Advocates for Rural Broadband

Summary: Protecting the Privacy of Customers of Broadband and Other Telecommunication Services (WC Docket No. 16-106)

Adopted March 31; Released April 1, 2016
Comments Due: May 27, 2016
Reply Comments Due: June 27, 2016

I. Introduction

II. Executive Summary

- Framework for applying the traditional privacy requirements of the Communications Act to BIAS, including harmonizing privacy requirements for voice, cable and satellite providers
- Three main principles:
  - Transparency
  - Choice
  - Data Security and Breach Notification
- Should there be heightened protection for certain types of customer information?
- Theme throughout NPRM of benefits and burdens of their proposals, in particular burdens on small providers

III. Ensuring Privacy Protections for Customer of Broadband Services

A. Defining Key Terms

1. BIAS and BIAS Provider

- Mass market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up, and the functional equivalent (¶ 29)

2. Affiliate

- A person that (directly or indirectly) owns (10% interest or greater) or controls, is owned or controlled by, or is under common ownership or control with another person (¶30)

3. Customer

- Current or former, paying or non-paying subscriber to BIAS, and an applicant for BIAS (¶31)
- Are consumers hesitant to apply for BIAS or switch service providers out of concern that providers may stop protecting their privacy? (¶33)
- How should the FCC's rules reflect the possibility of multiple broadband users? (¶34)
  - Proposal is to limit notice and consent requirements to a single account holder as opposed to every individual who connects to a broadband service over that subscription (¶35)
- Should the FCC harmonize with voice, cable and satellite (re: subscriber not customer)? (¶37)

4. CPNI in Broadband Context

- Statutory definition of CPNI (¶38)
    - Should it include "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or carrier"
    - Includes any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS (¶39)
        - Includes information a provider causes to be collected and stored on CPE or other devices to allow collection or access by the carrier
        - Includes information a provider attaches to a customer's Internet traffic (if it otherwise fits in the definition of CPNI)
    - Should they provide a non-exhaustive list of CPNI in the broadband context? (¶40)
        - Service plan information, as analogous to telephony service plans (¶42)
        - Geo-location of the customer or his/her device(s) (¶43)
        - Media Access Control (MAC) addresses and other device identifiers, as analogous to the IMEI mobile device identifier in the telephony context (¶44)
            - Should they include device identifiers and other information in link layer protocol headers as CPNI?
        - Source and destination IP addresses and domain name information, as analogous to telephone numbers (¶45)
            - Should they include other information in Internet layer protocol headers to be CPNI because they may indicate the type and amount of use?
        - Traffic statistics, including short- and long-term measurements, as analogous to call detail information regarding the duration and timing of phone calls and aggregate minutes (¶47)
- What other information do BIAS providers have access to? (¶53)

5. Customer Proprietary Information

- Private information that customers have an interest in protecting from public disclosure (¶57)
    - Two categories:
        - CPNI
        - Personally Identifiable Information acquired in connection with provision of BIAS
- Should the FCC adopt a uniform definition of customer PI and harmonize with existing CPNI rules? Would a harmonized standard help reduce burdens, especially for small providers? (¶59)

6. Personally Identifiable Information

- Any information that is linked or linkable to an individual (¶60)
    - Linked or linkable if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual (¶61)
    - Should FCC provide an illustrative, non-exhaustive guidance regarding types of info that are PII?
        - Name
        - SSN
        - Date and place of birth

        - Mother's maiden name
        - Government ID number
        - Physical address
        - Email address or other addresses
        - Persistent online identifiers
        - Eponymous and non-eponymous online identities
        - Account numbers and other account information, including login information
        - Internet browsing history
        - Traffic statistics
        - Application usage data
        - Current or historical geo-location
        - Financial information
        - Shopping records
        - Medical and health information
        - Fact of a disability and related info
        - Family information
        - Race, religion, sexual identity/orientation, demographic info
        - Info identifying personally owned property
        - Telephone number (¶63-64)
            - There is no subscriber list information in the broadband context
            - Harmonize with voice rules, except where such information is published subscriber list information (¶64)
    - How to harmonize with use of interpretation of PII in cable and satellite context? (¶65)

