KLEIN LAW GROUP PLLC

1250 CONNECTICUT AVE N.W.
WASHINGTON, DC 20036
202.289.6955

ALBANY, NEW YORK
518.336.4300

Firm Advisory

April 14, 2016

FCC PROPOSES NEW BROADBAND PRIVACY AND DATA SECURITY RULES

FCC issues Notice of Proposed Rulemaking to establish broadband privacy and data security rules for Internet Service Providers.

Comment Date: May 27, 2016

Reply Comment Date: June 27, 2016

Background of NPRM:

- FCC Objective: apply traditional privacy requirements of the Communications Act to "the most significant communications technology of today: broadband Internet access service (BIAS)."
- FCC Rationale for its Approach: Close the gap between privacy and 21st century technology.
    - Consumers must be able to protect their privacy. Requires transparency, choice, and data security.
    - ISPs are the most important and extensive conduits of consumer info and have access to very sensitive and very personal information.
    - Close the gap: The current federal privacy regime (FTC and Administration efforts) doesn't apply traditional principles of privacy protection to broadband networks.
- The FCC is currently seeking comment from individuals, industry, interested public-interest organizations, academics, and federal and state agencies.
- The FCC's goal is that proposed regulations ensure consumers:
    - Have the information needed to understand what data the BIAS provider is collecting and what it does with that information;
    - Can decide how their information is used; and
    - Are protected against the unauthorized disclosure of their information.

Steps the FCC is Taking:

- Include within the definition of customer proprietary information (PI) protected by Section 222(a) both CPNI as established by Section 222(h), and personally identifiable information (PII) collected by the broadband providers through their provision of BIAS[1].
- The FCC proposes rules protecting consumer privacy using the three foundations of privacy – **transparency, choice, and security**.
- **Transparency**: enhance ability of consumers to make informed choices through effective disclosure of broadband providers' privacy policies that would include:
    - What customer information they collect and for what purposes;
    - What customer information they share and with what types of entities; and
    - How, and to what extent, customers can opt in or opt out of use and sharing of their personal information.
- **Choice**: empower customers to decide extent to which broadband providers can use/share customer's PI, while providing guidance to BIAS providers about their obligations.
    - The FCC looks to the FTC 2012 Privacy Report for a framework of best practices for providing consumers with privacy choices and proposes tiered approach to choice, with three categories of approval concerning use of customer PI obtained by virtue of providing the broadband service:
        - Approval that is inherent in the creation of the customer-broadband provider relationship.
            - Allow broadband provider to use/share customer data to provide broadband services (ex: ensuring a communication destined for a particular person reaches that destination), and for other purposes that make sense within the context of the broadband providers' relationships with their customers without additional approval from the customer.
        - Opt-out approval.
            - Allow broadband providers themselves (or through affiliates that provide communications-related services) to use customer PI to market other communications-related services subject to opt-out approval of the customer.
            - Opt-out must be clearly disclosed, easily used, and continuously available.
            - Note: communications-related services would not include edge services offered by the broadband provider.
        - Opt-in approval.

[1] In the 2015 Open Internet Order, the FCC concluded that Section 222 should be applied to BIAS. *See 2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462. (*see* ¶ 13 of NPRM)

- Require broadband providers to receive opt-in approval from their customers before sharing customer information with noncommunications-related affiliates or third parties or before using customer information themselves (or through their communications-related affiliates) for any purpose outside of those described above.
    - Opt-in approval is needed to protect reasonable expectations of consumers, who may not understand their broadband provider can sell/share their information with unrelated companies for diverse purposes (ex: targeted advertising), or can repurpose customer information.

