CENTER FOR DEMOCRACY & TECHNOLOGY

Broadband Privacy Cheat Sheet:
Everything You Need to Know About the FCC's New Privacy Rules for Broadband Providers

On October 27, 2016, the Federal Communications Commission (FCC) voted on rules to protect internet users' privacy by requiring broadband providers to get consent before using and sharing customers' data. The rules implement a statutory obligation under 47 U.S.C. § 222 for telecommunications carriers to protect the confidentiality of customer information. The Commission has adapted this mandate for broadband internet access service (BIAS) providers, which it reclassified as telecommunications carriers in the 2015 Open Internet Order. The Commission also harmonized the rules for all telecommunications carriers, including telephone service providers. This cheat sheet is designed to give policy makers, members of media, and the public an overview and understanding of the important details in the rulemaking.

I. The rule protects all broadband users.

A. Carriers must protect the information of current subscribers, former subscribers, and applicants to subscription services.

- The rule protects "customers," which the Commission defines as (1) current and former subscribers to a telecommunications service or (2) applicants for a telecommunications service. Protection under the rule "begins when a person applies for service and continues after a subscriber terminates his or her service."

- The Commission recommends that "[i]f carriers want to limit their obligations with respect to applicants and former customers, they can and should adopt data minimization practices and destroy applicants' and former customers' confidential information as soon as practicable . . ."

B. All users of a subscription service are protected.

- "Customers" include all users of a subscription service, such as members of a household and their guests who use the same subscription. However, the subscriber's privacy choices apply to all users of the subscription. In other words, all users of a single subscription are treated as one customer.

CENTER FOR DEMOCRACY & TECHNOLOGY

II. The rule covers data that broadband providers obtain by virtue of providing broadband internet service.

A. The rules do not protect information obtained in the provision of other communications services, such as edge services.

- The rule governs only information collected by virtue of the telecommunications provider-customer relationship. It does not govern information that BIAS providers obtain by virtue of providing non-telecommunications services, such as edge service like email, websites, cloud storage services, social media sites, music streaming, or video streaming. The FCC does not have authority under Section 222 to regulate the information practices of edge providers.

- For example, if Verizon collects a customer's browsing history in the course of its provision of broadband internet services, it must protect that information under Section 222. However, any browsing history it collects through its AOL services is not subject to Section 222. This means that the same piece of information may be subject to two different sets of privacy laws and policies depending on how it was collected.

B. Section 222 applies to customer proprietary information (PI), which includes (1) customer proprietary network information (CPNI), (2) personally identifiable information (PII), and (3) the content of communications.

- **CPNI** is information that relates to the quantity, technical configuration, type, destination, location, and amount of a telecommunications service subscribed to by a customer. CPNI includes:
  - broadband service plans;
  - geolocation information, which includes any information related to the location of a customer or device;
  - MAC addresses and other device identifiers;
  - IP addresses and domain name information;
  - traffic statistics;
  - port information;
  - application headers, including those attached by the provider;
  - application usage;
  - application payload, which is the part of the IP packet containing the substance of the communications between the customer and the entity with which the customer is communicating;

  - information that BIAS providers cause to be collected or stored on a customer's device, including customer premise equipment, such as wireless routers.

- **PII** is any information that is linked or reasonably linkable to an individual or device. The information may be linkable on its own, in context, or in combination with other information. This category covers traditional PII, such as names, social security numbers, and email addresses, as well as MAC and IP addresses, which are considered linkable to a device.

- The **content of communications** is broadly defined to include any information that "conveys or implies any part of [the] substance, purport, or meaning" of the communication.

  - The Commission sought to create a flexible definition that is not tied to the traditional content/metadata distinction, acknowledging that "sophisticated monitoring techniques have blurred the line between content and metadata, with metadata increasingly being used to make valuable determinations about users previously only possible with content."

  - Application payload is always content, and other portions of the packet, such as the application header, may also convey the content of communications.

III. Consent is not required for de-identified data, but the rule imposes strong de-identification requirements.

A. Providers can use and share de-identified customer data without obtaining opt-in or opt-out consent.

B. Providers bear the burden of ensuring that information is effectively de-identified, according to a three-part framework.

- The Commission adopts the Federal Trade Commission (FTC)'s three-part framework for ensuring that data is properly de-identification. Under this framework, a telecommunications carrier that wishes to use and share de-identified data outside of the consent regime must:

- Determine that the information is not be reasonably linkable to an individual or device;
    - The information must not, on its own, in context, or in combination, (1) identify an individual or device, or (2) logically associate with other information about a specific individual or device.
- Publicly commit to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and
- The provider must contractually prohibit any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data.
    - The Commission exempts from this requirement the disclosure of "highly abstract statistical information," such as the total number of subscribers to a service, which is "not possible to re-identify."

IV. Carriers must provide clear, conspicuous, and persistently available privacy policy notices.

A. Providers must present clear and conspicuous privacy notices to customers at the point of sale and maintain such notices on their websites and applications.