7. Content of Customer Communications

- Is there a need to provide heightened privacy protections to content of communications beyond Section 705 and ECPA? (¶67)

8. Opt-Out and Opt-In Approval

- Opt-Out: A method for obtaining customer consent to use, disclose or permit access to the customer's PI in which a customer is deemed to have consented to the use, disclosure, or access to the customer's covered information if the customers has failed to object thereto after the customer is provided appropriate notification (¶68)
    - Eliminates in broadband context 30-day waiting period required to make voice customer opt-out approval effective
- Opt-In: A method for obtaining customer consent to use, disclose or permit access to the customer's PI that requires that the BIAS provider obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the covered information after the customer is provided appropriate notification (¶69)
- How can proposed definitions provide additional clarity for providers? (¶70)

9. Communications-Related Services and Related Terms

- Telecommunications, cable and satellite services regulated by the Commissions (much narrower than current definition) (¶71)
    - Current definition: Telecommunications services, information services typically provided by telecommunications carriers (not including retail consumer services

provided using websites (like travel reservation services)) and services related to the provision or maintenance of CPE

- Proposes to amend the current definition of "information services typically provided by telecom carriers" in its voice rules (¶73)
- What constitutes "marketing"? (¶73)

10. Aggregate Customer PI

- Collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed (¶74)
- Should this definition apply to both voice and BIAS?

11. Breach

- Any instance in which "a person, without authorization or exceeding authority, has gained access to, used, or disclosed customer PI" (¶75)
    - Does not include an intent element – ensure breach notification in case of inadvertent breaches that have potentially negative consequences for consumers (¶76)
    - Should the definition exempt "good faith acquisition" of data by an employee or agent where the information is not used improperly or further disclosed?
- How will including all CPI within the definition of "breach" affect small businesses? (¶77)

12. Other Definitions

- Should FCC adopt the current definition of CPE for broadband? (¶79)
- Are there other terms from the existing rules to revise, either to differentiate them or harmonize them with proposed broadband privacy rules? (¶80)
    - Proposes to exclude BIAS provider from definition of telecom carrier in voice CPNI rules (¶80)
    - Should FCC craft one uniform set of definitions for both voice and broadband CPNI? (¶80)

B. Providing Meaningful Notice of Privacy Policies

1. Privacy Notice Requirements

- What is provider experience with current CPNI privacy disclosures? (¶86)
- Notice must specify and describe: (¶83)
    - Types of CPI that the BIAS provider collects
    - How the BIAS provider uses, and
    - Categories of entities that will receive CPI from the BIAS providers and purposes of use by each category
        - Or should providers list specific entities? (¶85)
- Notice must:
    - Advise customers of opt-in/opt-out rights and provide access to "simple, easy-to-access method for customer to provide or withdraw consent, made persistently available at no additional cost to customers
    - Explain that denial of approval will not affect provision of any services to which the customer subscribes

    - Explain that any approval, denial or withdrawal of approval is valid until affirmatively revoked at any time (subject to compelled disclosure by law)
- Notices must be:
    - Comprehensible and not misleading
    - Clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the customer, and
    - Be completely translated into another language if any portion is translated
- Timing:
    - Must be made available at the point of sale prior to purchase (online, in person, over phone, or via other means)
    - Must be persistently available via a link on the BIAS provider's homepage, through mobile application, and any functional equivalent
- Any other information that should or should not be included, for example information re: data security practices or retention/deletion of CPI? (¶84)
- Seeks comment from voice providers on their experience with privacy disclosure when seeking approval for using or sharing CPNI? (¶86)
- What would be the cost of compliance of supplying customers with privacy practice notifications via email or as part of the customer's regular bill? (¶ 87)
- Would the administrative costs of providing annual notices outweigh benefits to consumers of receiving annual notices? (¶88)
- What are the estimated costs of compliance that this notice framework will impose on providers? (¶89)
- Should the FCC adopt a standardized approach for BIAS providers' privacy notices? (¶91)
    - Would voluntary safe harbor disclosure ease regulatory burden on providers, particularly small providers? (¶92)
    - Are more general guidelines that allow for flexibility preferable to creation of a uniform template? (¶93)
- Should the FCC require a layered privacy notice that includes plain-language in addition to more in-depth disclosure? (¶94)
- Should the FCC require BIAS providers to create a consumer-facing privacy dashboard? What are the costs and benefits, and alternatives to minimize burdens on small providers? (¶95)

