DrinkerBiddle

Client Alert

March 16, 2017

FCC Stays Portion of Broadband Privacy Rules

By Kenneth K. Dort, Katherine E. Armstrong, Lee G. Petro and Anthony D. Glosson

Key Takeaways

- FCC stays enforcement of new data security requirements for broadband providers.
- Republican FCC and FTC regulators issue a joint statement contending that the move would allow the two agencies to develop a comprehensive and consistent privacy framework.
- Democratic commissioners from both agencies issue a joint statement expressing concern that broadband providers would lack sufficient federal data security regulation while the stay remains in place.
- Broadband internet access service providers should still consider what compliance might require of them in case the rules as reformed retain elements of the stayed rules.

In a much anticipated announcement on Wednesday, March 1, 2017, FCC Chairman Ajit Pai stayed a portion[1] of the broadband privacy rules released on November 2, 2016, that would have required broadband service providers to adhere to an FCC-defined standard of "reasonable" data security practices.[2] The March 1 action drew criticism from privacy activists, who contended that the FCC's stricter rules were justified by a broadband market that is relatively more consolidated than the edge provider competitors. Conversely, many broadband internet access providers praised the decision as a step toward a "common sense" even-handed approach to privacy regulation. The move also suggests that Chairman Pai will take a proactive approach toward addressing privacy regulations, perhaps lessening the likelihood that Congress will exercise its Congressional Review Act authorities to veto the controversial privacy rules – a course of action that could dramatically limit the FCC's ability to regulate broadband privacy in the future.

The November 2016 rules were initially adopted to address the data privacy regulatory gap created when the FCC assumed regulatory authority over broadband providers by classifying them as telecommunications service providers subject to many of the rules that the FCC has promulgated under Title II of the Communications Act of 1934. This approach represented a dramatic departure from the historical status of broadband internet access service as an "information service," subject mainly to the Federal Trade Commission's (FTC) Section 5 enforcement authority.

Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in interstate commerce. The FTC's privacy and data security agenda has focused on misrepresentations of privacy and data security practices as well as unfair acts or practices that cause consumer harm. Although the FTC does not have authority to regulate telecommunications service providers,[3] it has brought enforcement actions against telecommunications service providers for what it viewed as non-carrier or service provider activities. When the FCC reclassified broadband internet access service, that reclassification effectively removed such entities from the FTC's jurisdiction and created a privacy regulatory gap. Following the FCC's assertion of regulatory authority over broadband providers, the Section 5 regime continues to apply to edge providers, but broadband providers were no longer subject to the FTC's Section 5 authority.

Under the leadership of Chairman Wheeler, there was disagreement between the FCC's Democratic and Republican commissioners about the way to address consumer privacy and broadband services. The November 2016 rules that the FCC ultimately adopted include detailed data privacy obligations, a breach notification procedure, a notice-and-choice framework governing the collection of personal information, and a prohibition on conditioning broadband service on the waiver of any FCC-mandated privacy rights, in addition to the stayed data security requirements. There was concern raised by the Republican commissioners, policy analysts, and many broadband providers that the privacy regulations would subject broadband internet access service providers to a higher degree of regulatory scrutiny than that faced by edge providers and other competitors in the consumer data market. Instead, Republican commissioners argued that the FCC should conform its broadband privacy rules to those applicable to edge providers under Section 5 of the FTC Act. These concerns were echoed by FTC staff, which noted in comments filed to the FCC docket that any approach that treated broadband providers differently than their edge provider

1 See 47 C.F.R. 64.2005 (as amended).

2 Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report and Order, 31 FCC Rcd 13911, 14009 (2016).

3 See AT&T vs. FTC, 15-16585 (Aug. 29, 2016), https://cdn.ca9.uscourts.gov/datastore/opinions/2016/08/29/15-16585.pdf.

competitors would be "not optimal."

The FCC's order adopting the rules was published in the Federal Register on December 12, 2016, kicking off a set of staggered effective dates for various components of the broader rules. Specifically, the timeline had been set to unfold as follows:

- January 3, 2017 – Prohibition on Conditioning Service on Consumer's Waiver of Privacy Rights becomes effective.
- March 2, 2017 – Data Security rules become effective.
- June 2, 2017 – Breach Notification procedures become effective (unless OMB fails to approve the breach notification rules prior to this date, in which case the Wireline Competition Bureau will issue a public notice upon OMB approval setting the compliance date at eight weeks after the date of the public notice).
- December 2, 2017 – Notice and Choice rules become effective (unless OMB fails to approve the notice and choice rules prior to this date, in which case the Wireline Competition Bureau will issue a public notice upon OMB approval setting the compliance date at eight weeks after the date of the public notice).

At the time Commissioner Ajit Pai was appointed Chairman by President Trump, the initial prohibition on conditioning broadband internet access service on the waiver of FCC-created privacy rights had already become effective, but the other components of the data privacy rules were not yet in force. On March 1, 2017, Chairman Pai held a vote to stay the applicability of the data security portion of the broadband privacy rules. In an unusual joint statement by Chairman Pai and FTC Acting Chairman Maureen Ohlhausen, these regulators explained that the reprieve would enable both agencies to coordinate on a comprehensive privacy regulatory framework to ensure regulatory parity between broadband internet access providers and edge providers. FCC Democratic Commissioner Mignon Clyburn issued a joint statement with FTC Democratic Commissioner Terrell McSweeny criticizing the stay of the rules as harmful to consumer privacy and ultimately dissented from the stay order, contending that the data security rules were not as onerous as the majority suggested.

The FCC's vote to suspend enforcement of the rules had a number of immediate effects, including most prominently the fact that broadband internet access providers will not immediately be subject to liability for failure to meet the data security standards created by the November 2016 rules.

In the coming months, it is possible that additional deadlines will be reexamined or stayed, or the rules scrapped altogether as the FTC/FCC joint framework comes to fruition. Nevertheless, broadband internet access service providers may continue preparations to comply with the rules in case the stay is lifted or, as seems more likely, the reformed regime retains certain elements of the rules as they stand today.

It is noteworthy that the same day that the privacy rules were stayed, three bills were introduced in the House Energy and Commerce Committee by Democrats calling for FCC-led cybersecurity initiatives and regulations. One of the bills, the Interagency Cybersecurity Cooperation Act, calls on the FCC to create an interagency panel to investigate and review cyber incidents. Under the proposed Cybersecurity Responsibility Act, the FCC would set cybersecurity regulations for communications networks as a form of critical infrastructure protection. In addition, the Securing the Internet of Things Act requires that web-connected devices comply with design security principles established by NIST and the FCC.

Drinker Biddle's Information, Privacy, Security and Governance team will continue to monitor developments on this issue and update clients as events warrant.

Information Privacy, Security and Governance Team

Primary Contacts

Kenneth K. Dort
Partner
Chicago
(312) 569-1458
Kenneth.Dort@dbr.com

Katherine E. Armstrong
Counsel
Washington, D.C.
(202) 230-5674
Katherine.Armstrong@dbr.com

Lee G. Petro
Of Counsel
Washington, D.C.
(202) 230-5857
Lee.Petro@dbr.com

Anthony D. Glosson
Associate
Washington, D.C.
(202) 230-5131
Anthony.Glosson@dbr.com

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON