Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 34, ISSUE 12 / NOVEMBER 18, 2016

EXPERT ANALYSIS

The FCC 'Opts-In' to Consumer Privacy With New Rules for Internet Service Providers

By Julie O'Neill, Esq., and Mary Race, Esq.
Morrison & Foerster

We may not think much about this when we log onto our computers to surf the web, but broadband Internet Service Providers (ISPs) collect a lot of consumer data, from the location of our devices to our web browsing habits. The Federal Communications Commission (FCC), on the other hand, has thought about this, and, on October 27, 2016, it adopted rules requiring ISPs to, among other things, give consumers more control over the use of their web browsing and other information.

Perhaps most notably, the rules will require ISPs to obtain opt-in consent to use customers' web browsing history or app usage, such as for targeted advertising purposes. Because the rules do not apply to social media platforms, websites, or apps (which are outside of the FCC's jurisdiction), ISPs have protested that the rules will place them at a competitive disadvantage.

The new rules, which will take effect in stages over the next two years, will require significant changes to how ISPs interact with their customers. The new rules contain the following key obligations:

- Notice: ISPs must give consumers clear notice about the collection, use, and sharing of their information. Notice must be both "immediate and persistent," meaning that it must be provided immediately when a customer signs up for a service, and it must be persistently available on the ISP's website or mobile app.

- Opt-In Consent: ISPs must obtain opt-in consent from their customers to use and share personal information that the rules categorize as "sensitive," including precise geo-location, health information, children's information, financial information, social security numbers, web browsing history, app usage history, and the content of communications.

- Opt-Out Consent: An ISP's use and sharing of non-sensitive personal information, such as email addresses and service tier information, will generally be subject to customers' opt-out consent. Consent will not be required in some cases, such as when information is used to provide the broadband service.

- De-identified Information: ISPs may use and share de-identified information without obtaining consent, provided that they (1) take specific steps to ensure the information cannot be reasonably linked a specific individual or device, (2) publicly commit to not attempt to re-identify the information, and (3) contractually prohibit the re-identification of shared information.

- Data Security: ISPs must develop and implement reasonable security practices to protect customer data.

- "Take-It-Or-Leave-It" Offers: ISPs cannot refuse to serve customers who don't consent to the use and sharing of their information for commercial purposes.

- "Pay for Privacy": If it chooses to offer a discount or other incentive in exchange for customer consent, an ISP must comply with heightened disclosure requirements. The FCC will evaluate the legitimacy of such "pay for privacy" programs on a case-by-case basis.

- Data Breach Notification: ISPs must notify customers (and, in certain cases, regulators) within 30 days of determining that an unauthorized disclosure of customer personal information has occurred, where such disclosure is reasonably likely to cause harm.

The final FCC order, once issued, will provide more information on the above requirements. It may also provoke a challenge by ISPs, who have never been subject to such consumer privacy rules in the past.

In addition, we might see consumer privacy advocates put pressure on entities that are not subject to the FCC's jurisdiction but that engage in the type of information collection practices targeted by the rules to also comply with them. While we do not expect that such entities would voluntarily do so, it is conceivable that the FCC's order will lead other federal or state regulators or legislators to seek to impose similar obligations on the same information practices of such other entities.

Julie O'Neill (L) is of counsel at **Morrison & Foerster** in Washington, where she provides clients with practical solutions to compliance challenges involving a wide variety of both online and offline privacy issues, including online and offline tracking, interest-based advertising, geo-targeting and other mobile tracking, personalization, and cross-device tracking. She can be reached at joneill@mofo.com. **Mary Race** (R) is an associate in the firm's privacy and data security group in Palo Alto, California. Her practice focuses on managing privacy and data security risks and helping clients develop comprehensive privacy programs that comply with U.S. and international laws. She can be reached at mrace@mofo.com. This expert analysis was first published Nov. 3 as a Morrison & Foerster Client Alert. Republished with permission.