2. Providing Notice of Material Changes in BIAS Providers' Privacy Policies

- Propose to require BIAS providers to notify their existing customers in advance of any material changes, and to include specific types of information within notices of material changes (¶96)
- Notice provided through: (¶96)
    - Email or another electronic means
    - On customers' bills for BIAS, and
    - Via a link on the provider's homepage, mobile application, and any functional equivalent
- Should the FCC require that notification occur within a specified timeframe in advance of the effectiveness of the change? If so, what timeframe is appropriate? (¶97)
- What will the costs/burdens be on small providers of this requirement? (¶101)

3. Mobile-Specific Considerations

- Any mobile-specific considerations to the notice requirements the FCC should consider? (¶102)

4. Harmonizing Notices for Voice, Video and Broadband Services

- Should the FCC harmonize required privacy notices for voice, video, and broadband services? (¶103)
    - If a BIAS provider also provides privacy notices to customers under the voice rules and/or cable/satellite statutory requirements, should the FCC allow that provider to combine the notices so that their customers only receive one? (¶105)

C. Customer Approval Requirements for Use and Disclosure of Customer PI

1. Types of Approval Required for Use and Disclosure of Customer PI

a) Permissible Uses and Disclosures of Customer PI for which Customer Approval is Implied or Unnecessary

- Propose to allow BIAS providers to use any CPI for purpose of providing BIAS or services necessary to, or used in, the provision of BIAS (¶113)
- Propose to permit BIAS providers to use CPI for the purpose of marketing additional BIAS offerings in the same category of service to the customer, when the customer already subscribes to that category of service from the same provider without providing the opportunity to provider opt-in or opt-out consent (¶114)
    - How should content of communications be treated for marketing purposes (¶114)
- Proposes to adopt statutory exceptions in Section 222(d) (¶115)
    - Public safety and geo-location information (¶116)
    - Permit use of CPNI for protection from cyber security threats/vulnerabilities (¶117)
        - What about use of CPI?
    - Protection from robo-calls (¶118)
    - Inside wiring installation, maintenance, and repair services (¶121)

b) Customer Approval Required for Use and Disclosure of Customer PI for Marketing Communications-Related Services

- BIAS providers must provide notice and the opportunity to opt out before they may use CPI, or share such information with an affiliate that provides communications-related services, to market communications-related services to that customer (¶122)
    - What is the impact of bundled service offerings? (¶123)
    - What is the effect of these proposals on marketing of broadband and related services, including digital advertising? (¶124)
- Is an opt-in or opt-out approval more appropriate for all BIAS (and affiliate) uses and sharing for (other than for implied consent situations)? (¶126)
    - How should FCC determine if an affiliate relationship is clear to consumers (i.e., co-branding)? (¶126)
    - Treatment of affiliates as third parties and require opt-in approval? (¶126)
    - Treatment of third parties acting as contractors and performing functions for or on behalf of BIAS providers? (¶126)

c) Customer Approval Required for Use and Disclosure of Customer PI for All Other Purposes

- BIAS providers must obtain opt-in approval before (1) using CPI for purposes other than marketing communications-related services, (2) sharing CPI with communications-related affiliates for purposes other than marketing communications-related services, and (3) sharing CPI with all other affiliates and third parties. (¶127)
- Do BIAS providers need or benefit from using CPI for purposes other than marketing communications-related services? (¶128)
- What are the burdens of the opt-in framework for disclosure to third parties? (¶131)
- What effect will the opt-in framework have on marketing the broadband ecosystem? (¶132)
- Would opt-out framework be more appropriate? (¶133)

d) Other Choice Frameworks

- Should certain types of "highly sensitive" customer information be used by BIAS providers, even for the provision of the service, or shared with their affiliates offering communications-related services, only after receiving opt-in approval? (¶136)
    - Location information of children? (¶136)
    - Treatment of content of communications? (¶137)
- Should BIAS provider obtain consent before combining data acquired from third parties with information obtained by virtue of providing BIAS? (¶138)

