

FCC Votes to Impose Aggressive New Privacy Rules on Broadband Providers

October 27, 2016



At the Federal Communications Commission's ("FCC") Open Meeting on October 27, the Commission voted along party lines (3-2) to impose more stringent rules on broadband Internet service providers ("ISPs"). Chairman Tom Wheeler, along with Commissioners Rosenworcel and Clyburn voted in favor of the item, while Commissioners Pai and O'Rielly voted against it.

The new rules clarify the privacy requirements applicable to broadband ISPs pursuant to Section 222 of the Communications Act. The new rules also apply to voice services and treat call-detail records as "sensitive" in the context of voice services.

According to an FCC press release issued immediately after the meeting, these rules "establish a framework of customer consent required for ISPs to use and share their customers' personal information that is calibrated to the sensitivity of the information." The Commission further asserts that this approach is consistent with the existing privacy framework of the Federal Trade Commission ("FTC").

The actual text of the order is not yet available, but a [fact sheet](#) and [press release](#) outline the core components of the order. Under the order, mobile and fixed broadband ISPs will apparently be subject to the following requirements:

- **Opt-in:** ISPs must obtain affirmative consent from consumers to use and share "sensitive" information. Under the new rules, the following categories of information are included as sensitive: precise geo-location information, financial information, health information, children's information, Social Security numbers, web browsing history, app usage history, and the contents of communications.
- **Opt-out:** ISPs can use and share "non-sensitive" information unless a customer "opts out." All other individually identifiable customer information is considered "non-sensitive," and may be used by ISPs consistent with consumer expectations.

- **Exceptions to Consent:** Customer consent can be inferred for certain purposes specified in the statute, such as provision of broadband service, billing and collection, and marketing of services and equipment that are ancillary to broadband service. In such cases, no further consent is required beyond creation of the customer-ISP relationship.
- **Notice & Transparency:** ISPs must notify customers about the types of information collected, the uses that could be made of such information, and with whom such information may be shared. Although ISPs must provide such information to customers from the outset, it is a continuing obligation – ISPs must update their customers of material changes to their privacy policies and make such information persistently available on their website or mobile app. Moreover, in response to contemporary “pay for privacy” controversies, the Commission will impose heightened disclosure requirements where ISPs offer discounts in exchange for greater rights to use customer information. Finally, the Commission has directed its Consumer Advisory Committee to develop a privacy notification standard that will afford a safe harbor to adopting providers.

The rules also address other issues, including the following:

- *Data Protection:* The new rules impose requirement that ISPs utilize reasonable data security measures. To fulfill said requirement, ISPs may: a) adopt current industry best practices; b) provide accountability and oversight for security practices; c) use robust customer authentication tools; and d) conduct data disposal consistent with FTC best practices and the Consumer Privacy Bill of Rights.
- *Breach Response:* ISPs must notify affected customers of breaches within 30 days of the determination of a breach. They must notify the Commission, FBI, and Secret Service within 7 business days if a breach affects 5,000 or more customers. If a breach affects fewer than 5,000 customers, the ISPs must contemporaneously notify the Commission and affected customers (within 30 days).

The Rationale: Consumer Rights and Technological Change

In the fact sheet, the Commission states that ISPs serve as “a consumer’s ‘on-ramp’ to the Internet,” observing that “[p]roviders have the ability to see a tremendous amount of their customers’ personal information that passes over that Internet connection” and asserting that consumers should have the right to decide how such information is used and shared.

The Commission intends for the rules “to evolve with changing technologies and encourage innovation.”

De-identified Information:

ISPs may utilize de-identified information without consumer consent. De-identified information consists of data sets that have been modified so that they can no longer be traced to individual users or devices. However, in recognition of the fact that ISPs might otherwise have the ability and incentive to re-identify customer information, the order adopts a three-part test which the FTC created in 2012 to determine whether de-identified information may be shared without consumer consent.

Pursuant to this framework, in order for an ISP to rely on de-identification without notice and consent, it must:

1. Alter customer information so that it cannot reasonably be linked to a specific individual or device.
2. Publicly commit to (a) maintain and use the data in an unidentifiable format and (b) make no efforts to re-identify the information.
3. Contractually prohibit re-identification of shared information.

Consumer Empowerment Efforts: Ending Contracts of Adhesion and Enabling Dispute Resolution:

The Commission appears to be concerned with the bargaining power differential between customers and providers. In an effort to give consumers greater leverage, the order bans ISPs from “take-it-or-leave-it” offers and forces them to serve customers who do not consent to the commercial use or dissemination of their information.

The order also purportedly addresses a recent controversy over mandatory arbitration clauses in ISP-consumer contracts by reiterating the right of consumers to utilize the Commission’s informal dispute resolution process, and signals the Commission’s intent to more directly address the matter in a rulemaking in February 2017.

* * *

The Broadband Privacy Order is an important and controversial decision. Commissioner Clyburn claimed the rules amount to “strong privacy protections.” Commissioner Rosenworcel praised the benefits of the rules for consumer protection, but openly acknowledged that “with respect to the future of privacy, I think we still have work to do” and saw the need for further harmonization efforts vis-a-vis the FTC.

Commissioners Pai and O’Rielly both voiced strong dissents. Commissioner Pai emphasized that these rules were out of sync with FTC standards, warned that “[n]othing in these rules will stop edge providers from harvesting and monetizing your data,” and expressed concern that the order sets forth “one-sided rules that will cement edge providers’ dominance in the online advertising market.”

Commissioner O’Rielly expressed frustration with the order’s new opt-in requirements, stating that the use of an “opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism even when substantial benefits are at stake.”

FTC Chairwoman Edith Ramirez released a statement praising the order:

“I am pleased that the Federal Communications Commission has adopted rules that will protect the privacy of millions of broadband users. The rules will provide robust privacy protections, including protecting sensitive information such as consumers’ social security numbers, precise geolocation data, and content of communications, and requiring reasonable data security practices. We look forward to continuing to work with the FCC to protect the privacy of American consumers.”

Although the full order has yet to be released, at a press conference following the meeting, Chairman Wheeler indicated there was a relatively strong chance it will be released at some point in the next 24 to 48 hours.

Details aside, it is clear that today’s decision (if upheld) will change the communications and privacy landscape. We will post updates here as we learn more about the new Broadband Privacy rules.

Finally, Kelley Drye will soon offer a free webinar that will unpack the new order. Once the full order becomes available, we will announce the date and time of the webinar.