- **Data Security and Breach Notification**: The NPRM proposes:
    - Consumers should be able to rely on their broadband provider to take reasonable steps to safeguard customer information from unauthorized use, disclosure, or access.
    - To adopt a trigger as to when notice is needed, and seeks comment on under what circumstances BIAS providers should be required to notify customers of a breach of their PI.
    - To require broadband providers to notify affected customers **within 10 days** of the discovery of a breach that triggers customer notification requirements.
    - To define a "breach" as any instance in which "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."
        - This differs from 222 definition of breach in that the NPRM does not include an intent element, and covers all customer PI, not just CPNI.
    - To require that the FCC be notified of all data breaches, and that other federal law enforcement be notified of breaches that impact > 5,000 customers.
    - To require notification to federal law enforcement **within seven days** of discovery of such a breach, and **three days before notification** to the customer.
        - Exception: Law enforcement may seek delay of customer notification.
    - The FCC seeks comment on whether, in addition, BIAS providers should notify customers after discovery of conduct that could reasonably be tied to breach.
    - The FCC additionally seeks comment on whether there are other data security requirements that the Commission should adopt, such as data minimization requirements.
- The FCC is also seeking comment on the following issues:
    - Boundaries of transparency, choice, and security.
    - Content. Other federal laws (Section 705 of the Communications Act; Electronic Communications Privacy Act (including Wiretap Act provisions) already protect content carried over broadband networks. Is more protection needed?

    - Whether/how Section 222 should be applied to provide additional protection to some or all forms of content or to otherwise complement the effectiveness of existing federal laws.
  - Heightened Protection for Certain Types of Information. Whether there are particular types of information, (ex: Soc Sec numbers, location, financial account info) that, although included within the definition of customer PI, are so sensitive that they deserve special treatment.
    - Should the FCC create a separate category of highly sensitive information? How would such a regime be administered in practice?
  - Should the FCC update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding?
  - Adoption of 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.
  - Are any uses of data collected by virtue of providing the broadband service that should be prohibited altogether or otherwise subject to particular requirements? (Ex: practice of conditioning price discounts on a consumer's willingness to waive certain privacy interests.)
  - What barriers may exist to the ability of consumers to resolve disputes?
    - Right to access and correct the customer information their broadband provider maintains about them.
  - Proposed frameworks for protecting the privacy of broadband customers
  - Use of multi-stakeholder processes to further the privacy principles in the NPRM.
  - The FCC's legal authority to adopt these proposed rules.
    - NPRM relies on Section 222.
    - Are there are additional sources of statutory authority for any of the issues identified as a proposal or for which comment is sought?
    - The FCC notes that Section 705 of the Communications Act provides protection for the content of communications.

Preemption:

- The FCC proposes to preempt state laws only to the extent that they are inconsistent with any rules adopted by the Commission.
  - The FCC sees this as consistent with its approach to the current Section 222 rules.
- While the states are "very active participants" in ensuring their citizens have privacy and data security protections, the FCC is tasked with implementing Section 222.

- The FCC has previously found that they "may preempt state regulation of intrastate telecommunications matters 'where such regulation would negate the Commission's exercise of its lawful authority because regulation of the interstate aspects of the matter cannot be severed from regulation of the intrastate aspects.'" (See *2002 CPNI Order*, 17 FCC Rcd at 14890, para. 69 (quoting *1998 CPNI Order*, 13 FCC Rcd at 8075-76, para. 16).
- The FCC has interpreted this limited exercise of its preemption authority to allow states to craft laws regarding the collection, use, disclosure, and security of customer data that are more restrictive than those adopted by the Commission, provided that regulated entities are able to comply with both federal and state laws.

- The FCC considers its proposal to be consistent with both prior CPNI Orders, and its goal of allowing states to craft their own laws related to the use of personal information, including CPNI.
- Citing previous CPNI orders, the FCC proposes to preempt inconsistent state laws on a case-by-case basis, without the presumption that more restrictive state requirements are inconsistent with FCC rules.
- The FCC is currently seeking comment on:
  - State law preemption proposal above.
  - Any alternative approaches it may take to state laws governing customer PI collected by BIAS providers and addressed by the FCC's proposed rules.
  - Whether broader application of its preemption authority is warranted, or, alternatively, whether the FCC should decline to preempt state law in this area altogether.
  - Benefits and risks presented by these competing approaches to preemption.

As we remain active in matters at the Commission, we would be pleased to provide further information or assistance in preparing comments.

ANDY KLEIN	202-289-6955	AKLEIN@KLEINLAWPLLC.COM
PHILIP MACRES	202-289-6956	PMACRES@KLEINLAWPLLC.COM
ALLEN ZORACKI	518-336-4300	AZORACKI@KLEINLAWPLLC.COM
MIKE GUSSOW	202-289-6966	MGUSSOW@KLEINLAWPLLC.COM
SUSAN GOLDHAR ORNSTEIN	202-289-6955	SGOLDHAR@KLEINLAWPLLC.COM