2. Requirements for Soliciting Customer Opt-Out and Opt-In Approval

- Propose to require BIAS providers to solicit approval—subsequent to the point of sale—the first time that a BIAS provider intends to use or disclose CPI in manner that requires approval (¶140)
    - Types of CPI, purposes, and entities with which CPI will be shared
    - Could notices upon use or disclosure contribute to "notice fatigue" over time? (¶141)
- Should BIAS providers be required to solicit "just in time" approval whenever CPI is collected or each time the broadband provider intents to use or disclose the relevant CPI? What are the practical/technical realities of this approach? (¶142)
- Should FCC permit each BIAS provider to determine the best method for soliciting customer approval or require a specific method(s)? (¶143)
- Propose to require BIAS providers to make available a clearly disclosed, easy-to-use method for customer to deny/grant approval, such as a dashboard or other user interface that the readily apparent and easy to comprehend, and be made available at no cost to the customer (¶144)
    - Link on homepage, mobile application and any functional equivalent
    - What about other means (e.g., in writing, toll-free number, or dedicated email address)? (¶145)
- Propose that approval/disapproval must remain in effect until the customer revokes/limits approval/disapproval (¶147)
    - Propose that BIAS providers must act "promptly" after consent/withdrawal
    - Should the FCC define "promptly"?
    - How long should providers have to update consent choices?
    - Should withdrawal of consent require disposal of already-collected data immediately, after a period of time, or not at all?
- Should FCC apply or adapt current voice notice requirements specific to one-time usage of CPNI to BIAS providers' one-time usage of CPI? Do they make sense as extended to all customer proprietary information? (¶148)

3. Documenting Compliance with Proposed Customer Consent Requirements

- Propose to require BIAS providers to document the status of customer's approval for the use and disclosure of CPI (¶149)
    - Maintain records on CPI disclosure to third-parties for at least one year
    - Maintain records of customer notices and approval for at least one year
    - Adequately train and supervise personnel on CPI access
    - Establish supervisory review processes, and
    - Provide prompt notice to the FCC of unauthorized uses or disclosures
- Should BIAS providers file annual compliance certifications with the FCC? (¶149)

4. Small BIAS Providers

- Are there any small-provider exemptions that could be built into the approval framework? (¶151)
    - Allow small providers who already obtained customer approval to use CPI to grandfather approvals?
    - Should this be allowed for disclosure to third parties?
    - Exempt providers that collect data from fewer than 5,000 customers a year, provided they do not share data with third parties?
- How should small provider be defined?

5. Harmonizing Customer Approval Requirements

- Should FCC harmonize existing customer approval requirements for voice with those proposed for BIAS? (¶152)
- Should FCC harmonize approval requirements for BIAS customers with subscriber information of cable/satellite providers? (¶153)

D. Use and Disclosure of Aggregate Customer PI

- Propose to allow BIAS providers to use, disclose, and permit access to aggregate CPI if the provider (1) determines that the aggregated CPIT is not reasonably linkable to a specific individual or device; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure that those contracts are not violated (¶154)
- Should FCC extend this rule to providers of voice? (¶156)
- What kinds of aggregate, non-identifiable information do or can BIAS providers use and share? (¶156)
- Should the FCC provide guidance on what is linked and linkable? (¶158)
    - NIST defines linked information as "information about or related to an individual that is logically associated with other information about the individual, and linkable information as "information about or related to an individual for which there is a possibility of logical association with other information about the individual". Should FCC use this definition?

