Client Advisory: The FCC's Broadband Privacy Order

November 10, 2016

On Wednesday, November 2, 2016, the Federal Communications Commission (FCC) released the text of its long-awaited Broadband Privacy Order, which it adopted on October 27, 2016. For an overview of the Order, you may read our client advisory here.

The practical impact and reach of the rules will not be known for some time, but at this point we can offer a few of our key takeaways from the Order:

- **All carriers must prepare and maintain public-facing privacy notices.** The Commission's new notice rules will require all telecommunications carriers to draft and post public-facing privacy policies that describe their collection, use, and sharing of customer PI. Formerly, this obligation only applied to BIAS providers (through the Commission's transparency rule). We expect that disclosures in these privacy policies will be a significant area of enforcement, similar to the Commission's enforcement of annual CPNI certifications.
- **The sensitivity-based consent framework upends the existing CPNI approval framework.** The Commission's adopted rules fundamentally reshape the consent framework for telecommunications carriers, focusing on the sensitivity of the information, rather than on the particular uses and recipients of the information (as the voice CPNI rules did). As a result, all carriers should carefully review and revise their policies, procedures, and systems for obtaining and tracking customer approval.
- **The Order leaves a significant interpretive role for FCC's Enforcement Bureau with respect to data security.** Unlike the existing voice CPNI rules and the Commission's proposed data security rules, which mandated specific data security compliance practices, the new rules simply require carriers to adopt "reasonable" data security practices. By focusing on the "reasonableness" of carriers' privacy and data security practices, the Commission leaves significant room for its Enforcement Bureau to interpret whether particular practices are reasonable, in a manner similar to the FTC's approach to privacy and data security enforcement. For this reason, providers should carefully review the Commission's "exemplary" data security practices and Enforcement Bureau consent decrees in order to gauge which practices the Commission expects of providers.
- **Now is the time to begin reviewing contracts with vendors.** In the Order, the Commission makes clear that carriers will be held responsible for the acts of their agents, vendors, and other third parties with whom they share customer PI. As a result, carriers should take the opportunity now to review contracts with those third parties to determine whether they include specific terms addressing privacy and security. This is particularly important for non-BIAS telecommunications carriers serving enterprise customers, who will be able to take advantage of the Commission's expanded business customer exemption.

Kelley Drye's Communications and Privacy & Information Security practice groups are well-versed in

privacy law at the federal and state level, and stand ready to help interested parties understand the scope of these rules and how to operationalize them. Should you have any questions, please contact any of the attorneys listed in the margin.