first data security enforcement action involving a cable operator as well as its first action involving a hacking incident. Representing the FCC's third data security settlement in 2015, the Cox action signals that the agency's presence will continue to grow in a crowded field of regulators claiming authority in the privacy and data security space. Moreover, for the first time, the FCC imposed specific technological requirements on a company rather than merely requiring compliance with general data security standards. This use of specificity stands in marked contrast to the approach historically used by the Federal Trade Commission, the most active federal agency in the area of data security, whose consent orders have utilized a general "reasonableness" standard.

The FCC's enforcement action relates to an August 2014 breach by a hacker who allegedly used a social engineering plot called pretexting to gain access to Cox's systems. According to the FCC, the hacker, part of the "Lizard Squad" group that has conducted well-publicized breaches of other companies' networks, pretended to be a member of Cox's information technology department and convinced a Cox customer service representative and a Cox contractor to enter their credentials into a fake website. From there, the hacker was able to view certain personal information of some of Cox's current and former customers, including their names, home addresses, email addresses, phone numbers, partial Social Security Numbers, and partial driver's license numbers. The hacker was also able to access some telephone customers' account-related data, known as customer proprietary network information ("CPNI"). In addition, the hacker posted the personal information of at least eight customers on social media sites, changed the passwords of at least 28 other customers, and shared some of the personal information with another hacker. Incidentally, one of the customers about whom the hacker obtained information was a well-known data security researcher. Cox was alerted to the breach from a customer who found their account information on a social media website. Within six days, Cox contacted the FBI but allegedly never disclosed the breach to the FCC, which the FCC viewed as a violation of its regulations.

The FCC's settlement with Cox resolved the FCC's investigation into whether Cox violated Sections 201(b) and 222(a) and (c), and 631 of the Communications Act of 1934, and Sections 64.2010(a) and 64.2011(b) of the FCC's rules. Section 201(b) requires that certain practices in connection with communication services must be just and reasonable, and the FCC interprets this provision as requiring companies to employ just and reasonable practices to protect consumers' proprietary information. The FCC also asserts that Section 222 requires telecommunications carriers to protect both CPNI and other customer information that is not CPNI, and points to Section 222's restrictions on how such carriers can "use, disclose, or permit access to" CPNI. Section 631 places certain restrictions on cable operators' disclosure of subscribers' personally identifiable information without their consent and requires the cable operator to take certain actions to prevent unauthorized access to such information. Section 64.2010(a) of the FCC's rules imposes certain requirements on telecommunications carriers to take reasonable steps to safeguard CPNI. Section 64.2011(b) requires telecommunications carriers to notify the FCC of certain compromises of CPNI.

Pursuant to the terms of the consent decree, Cox agreed to pay a penalty of $595,000, the smallest of the three penalties it has secured in its data security actions to date. Cox also agreed to improve its data security practices by developing and implementing a data security compliance plan, which includes a risk assessment, a documented information security program, an employee training program, and other measures. Cox further agreed to designate a compliance officer who will be responsible for ensuring Cox's compliance with the obligations under the consent decree. Cox also promised to notify certain customers of unauthorized access to their information and to provide them with a year of complimentary credit monitoring.

The FCC's action against Cox reveals the growing scope of the FCC's claim of authority with respect to data security, both in terms of the nature of the entities and the type of incidents it seeks to regulate. While previous enforcement actions involved only telecommunications providers (AT&T and TerraCom/YourTel), the Cox action represents the FCC's first action against a cable provider and therefore the agency's first application of Section 631 to the data security context. Moreover, the Cox action is the first time the FCC has sought to hold a company responsible for unauthorized access occurring in the context of an alleged hacking incident, unlike its prior actions, which involved allegations of unauthorized access by companies' own personnel or storage of personal information in Internet folders accessible via a search engine and basic manipulation.

The consent decree also requires Cox to implement specific technological solutions, a substantial departure from the more general requirements agreed to by AT&T and TerraCom/YourTel. For instance, the decree requires Cox to implement a security information and event management (SIEM) system and site-to-site VPN for access to its network by its vendors. It also provides that the required data security risk assessment must be conducted with reference to the NIST Cybersecurity Framework, and requires the use of multi-factor authentication or equivalent controls for remote access, annual penetration testing, and annual test exercises of the company's incident response plan. In addition, in connection with future data security breaches, Cox must offer complimentary credit monitoring to certain customers whose unredacted and/or unencrypted personal information or CPNI is reasonably believed to have been acquired, as well as take certain steps to monitor known websites for breach activity to identify potentially stolen personal information or CPNI. By contrast, the FCC's prior consent decrees, as well as those entered into by the Federal Trade Commission, the federal agency most active in the area of data security, have typically imposed a general "reasonableness" standard on the target of the investigation. Also, notably, the technical requirements in the Cox consent decree do not appear to be limited to remediating the particular alleged deficiencies that the FCC contended led to the data security breach. For instance, SIEM systems do not typically address phishing scams like the one purportedly used against Cox.

The Cox action also suggests that a data security breach of limited scope may nevertheless result in an FCC enforcement action. The hacker in the Cox action allegedly viewed without authorization the personal information of at least 61 customers and the CPNI of four of those 61 customers. The hacker also allegedly publicly disclosed personal information or CPNI of eight of those 61 customers. The Cox incident is therefore far removed from the AT&T and TerraCom/YourTel incidents, which allegedly involved more than 51,000 and 300,000 customers, respectively, whose personal information had been exposed. Furthermore, as the Cox consent decree itself notes, only limited types of personal information were alleged to have been stolen.

Finally, companies should take note of the position taken by the FCC in this case that simply notifying and coordinating with law enforcement in connection with the security breach, as Cox did, was not sufficient, and that Cox should also have notified the FCC. When assessing whether and to whom notifications should be made in the wake of a data security breach, companies should carefully consider whether their primary regulator – even if not the FCC – may take a similar position.

For more information regarding the settlement between Cox and the FCC or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.