- Should FCC require BIAS providers to retain documentation outlining methods and results of analysis showing information has been rendered not reasonably linkable? (¶159)
- How could or should a BIAS provider satisfy the requirement to make a public commitment not to re-identify aggregate CPI, for example in privacy policy? (¶160)
- What types of monitoring and remediation steps should BIAS providers be required to take to ensure that entities with which they have shared aggregate CPI are not attempting to re-identify the data? (¶162)
- Should FCC develop a list of identifiers that must be removed from data? If so, what identifiers? (¶163)
- Should the FCC adopt an "actual knowledge" standard? (¶163)
- Seeks comment on costs and benefits of each prong, and how FCC could limit burdens on small providers (¶164)
- Seeks comment on treatment of de-identified but non-collective data (¶165)
- Should, for the sake of harmonization, FCC apply these rules to all other telecommunications carriers (not just BIAS providers) and all providers regardless of technology used to provide service? (¶166)

E. Security Customer Proprietary Information

1. General Standard

- Require BIAS providers to protect security, confidentiality and integrity of all CPI that BIAS providers receive, maintain, use, disclose or permit access to from unauthorized uses or disclosures by adopting security practices calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility (¶170)
    - Should FCC define "security, confidentiality, and integrity"? (¶173)
    - How should the FCC treat contents of communication? (¶173)

2. Protecting against Unauthorized Use or Disclosure of Customer PI

- Propose to require every BIAS provider to: (¶174)
    - Establish and perform regular risk assessments and promptly address any weaknesses in the provider's data security system identified by such assessments
    - Train employees, contractors, and affiliates that handle CPI about the BIAS provider's data security procedures
    - Ensure due diligence and oversight of security requirements by designating a senior management official with responsibility for implementing and maintaining the BIAS provider's data security procedures
    - Establish and use robust customer authentication procedures to grant customers or their designees' access to CPI, and
    - Take responsibility for the use of CPI by third parties with whom they share information.
- Propose not to specify technical measures for implementing the data security requirements (¶175)
- To what extent are some or all BIAS providers already engaged in these or other data security measures? (¶177)
- What are the costs involved with each element of the proposal? Are there any costs/burdens unique to small entities? (¶177)
- Should FCC establish safe harbors or convene stakeholders to establish best practices? (¶178)

- Should FCC prescribe specific administrative, technical, and physical conditions that must be included as part of a BIAS provider's plan to secure CPI? (¶179)
    - Would this unnecessarily limit additional protective measures that a BIAS provider would otherwise implement? Would specific data security measures reduce incentive to be more innovative with security? (¶179)

a) Risk Management Assessments

- Propose to allow each BIAS provider to determine the particulars of and design its own risk management program, taking into account the probability and criticality of threats and vulnerabilities that may impact the confidentiality of CPI (¶180)
- Should FCC require technical audits such as penetration tests, given concerns about the adequacy of survey-based risk assessments? (¶181)
- Alternatively, should FCC specify the manner of risk assessment design and conduct? (¶182)
- Should FCC establish a safe harbor with specific criteria to be included in a risk assessment in order to qualify for the safe harbor? (¶182)
- How often should FCC require BIAS provider to conduct risk assessments, or should FCC leave "regular" undefined? (¶183)
- Should FCC define "promptly" as part of requirement to promptly address weaknesses? If so, what would be a reasonable amount of time? (¶184)

b) Employee Training

- Proposes to requiring training and sanctioning for violations of security measures by employees, agents, or contractors (¶185)
- Should FCC specify topics that must be included in training programs? (¶187)
- Should FCC require training to be done on an annual basis, or establish a minimum frequency? (¶187)

c) Ensuring Due Diligence and Corporate Accountability

- Many BIAS providers currently have senior officials responsible for privacy and data security. What is the burden of such a requirement? (¶189)
- Should FCC specify qualifications that a senior management official should or must have? (¶190)

d) Customer Authentication Requirements

- Seek comment on whether FCC should require providers to use, at a minimum, a multi-factor authentication before granting access to CPI or before accepting another person as designee (¶191)
- Robust Authentication:
    - Does not propose it, but seeks comment on the advantages and disadvantages of requiring multi-factor authentication (costs) (¶194)
    - Would a multi-factor authentication requirement unduly burden small providers? (¶194)
    - How would multi-factor authentication work for interactions that are off-line?
    - Should FCC rules prohibit BIAS provides from requiring their customer to provide biometric information as part of any authentication scheme? (¶195)
    - Should FCC require password protection? (¶196)

