

Congress Has Repealed the FCC's Privacy Rules – Now What?

March 29, 2017

By narrow and largely party-line votes, the Senate and the House of Representatives have repealed the Federal Communications Commission's privacy rules. The repeal occurred pursuant to the Congressional Review Act (CRA), a seldom used (until this year) procedure that allows Congress to overturn recently adopted agency rules. Prior to this year, the CRA had been used only once to nullify an agency's rules. The administration has already indicated President Trump will sign the disapproval legislation.

Once the president signs, the FCC's privacy and cybersecurity rules that applied to broadband providers and traditional telecommunications carriers will be wholly vitiated. Internet service providers (ISPs) nevertheless remain subject to statutory privacy provisions, as well as a variety of state privacy and breach notification requirements. FCC Chairman Ajit Pai and acting Federal Trade Commission Chair Maureen Ohlhausen have pledged to enforce privacy rules consistent with FTC guidance and to move forward on new, uniform privacy requirements equally applicable to all companies in the internet ecosystem. ISPs have announced a set of privacy and data security principles with which they agree to comply pending new rules.

Agency adoption of new privacy rules may, however, be complicated by the CRA's ban on agencies adopting substantially similar rules in the future. The scope of this ban is unclear as the term "substantially similar" is not defined in the CRA, and the courts have provided no guidance as to its meaning. It is not even clear that the courts could interpret the scope of the ban on substantially similar rules because the CRA by its terms precludes judicial review. The CRA disapproval raises questions regarding the latitude the FCC has to adopt new privacy rules in the future.

These actions have no effect on other companies in the internet ecosystem that are not ISPs, *i.e.*, so-called edge or content providers. Those entities were not covered by the FCC's privacy rules.

Background

The [FCC's privacy rules](#), adopted in late 2016, have been highly controversial. The rules were adopted in the wake of the FCC's earlier determination, as part of its Net Neutrality Order, that broadband internet access service is a telecommunications service and internet service providers (ISPs) are common carriers. That ruling carried two significant consequences. First, it removed FTC jurisdiction over ISPs. The FTC is statutorily barred from overseeing common carriers. Second, ISPs became subject to the Communications Act's Section 222 privacy rules for telecommunications carriers. Recognizing that the FCC's previous interpretations of Section 222 (dating back to 1996) were focused on traditional telecommunications services, the FCC declared it would forbear from applying those rules to broadband services, and devised new rules for ISPs governing privacy as well as cybersecurity.

A key objection to the FCC's ISP privacy rules is that they impose stricter requirements on ISPs than the FTC applies to other internet companies. For example, unlike the FTC's practice, the FCC's rules defined sensitive information requiring opt-in consent to include web browsing and app usage history. Numerous parties, including ISPs, digital advertisers, the Consumer Technology Association and app developers, opposed the rules and many filed petitions to reconsider and/or stay the FCC's rules. The privacy rules actually have not gone into effect, in part because the FCC has [stayed certain of the rules](#) relating to cybersecurity and in

part because other aspects of the rules were not slated to go into effect until later this year.

Privacy requirements after CRA disapproval

Nullification of the FCC's ISP privacy rules do not leave ISPs privacy and cyber security practices wholly unregulated. As long as they are deemed common carriers, ISPs remain subject to the privacy provisions of Section 222 of the Communications Act, but without the gloss of any FCC interpretations of those requirements. The FCC has stated its intent to enforce some baseline of privacy and cybersecurity rules and noted as well the continued applicability of state privacy and breach notification rules.

Concurrent with the earlier stay of a portion of the FCC's rules relating to cybersecurity rules noted above, the FCC recently [issued a statement](#) regarding privacy obligations pending future action:

ISPs have been – and will continue to be – obligated to comply with Section 222 of the Communications Act and other applicable federal and state privacy, data security, and breach notification laws. In addition, broadband providers have released a voluntary set of "ISP Privacy Principles" that are consistent with the Federal Trade Commission's long-standing privacy framework. (Described in the next paragraph.) For other telecommunications carriers, the Commission's preexisting rules governing data security will remain in place.

As noted in the FCC's statement, ISPs have committed to a set of privacy principles set forth in [FCC filings](#). These principles are intended to be consistent with FTC guidance and include the following voluntary commitments:

- transparency and customer notice regarding data collection practices;
- customer opt-in consent for sensitive information as defined by FTC practice (e.g., children's information, financial and health information, social security numbers and certain geolocation information); opt-out consent for non-sensitive customer information for personalized third-party marketing (presumably including general web browsing and app history that the FCC's privacy rules had deemed sensitive and requiring opt-in consent); and implied consent to use customer information in activities like service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with law, and first-party marketing;
- reasonable data security measures consistent with FTC guidance; and
- compliance with breach notification as required by applicable state laws.

Proponents of the now-repealed FCC rules argue that voluntary commitments are insufficient to curb potentially economically advantageous data use. Internet service providers must, however, be sensitive to consumers' privacy concerns and will continue to seek to avoid the repercussions of data breaches, including potentially costly litigation. Moreover, other participants in the internet ecosystem, such as digital advertisers, have developed their own set of privacy guidelines governing customer rights.

What's next

It is unclear whether or when Chairman Pai will seek to adopt a revised set of ISP privacy rules. Future FCC action is, to some extent, clouded by efforts to reverse the FCC's finding that ISPs are common carriers. Should that occur, jurisdiction over ISP privacy and security practices would revert to the FTC. FTC jurisdiction is itself clouded by the Ninth Circuit's opinion in the [FTC v. AT&T Mobility case](#), in which the court concluded that the FTC lacks jurisdiction over at least some of a company's non-common carrier activities if the company is a common carrier in other activities. Moreover, as noted above, the CRA's ban on adopting "substantially similar" rules may also hamstring future FCC actions.

Nevertheless, Chairman Pai has indicated his interest in adopting a new set of privacy rules that are consistent with FTC guidance and that would create uniform standards across the internet ecosystem. In this regard, Chairman Pai and acting FTC Commissioner Ohlhausen [issued a joint statement](#) on March 1st promising to "work together to establish a technology-neutral

privacy framework for the online world." They stated this framework would follow FTC practices and create a uniform and consistent set of privacy rules applicable to entities in the internet ecosystem. It is also possible that Congress could reintroduce legislation in this space, creating the impetus for a new rulemaking. The prospects and timing for any legislative action are uncertain.

As is clear from the Congressional debate on the CRA, the issue of ISP privacy has become highly politicized, with sharp rhetoric on both sides. This may create some pressure on the FCC to adopt a revised set of rules. Cooley's FCC and privacy lawyers will continue to monitor developments and stand ready to provide further information or guidance.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Robert M. McDowell Washington, DC	rmcdowell@cooley.com +1 202 842 7862
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.