Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What FCC's Transparency Rule Means For Internet Privacy

Law360, New York (April 21, 2015, 3:15 PM ET) --

Stephen Ruckman

There has been extensive coverage of the Federal Communication Commission's new Open Internet Order, including questions about its ultimate fate, given pending court challenges. One element of the order that has not gotten attention, though, is the only element to have withstood the prior order's court challenge: the "transparency rule."

The transparency rule is intended to ensure that broadband Internet service providers provide consumers access to the information they need to make informed choices about the broadband Internet services they purchase. The newly adopted Open Internet Order has not only retained but enhanced the transparency rule, suggesting that it will be a key FCC tool for protecting consumers in their use of the Internet, and recent FCC enforcement activity suggests one significant use of this tool will be to protect consumers' privacy.

Getting Clear on the Transparency Rule

So what exactly does the transparency rule require? The transparency rule mandates that U.S. providers of fixed and mobile broadband Internet services "publicly disclose accurate information regarding the network management practices, performance, and commercial terms of [their] broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings."

The touchstone of the rule is accuracy. In order for consumers to make an informed purchase, the information critical to that decision must be accurate. Therefore, ISPs are prohibited from making claims about their service that are inaccurate, inconsistent with disclosures, or deceptive or misleading. And the disclosures themselves must meet enhanced requirements under the new Open Internet Order, to both their content and their means.

Violators of the rule are subject to commission enforcement, including monetary penalties that range from $16,000 to $1,575,000 for any single act or failure to act, depending on the nature of the violation and the entity involved. Those are some potentially hefty penalties, and the commission declared in its new Open Internet Order that it would not be shy in levying them where needed.

How the Transparency Rule Impacts Internet Privacy

On its surface, the transparency rule does not appear to be about consumers' online privacy, but the commission has made clear that "commercial terms" under the rule include privacy policies, and stressed in the new order that commercial terms must, at a minimum, be prominently displayed on a publicly available website, with disclosure of relevant information occurring at the point of sale. This means that ISPs need to be considering transparency about consumer privacy as a critical component of their compliance with the rule.

Compliance on privacy extends beyond privacy policies, too. In a recent FCC enforcement advisory, the commission reminded ISPs that, because a "core purpose" of the rule is to "allow consumers to understand what they are purchasing," a provider's advertising regarding how it treats its customers must match what actually occurs. The advisory states: "[T]he Transparency Rule can achieve its purpose of sufficiently informing consumers only if advertisements and other public statements that ... providers make about their services are accurate and consistent with any official disclosures that providers post on their websites or make available in stores or over the phone." It goes on to mention mailings, ads on the sides of buses and in retail stores, and website banner ads as examples. The commission is essentially saying that accuracy about privacy in all of these consumer-facing communications is important to enable consumers to make sufficiently informed choices about the broadband services they purchase.

Indeed, consumers are saying the same thing. A recent survey by TRUSTe found that 45 percent of U.S. Internet users think online privacy is even more important than national security, and that 91 percent of users would avoid companies that do not protect their Internet privacy. According to those surveyed, the key to reducing these concerns is more transparency from companies about privacy. In an era of frequent, often high-profile data breaches involving sensitive consumer information, it is reasonable that consumers are making privacy — and companies' handling of privacy — a major consideration in their choice of Internet services.

Transparency Rule as One Piece of a Larger FCC Privacy Enforcement Strategy

The high value consumers place on privacy has not gone unnoticed by the FCC, which has recently been taking more action to protect consumer privacy and data security. Just a few weeks ago, the FCC entered into a $25 million consent decree with AT&T Inc. for failing to properly protect the privacy of the personal information of up to 280,000 of its customers, the largest privacy and data security action in the commission's history. And this past fall, the FCC proposed a $10 million fine against two other phone companies for allegedly collecting personal information about customers — including drivers' license numbers and even Social Security numbers — and then storing them on servers accessible to anyone able to do a Google search. The commission alleges that up to 305,000 consumers were exposed to identity theft and fraud involving their personal information due to these "lax data security practices."

While these actions were not brought under the Open Internet Order's transparency rule, they provide a strong indication that the FCC will not hesitate to use all legal tools available to protect Internet privacy. The second action is of particular interest because it includes allegations that the phone companies violated the Communications Act by "representing in their privacy policies that they protected customers' personal information, when in fact they did not." Thus part of what triggered FCC enforcement in that case was inconsistency between disclosures about privacy and actual practices. The message from these enforcement actions is plain: Privacy and data security are on the FCC's enforcement radar.

Broadband Providers Beware: Transparency Means Being Clear About How You Handle Consumer's Personal Data

So what does this mean for ISPs? It means they should take a hard look at how the language in their privacy policies and data use policies squares with the ways they communicate to consumers about their services. Now that the transparency rule has been reaffirmed — and indeed strengthened — the FCC will surely use this tool to take on what it sees as inadequacies in privacy and data security disclosures, so providers of broadband Internet access services should beware: Not only must they pay special attention to consumer-facing disclosures about privacy and data security to ensure those reflect actual practices, but they must ensure that the information in those disclosures is consistent with public advertisements and other public statements concerning the service made in marketing campaigns.

Whether they are publishing a full-page ad, Facebook post or tweet, ISPs must be cognizant that what they advertise or air on social media about how they treat consumers' information shapes consumer expectations, and those expectations should be matched by actual business practices. Providers can avoid a transparency rule violation, and the hefty forfeitures, by regularly reviewing their privacy and data security disclosures and all corresponding public advertisements to ensure that they are consistent and accurately reflect the current protections offered.

—By Stephen M. Ruckman and Anoush Garakani, BuckleySandler LLP

Stephen Ruckman is an associate in BuckleySandler's Washington, D.C., office and a former senior policy adviser at the Federal Communications Commission's Enforcement Bureau. Before joining the FCC, Ruckman was the first director of the Maryland Attorney General's Office's Internet Privacy Unit.

Anoush Garakani is an associate in the firm's Washington office.