    - Concerns whether a password is a sufficient safeguard. Should FCC prescribe additional requirements, such as mandating use of secret questions or character limitations? (¶197)
    - Should FCC adopt specific authentication procedures for particular scenarios (like the telephone call authentication procedures effective today) or adopt a flexible system? (¶198)
    - Are there other authentication methods to make it less cumbersome for consumers, like working with edge providers? (¶199)
    - Should FCC harmonize existing authentication requirements with the proposed requirements for BIAS providers? (¶200)
        - Are voice requirements relevant and/or effective?
        - What about specific rules for cable and satellite providers?
    - Should FCC adopt employee and contractor authentication requirements? (¶200)
- Propose requiring BIAS providers to notify customer of account changes, and attempted account changes (¶201)
    - How can this proposal be implemented with minimal burdens to customers and BIAS providers? (¶202)
    - How can FCC ensure that notice requirement does not impose an undue burden on small providers?
    - Should BIAS providers be required to send the notification to anther form of customer contact information than what is listed as the point of contact for any multi-factor authentication mechanism? (¶202)
    - How can BIAS providers be sure they are sending the authentication notification to the correct customer and not a bad actor?
    - Will notice when someone had unsuccessfully attempted to access the customer's account or change account information result in notice fatigue? (¶203)
    - Should FCC harmonize account change notification requirements for voice and BIAS providers? For cable and satellite providers? (¶204)
- Should FCC adopt rules requiring BIAS providers to provide customers with access to all CPI in their possession, including CPNI, and a right to correct that data? (¶205)
    - Seeks comment on different forms that CPI could take when collected and retained by broadband providers (¶206)
    - Are there certain sensitive classes of CPI, such as search and browsing history or location data, that a BIAS customer should always have the ability to access?
    - How should FCC take into account competitive effects of rules applicable to broadband providers? Should FCC consider restrictions, or lack thereof, that are currently placed on edge providers in crafting rules for broadband providers? (¶206)
    - Should FCC extend right to correct personal information (available to cable and satellite subscribers) to broadband? (¶207)
    - Should FCC harmonize BIAS and voice service rules with respect to right of access to CPI? (¶208)
    - If FCC adopts rules to make CPI accessible to consumers, should FCC adopt rules requiring BIAS providers to give customers clear and conspicuous notice? (¶209)

e) Accountability for Third Party Misuse of CPI

- What are the benefits and drawbacks of holding providers accountable for the data security practices of its contractors, joint-venture partners, or any other third parties with which it contracts and shares CPI? (¶211)

- Should BIAS providers be liable for third party handling of CPI for the entire lifecycle of the data or for a more limited duration? (¶211)
- Should FCC require providers to obtain specific contractual commitments from third party recipients of CPI to ensure data protection? (¶212)
- Should FCC require mobile BIAS providers to use contractual relationship with device or OS manufacturers that manufacture devices and hardware that operate on their network? (¶213)
- What other alternatives should FCC consider regarding accountability for downstream privacy violations? (¶214)

f) Other Safeguards

- Are there other safeguards that BIAS providers should employ? (¶215)
    - Restricting access to sensitive data
    - Setting criteria for secure passwords
    - Segmenting networks
    - Requiring secure access for employees, agents and contractors
    - Keeping software patched and updated
- Should FCC require or encourage BIAS providers to use standard encryption when handling and storing personal information, or mandate that CPI be encrypted when stored? (¶216)

3. Factors for Consideration in Implementing Proposed Customer Data Security Measures

- BIAS providers should, at a minimum take into account the nature and scope of the BIAS provider's activities and the sensitivity of the underlying data (¶217-220)

