Published on *The National Law Review* https://natlawreview.com

FCC Issues New Privacy Rules for Internet Service Providers: Safeguarding Consumers or Lulling Them Into False Sense of Privacy?

Article By:

Laura E. Jehl

Jonathan E. Meyer

J. Aaron George

Carrie Ross

Megan R. Grant

Last Thursday, in a vote split along party lines, the ***Federal Communications Commission ("FCC")*** approved a new regulatory regime staking its claim to privacy regulation of both fixed and mobile *Internet service providers ("ISPs")* like ***Comcast, Verizon,*** and ***AT&T***. The FCC's rules follow its decision in the Open Internet Order, to classify broadband Internet access service as a common-carrier telecommunications service. The FCC's new rules are intended to give consumers control over the ways in which ISPs use and share their customers' private information. While the FCC has yet to release its Report and Order, the FCC's Fact Sheet and statements by the commissioners indicate that the new privacy rules in many respects track the proposed rules the FCC put forward earlier this year, which seek to make the FCC the "toughest" privacy regulator in the Internet ecosystem by imposing on ISPs significantly more onerous and restrictive requirements for use and collection of consumer data than the Federal Trade Commission ("FTC") imposes on its non-ISP competitors.

As we have discussed in previous blog posts covering issues related to privacy, cybersecurity, and enforcement, the FCC's new rules reflect ongoing efforts by federal agencies to assert jurisdiction over privacy regulation of the Internet ecosystem, sometimes in parallel but often at odds with one another. These compound and conflicting regulations result in heightened risk, compliance costs, and uncertainty, in addition to potential competitive imbalances for industry. They also result in confusion for consumers about what information concerning themselves and their online habits is and is not protected, and by whom.

Historically, the FTC has been the country's leading privacy regulator of the Internet ecosystem. The FTC relies on its broad jurisdictional mandate to regulate "unfair and deceptive trade practices" to

enforce a privacy regime applicable to websites, applications, web browsers, search engines, social networks, and other "edge providers" that collect consumer data like ***Google*** and ***Netflix***. And, while the FTC's jurisdiction likely does not extend to common-carrier ISPs who collect consumer data, it regulates others in the Internet ecosystem who compete directly with ISPs in the online advertising market.

The FCC's new rules share characteristics with the FTC's long-standing regulation in this space, including requiring fixed ISPs and mobile data carriers that offer broadband services to obtain affirmative "opt-in" consent from consumers prior to using, sharing, or selling sensitive information. The FCC's definition of "sensitive information," however, is far more expansive than the FTC's definition and includes geo-location information, web browsing and app usage history, in addition to the health and financial information considered sensitive by the FTC. Consumers will have the option to "opt-out" and prevent ISPs from using and sharing "non-sensitive" individually identifiable customer information as well. The rules also require ISPs to provide customers with information about their collection, use, and sharing of consumer data and to comply with additional protocols to protect consumer information. Finally, the rules require that ISPs adhere to new notification protocols in the event of a data breach that includes consumer information, providing notice to affected customers no later than 30 days after reasonable determination of a breach, and notice to the FCC, Federal Bureau of Investigation, and U.S. Secret Service within 7 days if the breach affects more than 5,000 customers, a much shorter timeline than any other federal or state data breach notification requirement.

Reactions to the FCC's announcement varied. Senate Judiciary Committee Ranking Member Patrick Leahy (D-VT) praised the decision in a public statement, as did Senator Ed Markey (D-MA), while Senator Steve Daines (R-MT) criticized it as "out of touch and out of date." Similarly, the Center for Digital Democracy and Public Knowledge praised the decision, while the NCTA, American Cable Association, Direct Marketing Association and the Association of National Advertisers, among others, criticized it.

The FCC's heightened privacy regulatory regime for ISPs likely will require significant changes (at significant cost) to many ISPs' handling, storage, and use of customer information, as well as their marketing practices, privacy policies, data protection standards, systems and protocols and breach-notification requirements. But that regime may fall short of meeting the FCC's lofty promise that consumers will enjoy the "meaningful choice" that "they deserve," and may even harm the consumers the FCC intends to protect.

First, the rules reach ISPs only, who only represent a subset of the players in the Internet ecosystem who have access to consumer data and compete in the multi-billion dollar market for that information. And the rules subject ISPs to vastly more stringent regulation than their non-ISP (or "edge") competitors, even though edge providers collect and use significantly more consumer information than do ISPs. The "meaningful choice" the FCC seeks to empower thus stops at the Internet connection. As soon as consumers use the connections provided by their ISPs to access non-ISP browsers, websites, apps, search engines, social networks, video streaming sites—virtually the entire Internet—the FCC's protections fall away (at least with respect to the sites consumers access). As Commissioner Ajit Pai observed in his statement dissenting from the FCC's order, "those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulation than those who have less insight (ISPs)." Nothing in the new rules will stop edge providers from using consumer data not deemed "sensitive" by the FTC to profit from targeted advertising and the ability to provide consumers supplemental benefits or products. The FCC's new framework requires "opt in" consent before ISPs could use and profit from the same kinds of

information, which consumers understandably are loathe to provide in an era of seemingly endless email hacks and data breaches. As a result, ISPs will either (a) be locked out of this market for consumer data, or (b) be forced to offer financial incentives to their customers to obtain their opt-in consent. Either way, this approach gives edge providers an unfair competitive advantage, arguably without creating any concrete consumer benefits.

Second, Chairman Wheeler's assertion that the new rules represent a "significant step to safeguard consumer privacy in this time of rapid technological change" may mislead consumers into believing their data is secure when it is not. The Fact Sheet does not explain to consumers that, while ISPs will no longer be permitted to monitor their customers' web browsing history without consent, that same browsing history will continue to be mined, used and sold by search engine providers, social media websites and other Internet destinations. Even when a consumer opts out of sharing sensitive information with his or her ISP, that consumer will still receive targeted advertising derived from Internet use data collected by non-ISP edge providers. Thus, while the FCC's strict regulation of ISP data collection and use practices may be well-intended, the narrow limits of FCC jurisdiction mean that the Commission simply cannot deliver on its promises of heightened consumer privacy across the Internet ecosystem. It remains to be seen whether the FCC's final Report and Order will clearly and transparently signal the limits of the protections it seeks to offer. If not, the rules risk lulling consumers into a false sense of privacy, or creating confusion about who is accessing their information and for what purposes, undermining the consumer protections the rules promise.

It is possible that the FCC is betting that the FTC will follow suit and impose a similar regime on the edge providers it regulates. However, such a bet seems ill-considered and speculative at best, as such a shift by the FTC appears highly unlikely any time soon.

As a result, when the new FCC rules take effect, very little will change for American consumers. Their online behavior will continue to be tracked, harvested and monetized by companies of all kinds . . . except ISPs. The FCC's new rules simply mean that the same consumer information will be subject to different standards depending upon which agency regulates the company collecting it.

National Law Review, Volume VI, Number 307