- The Commission requires telecommunications carriers to provide customers with privacy notices that present information in a way that is clear and conspicuous, in language that is comprehensible and not misleading.
- Privacy notices must inform customers about what confidential information providers collect, how they use it, and under what circumstances they share it.
    - Providers may disclose categories of entities with which it shares information rather than naming individual entities.
- Providers must inform customers about their rights to opt in to or out of the use or sharing of their confidential information.
- Providers must inform customers that denying a provider the ability to use or share confidential information will not affect their ability to receive service.

- Providers must present privacy notices to customers at the point of sale, prior to the purchase of service.

- Carriers must make privacy notices persistently available on the provider's website and on any apps or functional equivalents provided by the carrier.

- The Commission does not require periodic notice and the new rule eliminates the existing biannual notice requirement under Section 222. The Commission cites notice fatigue as its primary reason for eliminating this requirement.

- Although the Commission declined to prescribe any form or language requirements for privacy notices, it has directed the FCC Consumer Advisory Committee to formulate a proposed standardized notice format that would provide a voluntary safe harbor for telecommunications carriers.

B. Providers must give advance notice of material changes to privacy policies and obtain opt-in consent for material retroactive changes.

C. Providers must give customers a simple, easy-to-use mechanism for opting in to or out of the use and sharing of their information.

V. Carriers must obtain opt-in consent to use or share customers' sensitive information.

- Sensitive information includes:
  - financial information;
  - health information;
  - social security numbers;
  - precise geolocation information, which includes but is not limited to GPS-based, WiFi-based, or cell-based location information;
  - information pertaining to children;
  - the content of communications, which is defined broadly, as explained in section II.B of this document;
  - web browsing history and application usage history;
    - Web browsing history and application usage history "includes information from network traffic related to web browsing or other applications (including the application layer of such traffic), and information from network traffic indicating the website or party with

which the consumer is communicating (e.g., their domains and IP addresses)."

- the functional equivalents of web browsing and app usage history.

VI. Carriers must obtain opt-out consent for most uses of non-sensitive information.

- "Non-sensitive information" is anything that does not fall into the "sensitive category.

- Carriers must obtain opt-out consent to use and share non-sensitive information, subject to several exceptions, including information used for the provision of the telecommunications service and for certain first-party marketing.

VII. Carriers do not need additional consent to use information for purposes of providing the broadband service.

A. Provision of the telecommunications service includes a variety of necessary services.

- These include billing, detecting fraud, and protecting the network.

B. Carriers can use and share customer information for certain research purposes without additional consent.

- Research to improve or protect the network, including cybersecurity research, falls under the services necessary to the provision of the telecommunications service. Thus, telecommunications carriers can use and share customer PI for these limited research purposes.

- The Commission urges carriers to minimize the privacy risks that may stem from research by limiting disclosure of information to that which is reasonably necessary to achieve the research purpose and by ensuring that the entities to which information is disclosed will likewise safeguard customer privacy.

VIII. Carriers can use non-sensitive information to market certain communications services without additional consent.

- Telecommunications carriers can infer consent to use and share non-sensitive customer PI to market "other communications services commonly marketed with the telecommunications service to which the customer already subscribes."

- For example, carriers can use non-sensitive customer PI to market voice or video services to an existing broadband subscriber.

IX. Carriers must maintain reasonable data security standards and practices.

- Consistent with the FTC's approach to data security, the FCC requires telecommunications carriers to take reasonable measures to secure customer PI. Providers must calibrate their security measures to "the sensitivity of the underlying data." The Commission declined to prescribe specific security measures, opting for a flexible standard that accommodates the varying needs and risks of different providers as well as the evolving nature of technology and data security tools.

X. Carriers must notify affected customers and relevant agencies of data breaches.

- Data breach notification is required unless the carrier investigates and reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach.
    - Harm is broadly construed to encompass financial, physical, and emotional harm.
    - The rules establish a rebuttable presumption that any breach involving sensitive customer PI presumptively poses a reasonable likelihood of customer harm and would therefore require notification.

XI. Carriers may not condition service on customers' consent to allow the provider to use or share their data.

A. "Take-it-or-leave-it" offerings are prohibited.
    - Providers may not condition service on a customer surrendering his or her privacy rights.

B. Providers offering financial incentives in exchange for consent to use and disclose customer data must meet heightened disclosure requirements.
    - Carriers offering such incentives must provide clear and conspicuous notice of the terms of any financial incentive and must at least as prominently provide

information to customers about equivalent plans that do not require exchanging personal information.

C. The Commission reserves the right to take action against providers engaged financial incentive practices that are unjust, unreasonable, or discriminatory.

- Under Sections 201 and 222, the Commission can prohibit, on a case-by-case basis, "practices that unreasonably interfere with or unreasonably disadvantage the ability of consumers to reach the Internet content, services, and applications of their choosing."