4. Limiting Collection, Retention, and Disposal of Data

- Should FCC adopt rules limiting collection of sensitive customer information, or providing customer control over the collection of such information (¶222)
    - Ex ante rules? (¶223)
    - Are there particular types of customer data that providers should be prohibited from collecting? (¶224)
    - Is it possible for a BIAS provider to reasonably distinguish between types of data that it collects? (¶224)
- Should FCC require BIAS providers to set reasonable retention limits for CPI? What should those limits be? (¶225)
    - Should FCC adopt a specific timeframe or a flexible standard for data retention? (¶227)
    - Should FCC adopt different data retention limits for different categories of data? How should those categories be defined and what should retention periods be? (¶228)
    - How can FCC's rules take into account the benefits of data retention? (¶229)
- Should FCC implement specific measures for BIAS providers when disposing of CPI or should FCC establish a general data destruction requirement but allow industry to determine best practices? (¶230)
    - What types of data destruction practices do BIAS providers currently abide by?
    - What are the costs and burdens? Would the requirements be particularly burdensome for small BIAS providers? Could the BIAS provider absorb the costs of a data destruction program or would costs be passed on to consumers? (¶232)

- If FCC adopts data destruction requirements for BIAS providers, should it adopt them for voice?

F. Data Breach Notification Requirements

1. Customer Notification

- Propose to require BIAS provides and other telecommunications carriers to notify customer of breaches of CPI no later than 10 days after discovery of the breach, absent a request by federal law enforcement to delay customer notification (¶236)
- Notification trigger
  - Should FCC require reporting based on the likelihood of misuse of the data or of harm to the consumer? (¶237)
  - If FCC allows time for appropriate investigation, how much time should providers have before they need to make their determination or disclose the breach to customers? (¶238)
  - Should different triggers apply to different types of CPI?
- Should FCC adopt a more flexible standard for timing of customer notification (similar to telephone CPNI breach notification), for example as expeditiously as practicable or without unreasonable delay? (¶241)
- Should breaches of voice CPI be distinguished from breaches of broadband CPI? What would the impact be on small providers? (¶241)
- Seeks comment on whether FCC should require notice when the telecommunications carrier discovered conduct that would reasonably lead to exposure of CPI (¶242)
- Content: (¶243)
  - Date
  - Description of CPI at issue
  - Information to contact the provider to inquire about the breach
  - Information about contacting the FCC and relevant state regulatory agencies
  - Information about credit reporting agencies and steps to prevent identify theft (including any credit monitoring the telecom is offering)
  - Should content requirements vary based on the type of information breached, number of consumers affected, extent of economic harm, etc.? (¶244)
- Propose that carriers provide written notification to the customer's address of record, email address, or by contacting the customer by other electronic means using contact information the customer has provided for such purpose (¶245)
  - Service providers should be in the best position to know how to reach their customers (¶245)

2. Notification to Federal Law Enforcement and the Commission

- Propose to require telecommunications provider to notify the Commission no later than 7 days after discovering any breach of CPI, and to notify the FBI and Secret Service no later than 7 days after discovery of a breach reasonably believed to have affected at least 5,000 customers (¶246)
- Law enforcement notice must be at least three days before provider notifies its affected customers (¶246)
- Should FCC have a threshold for law enforcement notice? (¶247)
- Should other or different federal law enforcement agencies receive data breach notifications?
- Should FCC require reporting to state law enforcement? (¶247)

- Should FCC be notified of all breaches? Are there reasons that the Commission should not be notified of all breaches? (¶248)
- Should FCC require notice when the provider discovers conduct that would reasonably lead to exposure of CPI? (¶250)
- Propose to extent existing Section 222 requirements for both method and substance of data breach notification to law enforcement and the Commission (¶251)

3. Record Retention

- Propose to extend existing Section 222 record retention requirements regarding data breaches to BIAS providers (¶252)
    - Maintaining records of discovered breaches and notifications for at least two years
    - Must include the date of discovery, date law enforcement and FCC were notified, detailed description of PI breached, and circumstances around the breach
- How have telecommunications carriers found the current requirement to work? What have been the costs for compliance? (¶253)

4. Harmonization

- Should the FCC's proposed rules apply equally to all providers of telecommunications service or are there reasons that BIAS providers should have different notification requirements? (¶254)
- Should FCC harmonize rules for cable/satellite providers? (¶254)

