

Verizon Agrees to Pay \$1.35 Million to Settle FCC “Supercookie” Investigation

March 11, 2016

On March 7, 2016, the FCC’s Enforcement Bureau announced that it reached a [settlement](#) with Verizon Wireless to resolve an investigation into whether Verizon violated the Commission’s rules by inserting Unique Identifier Headers (UIDH) – informally known as “supercookies” – into consumers’ Internet traffic over its wireless network as part of the company’s targeted advertising programs, and then failing to disclose this practice to its customers or take adequate steps to protect the information. The consent decree requires Verizon to pay a \$1.35 million fine, as well as take other actions to avoid similar missteps in the future.

The Verizon consent decree is the latest in a series of high profile actions to enforce the Commission’s privacy and data security rules. Compared to other settlements, however, Verizon seems to have escaped this enforcement action relatively unscathed.

Background

Verizon first began inserting UIDH into certain subscribers’ HTTP Internet traffic in December 2012. Verizon was using these headers as part of two targeted advertising programs which “associate[d] the UIDH with customer proprietary information as well as demographic and interest information to create profiles in order to serve targeted advertisements.” The FCC began its investigation into Verizon’s use of UIDH in December 2014, following multiple news reports that Verizon’s actions could negatively impact consumer privacy. During the course of the investigation, the Commission learned that although Verizon had been inserting UIDH since 2012 and provided some general information about UIDH on its website, the company “did not specifically disclose the presence of UIDH and its uses until October 2014.” Additionally, one of Verizon’s advertising partners was able to use UIDH to restore deleted cookies on consumers’ mobile browsers.

In the consent decree, the Enforcement Bureau suggests that Verizon’s conduct potentially violated Section 222 of the Communications Act of 1934 (47 U.S.C. § 222) because the improper use of UIDH by its advertising partner indicated that Verizon failed to protect its customers’ proprietary information. Additionally, the decree notes that Verizon’s failure to adequately disclose its use of UIDH, particularly when consumers had to affirmatively opt out of the targeted advertising program, may have been a violation of the company’s obligation under the Commission’s Open Internet Transparency Rule (47 C.F.R. § 8.3) to “disclose accurate information regarding their mobile broadband Internet access services sufficient for consumers to make informed choices regarding such services.” (The consent decree noted that the conduct under investigation was not subject to the enhanced Transparency Rule adopted in the 2015 Open Internet Order because it predated the order.)

Terms of the Consent Decree

Under the terms of the consent decree, Verizon has agreed to pay a \$1.35 million fine, and to implement a wide-ranging compliance plan, which includes the following key elements:

- **Opt-In.** Verizon may not share customer UIDH with third parties for the purpose of delivering targeted advertising unless the customer gives Verizon prior opt-in consent. Moreover, customers that opt-in must be permitted to subsequently opt out at any time.
- **Security.** Verizon must only generate UIDH of a customer through “methods that comply with reasonable and accepted security standards.”
- **Operating Procedures.** Within 60 days, Verizon must establish operating procedures that ensure compliance with the consent decree.

Verizon also must appoint a compliance officer, report all instances of non-compliance with the consent decree within 15 days of discovery of the non-compliance, and submit periodic compliance reports to the Commission for the next three years.

Lessons Learned

In recent years, the Enforcement Bureau has been aggressive in its efforts to enforce the FCC’s rules, particularly with respect to consumer and privacy issues. We expect this trend to continue for the foreseeable future. While the terms of Verizon’s settlement are not as severe as many other recent FCC enforcement cases, this action nevertheless should serve as a reminder to all telecommunications and broadband providers to take affirmative steps to inventory their own data security policies, procedures, and practices, as well as those of their vendors, to ensure compliance with FCC rules and guidance.