Bloomberg BNA

Telecommunications Law Resource Center

VOL. 2015, NO. 31 JUNE 15, 2015

ISP PRIVACY PRACTICES

The authors discuss the precarious position of Internet service providers required, during the interim period between the effective date of the Open Internet rules and the enactment of regulations implementing the privacy protection requirements of Section 222 of the Communications Act, to take ''reasonable, good faith steps'' to comply with the law, but to do so without concrete guidance from the agency.

Will Broadband Providers Accept the FCC's Offer to Provide Guidance on Whether a Privacy Practice Is Reasonable?

BY MEGAN L. BROWN, SCOTT D. DELACOURT, MATTHEW J. GARDNER, KATHLEEN E. SCOTT

As a second act to its Open Internet or ''net neutrality'' order, the FCC has released a privacy Enforcement Advisory that is at least highly unorthodox, and perhaps unprecedented.

On May 20, 2015, the FCC's Enforcement Bureau (EB) issued an Enforcement Advisory pertaining to the privacy practices of Internet Service Providers (ISPs).[1] The Advisory informs broadband providers that Section 222 privacy protections will be enforced after the net neutrality rules take effect on June 12, 2015, but *before* the Commission adopts rules regarding how Section 222 applies to broadband. During this interim period, broadband providers are expected to take ''reasonable, good faith steps'' to comply with Section 222, which include employing ''effective privacy protections in line with their privacy policies and core tenets of basic privacy protections.''

The novelty of the Advisory is that the FCC has declared that it will take enforcement action while providing very little guidance about proscribed conduct or privacy practices that fall short of the articulated ''reasonableness'' standard.

An Offer of Help. Perhaps recognizing the practical difficulties for industry caught between the FCC's intent to enforce and the lack of a clear standard of conduct, the FCC extends an offer of help. If broadband providers have questions about what is reasonable, the FCC's EB states that it will provide ''informal and formal guidance.'' While no company is required to seek EB guidance with respect to a particular privacy prac-

Megan L. Brown is a partner in Wiley Rein's Telecom, Media & Technology, Cybersecurity, and Litigation practices. She can be reached at mbrown@wileyrein.com.

Scott D. Delacourt is a partner in the Telecom, Media & Technology Practice and chairs the firm's FTC Practice Group. He can be reached at sdelacourt@wileyrein.com.

Matthew J. Gardner is of counsel in the firm's Cybersecurity and White Collar Defense & Government Investigations practices. He can be reached at mgardner@wileyrein.com.

Kathleen E. Scott is an associate in the firm's Telecom, Media & Technology Practice. She can be reached at kscott@wileyrein.com.

[1] Open Internet Privacy Standard, Public Notice, Enforcement Advisory No. 2015-03 (May 20, 2015).

 ISSN

tice, requesting such guidance will ''tend to show that the broadband provider is acting in good faith.''

The FCC's promise to reward broadband companies that seek to work with the government is the third such governmental promise in recent weeks. In April 2015, the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice issued guidance for preparing and responding to data breaches.[2] As part of that guidance, CCIPS recommends that companies contact law enforcement both before and after a data breach occurs, touting numerous benefits to victim companies that work with law enforcement. In addition, also on May 20, 2015, the Federal Trade Commission publicly encouraged companies that have experienced a data breach to report it to appropriate authorities, noting that ''in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.''[3]

Is the Offer Enough? Will anyone take the FCC up on its offer? Several considerations may limit the utility and uptake of the FCC's advisory service.

First, the FCC's help will have limits. By the FCC's own terms, seeking guidance will simply ''tend to show'' that the provider is acting in good faith. Informal staff guidance will not be binding. While the FCC may be loath to bring enforcement actions for activity on which it has provided guidance, the agency has offered no safe harbor and companies have no formal protections.

Another practical constraint will be the danger that engaging the FCC will require sharing a great deal of information, possibly slowing a response. The FCC may be understandably reluctant to approve a new, innovative data use or policy without a detailed understanding of the practice. Among other things, the FCC is likely to want to understand what data is collected, how and why it is collected, how it is used, how it is protected, and what has been communicated to the customer about that collection. The agency may probe into vendor relationships, and other areas it considers relevant.

Broadband providers who are hoping for a quick answer from the FCC may be disappointed. Given the stakes, industry should expect a lengthy process, potentially involving significant disclosures to the FCC about a proposed data collection practice. Resulting ''analysis paralysis'' may make it hard for broadband providers to implement relevant and up-to-date privacy practices and also take advantage of the FCC's offer for informal guidance. And, once a question is posed to the FCC, a company will be hard-pressed to ignore advice or guidance the agency offers.

Disclosure Risk. A final issue will confront any company that considers providing information to the government: what happens to information exchanged with the FCC? More narrowly, will information provided or government guidance be subject to Freedom of Information Act (FOIA) or other public disclosure?

The FCC's Advisory does not mention the agency's rules for confidential treatment,[4] but anyone interacting with the FCC should consider those rules and FOIA Exemption 4 for trade secrets and commercial or financial information. The rules can be complicated, but in simplified form, for information to remain confidential, a submitter will have to show either that the information meets the definition of ''trade secrets,'' or is commercial or financial information that would not normally be released to the public by the provider and will cause harm if released by the agency. Whether a broadband provider would eventually be able to make and sustain that showing may not be clear at the outset of discussions, and in any event confidential treatment is never guaranteed, given the availability of judicial review of FOIA decisions. If commercial harm is a possibility, however, companies should consider including with the initial submission a request for confidential treatment, such as that contemplated under 47 C.F.R. § 0.459.

The FCC's advisory offers an option for broadband providers to address some of the regulatory uncertainty regarding permitted and prohibited practices in the data privacy area. But given the limits of the assistance the FCC is offering, the challenges FCC staff will face in green-lighting a privacy practice, and the risk that disclosures to the FCC will not be kept confidential, broadband providers will have to confront serious issues if they decide to accept the FCC's invitation.

---

[2] Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Div., U.S. Dep't of Justice, Best Practices for Victim Response and Reporting of Cyber Incidents, Version 1.0 (Apr. 2015).

[3] Mark Eichorn, *If the FTC Comes To Call*, FTC Business Blog (May 20, 2015, 10:51 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call?utm_source=govdelivery.

[4] *See e.g.*, 47 C.F.R. §§ 0.457(d), 0.459 (2015).

  ISSN