5. Third-Party Data Breach Notification

- Should FCC require BIAS providers to contractually require third parties with whom they share CPI to follow the same breach notification rules for BIAS providers? (¶255)
- Should FCC permit BIAS providers and third parties to determine by contract which party will provide notifications required when there is a third-party breach (and effect on dual notification)? (¶255)

G. Practices Implicating Privacy that May be Prohibited Under the Act

- Are there certain BIAS provider practices implicating privacy that FCC rules should prohibit or to which FCC should apply heightened notice and choice requirements? (¶256)
- Should FCC work with stakeholders to develop privacy best practices guidelines and create a "privacy protection seal" that BIAS providers could display on their websites to indicate compliance with those guidelines? (¶257)
- How can FCC encourage privacy-by-design practices? (¶257)
- Propose to prohibit BIAS providers from making service offers contingent on a customer surrendering his or her privacy rights (¶258)
    - Are there countervailing consumer benefits associated with these types of offers?
- Are business practices that offer customers financial inducements, such as lower monthly rates, for their consent to use and share their confidential information (e.g., ATT $30 off), permitted under the Communications Act? (¶259)
    - Should FCC accept that, upon being fully informed about he privacy rights they are exchanging for a discounted broadband price, consumers can and should be allowed to enter into such bargains? (¶263)

- Should use of Deep Packet Inspection for purposes other than providing broadband services, and reasonable management thereof, be prohibited or subject to heightened approval? (¶264)
    - For what purposes do broadband providers engage in DPI? (¶266)
- Should the use of persistent tracking technologies be prohibited, or subject to opt-out or opt-in consent? (¶268)
- Should FCC understand Section 222(b) as protecting information about all of the traffic that a BIAS provider receives from another provider from being used by the receiving BIAS provider for any purpose other than the provision of telecommunications service? (¶271)
- Are there other uses or disclosures of CPI that should be prohibited or subject to heightened notice and choice requirements? (¶272)

H. Dispute Resolution

- Is the current informal complaint resolution process sufficient to address customer concerns or complaints? (¶273)
- Should FCC prohibit BIAS providers from compelling arbitration in their contracts with customer? (¶274)
- Should FCC consider other dispute resolution proposals, including how to harmonize with the existing voice CPNI framework? (¶ 275)

I. Preemption of State Law

- Propose to preempt state laws only to the extent that they are inconsistent with any rules adopted by the Commission, provided that regulated entities can comply with both federal and state laws (¶276-77)
- Propose to preempt inconsistent state laws on a case-by-case basis, without the presumption that more restrictive state requirements are inconsistent with FCC rules (¶277)
- Is broader application of preemption authority warranted, or should FCC refrain from preemption altogether? (¶277)

J. Other Proposed Frameworks and Recommendations

- Describes and seeks comment on frameworks offered by Industry, New America's Open Technology Institute, Public Knowledge, Electronic Privacy Information Center, Information Technology and Innovation Foundation, and Digital Content Next (¶278-91)

K. Multi-Stakeholder Processes

- Are there specific ways the FCC should incorporate multi-stakeholder processes into its proposed approach to protecting privacy of CPI? (¶293)

IV. Legal Authority

- Finds legal support under a range of Communications Act provisions

A. Section 222

- Authority over customer proprietary information (a) and CPNI (c)

B. Additional Statutory Authority

1. Sections 201-202

- Practices that fail to protect the confidentiality of end users' proprietary information, will be unlawful if they unreasonably interfere with or disadvantage end user consumers' ability to select, access or use broadband services, applications or content (¶305, citing 2015 Open Internet Order)

2. Section 705

- Providers of communications services have obligations not to "divulge or publish the existence, contents, substance, purport, effect, or meaning" of communications that they carry on behalf of others (¶307)

3. Section 706

- Removing barriers to broadband deployment (by increasing consumer confidence in BIAS providers' practices, thereby boosting confidence in and therefore use of broadband services, which encourages the deployment on a reasonable and timely basis) (¶309)

4. Title III

- To the extent that BIAS is provided by licensed entities providing mobile BIAS (¶310)