SQUIRE PATTON BOGGS

FCC Says: Sign Up for Internet Service, Don't Sign Away Your Privacy Rights

On April 1, the Federal Communications Commission, in a 3-2 vote, released a Notice of Proposed Rulemaking proposing a regulatory framework for the data security and privacy practices of Internet Service Providers, i.e., companies that provide consumers retail broadband Internet access services.

I. How Did We Get Here?

The Federal Communications Commission (FCC) started the ball rolling in its 2015 Open Internet Order by deciding that Section 222 of the Communications Act would be one of a series of Title II requirements applicable to Internet Service Providers (ISPs). Conceding that its existing rules implementing that provision were tailored to voice services, it promised the Notice of Proposed Rulemaking (NPRM) at hand.

Since then there has been a healthy debate about whether the agency has the requisite "expertise" to regulate consumer privacy in this realm, previously left to the Federal Trade Commission (FTC) – traditionally the principal policeman on the consumer privacy beat. However, the FCC's decision to reclassify ISPs as "telecommunications carriers" deprived the FTC of jurisdiction, forcing that agency (and others) to press the FCC to adopt a case-by-case approach, based on general principles of unfairness and deceptiveness, rather than a specific set of regulations.

Instead, and perhaps not surprisingly, the FCC found that the "current federal privacy regime, including the important leadership of the [FTC]…does not now comprehensively apply the principles of privacy protection to [the] 21st century telecommunications services provided by broadband networks." According to the FCC, this "gap" must be closed, particularly because "ISPs are the most important and extensive conduits of consumer information," with access to "very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence or fears."

II. Where the FCC Proposes to Go: Transparency, Choice and Security

The NPRM, which runs nearly 150 pages in its entirety, is based on three core principles: transparency, choice, and security. In addition, the item broadens the debate by asking whether FCC rules applicable to other regulatees should be harmonized with the FCC's new rules. The NPRM also proposes definitions for relevant terms, which are key to understanding the scope of the proposed regulations.

A. Transparency – ISPs would be required to provide customers with clear, conspicuous, and persistent notice about: (a) what customer information they collect and for what purposes; (b) what customer information they share and with what types of entities and (c) how, and to what extent, customers can opt in or opt out of use and sharing of their customer proprietary information.

B. Choice – The proposal would afford different "choice" mechanisms based on how the data gathered would be used or shared.

- **Inherent Choice** – Inherent in a customer's decision to purchase the ISP's services is consent for the ISP to use and share gathered data as necessary to provide the services (e.g., to "ensure that a communication destined for a particular person reaches that destination" and for "certain other purposes that make sense within the context of the" broadband providers" relationships with their customers (e.g., contacting public safety).
- **Opt-Out Choice** – Customers could affirmatively opt-out if they did not want their data used for the purposes of marketing other communications-related services or shared with affiliates that provide communications-related services for the purposes of marketing such services. Opt out "must be clearly disclosed, easily used and continuously available." As proposed, these "related services" would not include "edge services offered by the broadband provider."
- **Opt-In Choice** – Before sharing customer proprietary information with "non-communications-related affiliates or third parties or before using this information themselves (or through their communications-related affiliates)" for any other purposes, opt-in approval from the customer must be obtained.

The NPRM also asks about special situations in which greater protections might be required, including "content" of personal communications and SSN, financial account information, or geo-location information, even though these are already included within the definition of customer proprietary information.

C. Security and Breach Notification – The NPRM proposes a trigger as to when ISPs would be required to notify their customers of breaches of their proprietary information. A breach is defined as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." The NPRM would require that broadband providers notify affected customers within 10 days of discovery of a breach and seeks comment on whether, "in addition, broadband providers should notify customers after discovery of conduct that could reasonably be tied to a breach." The FCC would be required to be notified of all breaches and other federal law enforcement would be required to be notified of breaches that impact more than 5,000 customers.

D. Harmonization With Traditional Telecom/VoIP/Cable/ Satellite Rules – The NPRM asks whether the FCC "should update rules that govern application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results" of this NPRM. It also seeks comment on adopting rules that "harmonize the privacy requirements for cable and satellite providers under Sections 631 and 338(i) of the Communications Act with the rules for telecommunications providers" – an invitation that will no doubt bring more participants to the comment table.

E. Other Key Issues – Other key issues on which the FCC seeks comment include whether there are uses of customer proprietary information that should be prohibited outright, and what barriers may exist to the ability of customers to resolve disputes.

F. Key Definitions – The FCC also proposes to define key terms that will enable regulatees and consumers to better understand the scope of the rules. For example, the while the FCC sticks with the definition adopted in the Open Internet Order for ISPs, it modifies the Section 222 definition of a customer from "a person or entity to which the telecommunications carrier is currently providing service," to "a current or former, paying or non-paying subscriber-to-broadband Internet access service" and "an applicant" for such service.

In addition, the NPRM applies the protections to "proprietary information of, and relating to…customers," to include "private information that customers have an interest in protecting from public disclosure. This "customer proprietary information" or "customer PI" falls into two categories: (1) "customer proprietary network information (CPNI)" would include, for example, service plan information, including type of service, service tier (e.g., speed), pricing, capacity and geo-location; and (2) "personally identifiable information" would include information such as name, SSN, and date and place of birth.

III. What's Next?

The NPRM sets a relatively tight period for comment, with initial comments due by May 27 and replies comments due by June 27. In view of the extent of the questions to which the FCC seeks input – Commissioner Rosenworcel estimates that there are more than 500 questions in the proposal – a request for extension of time may be inevitable. However, because the comment periods were not tied to Federal Register publication and the NPRM has been expected since last fall, the FCC may stick to the tight schedule.

IV. Who Should Pay Attention and Participate?

Obviously, the proposed regulations would apply to ISPs, but because the FCC is seeking to "harmonize" the traditional telecom/VoIP/Cable/ Satellite privacy rules with whatever it adopts for ISPs, any entity providing those services could be affected as well. Given the expansive nature of the FCC's proposed rules and rule revisions, the FCC needs insight from consumer groups and businesses alike – especially those mentioned above. As the FCC explains in the NPRM, "proposals are not decisions, which is why comment from individuals, industry, interested public-interest organizations, academics, and federal and state agencies is so critical." The best way to ensure that your company's interests are protected is to file comments, reply comments, and meet with FCC staff, as these rules – when they are ultimately promulgated – could have significant regulatory compliance and business policy implications. The learning curve for privacy regulators is steep, changing with each new technology. Staying ahead of the curve for companies means working with regulators to achieve practical solutions that benefit both consumers and industry.

Contacts

Paul C. Besozzi
Partner, Washington DC
T +1 202 457 5292
E paul.besozzi@squirepb.com

Robert B. Kelly
Partner, Washington DC
T +1 202 626 6216
E robert.kelly@squirepb.com

Ann J. LaFrance
Partner, London
T +44 207 655 1752
E ann.lafrance@squirepb.com

Philip R. Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squirepb.com

Koyulyn K. Miller
Associate, Washington DC
T +1 202 457 5321
E koyulyn.miller@squirepb.com