Chicago Daily Law Bulletin®

Volume 162, No. 96 Serving Chicago's legal community for 161 years

FCC proposal looks to expand privacy rules to broadband companies

Hackers are using increasingly sophisticated methods to access the personal information of consumers — from pretending to be employees to gain insider credentials to setting up fake e-mail addresses and websites to collect customer information.

The Communications Act imposes regulations on the communication industries in the United States, including telephone and radio, to protect sensitive customer information, but broadband Internet service providers aren't subject to these rules.

FCC Chairman Tom Wheeler hopes to change this. In March, he circulated Proposal to Give Broadband Consumers Increased Choice, Transparency & Security With Respect to Their Data, which proposes applying the act's privacy requirements to broadband providers to give customers the ability to decide how and to what extent their personal information is used and shared.

In a nutshell, Wheeler's Notice of Proposed Rulemaking would apply the privacy requirements of the Communications Act to broadband Internet access service.

The proposal would require that broadband providers obtain customer consent before using and sharing personal data and to take steps to protect that data. Broadband providers would also be required to report data breaches to the FCC and other government entities.

In 2015, the FCC investigated and reached settlements with three communications companies for failing to keep customers' personal data safe. All three settlements demonstrate the lengths to which hackers are going to access consumers' information. And the FCC's belief that the telecommunications companies alleged failure to safeguard customer information violates the Communications Act.

In April 2015, the agency settled with AT&T Services Inc. for $25 million, holding AT&T responsible for failing to protect the information of nearly 280,000 customers. At least two AT&T employees were allegedly involved in the breach and confessed to selling the customer information to a third party.

The FCC also reached a $3.5 million settlement with TerraCom Inc. and YourTel American Inc. in July. In this case, a vendor for the two companies stored the proprietary information of more than 300,000 customers in clear, readable text on servers that were accessible over the Internet.

According to the FCC, the data was not password protected or encrypted. The companies also didn't report the data breach to the agency until after news stories on the breach were published.

An FCC investigation of a data breach at Cox Communications Inc. resulted in a $595,000 settlement agreement in November for the company's failure to protect customer information or report the breaches to the agency.

According to the FCC's Enforcement Bureau, a member of a hacker group called Lizard Squad accessed Cox's customer information in 2014 by allegedly pretending to be a Cox tech employee. The hacker convinced a Cox customer service representative and a Cox contractor to enter their account IDs and passwords into a fake website controlled by the hacker.

Armed with the Cox credentials, the hacker accessed sensitive customer data including names, home addresses, e-mail addresses, phone numbers, partial Social Security numbers and partial driver's license numbers as well as customer proprietary network information belonging to the company's telephone customers.

The hacker allegedly shared the Cox credentials with another alleged member of the Lizard Squad, posted customers' personal information on social media sites and changed some customers' account passwords.

Enacted in 1934, the Communications Act regulates U.S. telephone, telegraph, television and radio communications, created the FCC and gave it the authority to regulate those industries.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

Even when data is encrypted, these providers still can see the websites that a customer visits, how often and the amount of time he or she spends on each website.

The act has been updated periodically to add provisions governing new communications technologies, including broadcast, cable and satellite television. The Telecommunications Act of 1996 amended the Communications Act to include telecommunications providers.

Broadband providers, also known as Internet service providers, have the ability to collect the personal information of customers and also can view customers' unencrypted online activities. The Internet providers also can track customers' locations and movements through their mobile devices.

Even when data is encrypted, these providers still can see the websites that a customer visits, how often and the amount of time he or she spends on each website.

"Using this information, ISPs can piece together enormous amounts of information about their customers — including private information such as a chronic medical condition or financial problems," according to a fact sheet published at the same time as Wheeler's proposal.

According to the fact sheet, the proposal "does not prohibit ISPs from using or sharing customer data, for any purpose." It merely proposes giving consumers the choice to opt out or to require that the provider first get permission from customers before using and sharing their data.

Social media websites like Facebook and Twitter, which are regulated by the Federal Trade Commission, are outside the scope of the proposal. The proposal's privacy rules would not apply to government surveillance, encryption or law enforcement.

In advocating for the application of privacy and data security rules to all Internet service providers, the proposal asserts that transparency and security are crucial to protecting consumer privacy and that broadband providers should give

their customers the ability to choose what personal data providers can collect and use and under what circumstances a provider can share consumer information with third parties or affiliated companies.

The proposal also asserts that broadband providers should be transparent and disclose what information they collected, how they use the information and under what circumstances they share it with other entities. Providers also should disclose privacy and data security in an easily understandable and accessible manner.

Finally, the proposal asserts that broadband providers have a responsibility to keep consumer data secure, both as it is stored and as it is transmitted across their networks.

To enforce the responsibility to protect consumer information and help consumers make educated decisions about privacy, the proposal creates three categories of data use.

The first category of data use is information used to provide and market the broadband provider's own services. For this category, consent is inherent in a customer's decision to purchase its services; no additional consent is needed to use the data for this purpose.

The second category of data use is using information for marketing other communications-related services and to share customer data with their affiliates for marketing.

For this category, the customer must be given the opportunity to opt-out of having his or her information used in this way. All remaining uses fall into the third category and requires an "opt-in" consent from customers.

Wheeler's proposal creates a data security standard, requiring broadband providers to take "reasonable steps" to safeguard customer information from unauthorized use or disclosure.

At minimum, broadband providers would have to: Adopt risk management practices; train personnel; adopt strong customer authentication requirements; designate a senior manager to be responsible for data security; and take responsibility for the use and protection of customer information when shared with third parties.

To encourage Internet service providers to protect the customer data, Wheeler's proposal also includes breach notification requirements. In the event of a data breach, providers must notify affected customers of breaches of their data no later than 10 days after discovery; the FCC must be notified of any breach of customer data no later than seven days after discovery; and the Federal Bureau of Investigation and the U.S. Secret Service must be notified no later than seven days after discovery of the breach in the event of breaches affecting more than 5,000 customers.

Privacy activists generally support the proposed rules. One notable critic of Wheeler's recommendations is FCC Commissioner Michael O'Rielly, who slammed the proposal in a short but strongly worded statement.

O'Rielly accuses Wheeler of "imposing troubling and conflicting 'privacy' rules on Internet companies as well as freelancing on topics like data security and data breach that are not even mentioned in the statute."

O'Rielly calls the proposal a "reckless approach to an important topic, especially where it clearly lacks expertise, personnel or understanding."

Among other organizations, the National Cable and Telecommunications Association says it is disappointed by Wheeler's attempt "to propose prescriptive rules on ISPs that are at odds with the requirements imposed on other large online entities."

The association calls for "an approach that will ensure greater consistency in consumer privacy protection and fair competition among all Internet participants."

Despite the criticism, the full commission voted 3-2 in favor of the proposal on March 31. The resulting 147-page notice of proposed rulemaking published in the Federal Register poses more than 500 questions for comment.

While the agency called for initial comments by May 27, at least one group has asked the FCC to extend the comment period for another 60 days, an extension until July 26.