FACT SHEET: THE FCC ADOPTS ORDER TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION

The Federal Communications Commission (FCC) adopted an Order at the October meeting that will give consumers the tools they need to choose how their Internet service providers (ISPs) use and share their personal data. Building on widely accepted privacy principles, the rules require that ISPs provide their customers with meaningful choice and keep customer data secure while giving ISPs the flexibility they need to continue to innovate. The rules do not prohibit ISPs from using or sharing their customers' information — they simply require ISPs to put their customers in the driver's seat when it comes to those decisions. The approach the Commission adopted reflects extensive public comments received in response to the comprehensive proposal adopted by the Commission in March 2016.

Whose Data Is It Anyway? Consumers Deserve Increased Choice, Transparency, and Security Online

In today's digital world, consumers deserve the ability to make informed choices about their online privacy, but there are currently no rules in place outlining how ISPs may use and share their customers' private information. ISPs serve as a consumer's "on-ramp" to the Internet. Providers have the ability to see a tremendous amount of their customers' personal information that passes over that Internet connection, including their browsing habits. Consumers deserve the right to decide how that information is used and shared — and to protect their privacy and their children's privacy online.

First Principles: Designed to Protect Consumers, Evolve with Changing Technology

The FCC's Open Internet Order reclassified broadband Internet access service as a telecommunications service. Section 222 of Title II of the Communications Act requires telecommunications carriers to protect the privacy of their customers' information. The FCC, as mandated by Congress, has successfully overseen consumer privacy with regard to the telephone network for decades, and these proposed rules would apply that expertise to the world of broadband.

The rules are designed to evolve with changing technologies and encourage innovation, and are in harmony with other key privacy frameworks and principles — including those outlined by the Federal Trade Commission and the Administration's Consumer Privacy Bill of Rights. They also reflect careful consideration of the needs of smaller ISPs. The rules give consumers greater control over their ISPs' use and sharing of their personal information, and provide them with ways to easily adjust their privacy preferences over time.

Clear Notice: ISPs Must Tell Customers about the Collection, Use, and Sharing of Their Information

Every day, consumers hand over personal information — including very sensitive information — to their ISPs simply by using their service. Consumers deserve to know how their provider handles that information. The rules require that ISPs, whether they offer mobile broadband or fixed broadband to people's homes, to:

- Notify customers about what types of information the ISP collects about its customers.
- Specify how and for what purposes the ISP uses and shares this information.
- Identify the types of entities with which the ISP shares this information.

Immediate and persistent notification

ISPs must provide this information when a customer signs up for service, and update customers when the ISP's privacy policy changes in significant ways. In addition, the information must be persistently available on the ISP's website or mobile app.

Multi-stakeholder approach
Recognizing the value of multi-stakeholder processes, the Commission directs the Consumer Advisory Committee (CAC) to develop a standardized privacy notice format that is voluntary and can serve as a 'safe-harbor' for those providers that choose to adopt it.

Increased Consumer Choice: Use of Personal Information Based on Sensitivity
The type of customer consent required for ISPs to use and share their customers' personal information is calibrated to the sensitivity of the information, in line with approaches taken by other privacy frameworks, including the FTC's and the Administration's Consumer Privacy Bill of Rights. The focus on the sensitivity of the information — rather than how it is used — is in line with customer expectations. Customers generally want more controls in place before their sensitive information is used or shared.

- **Opt-In: ISPs will be required to obtain "opt-in" consent to use and share sensitive information** ISPs will have to obtain affirmative permission from consumers — opt-in consent — to use and share sensitive information. The Order specifies categories of information that will be considered "sensitive," including:

    - **Precise geo-location** *(typically the real-world location of a mobile phone or other device)*
    - **Children's information**
    - **Health information**
    - **Financial information**
    - **Social Security numbers**
    - **Web browsing history**
    - **App usage history**
    - **The content of communication**

- **Opt-out: Use and sharing of non-sensitive information would be subject to opt-out consent requirements in most cases.** All other individually identifiable customer information — for example, service tier information — is considered non-sensitive and the use of sharing of that information will be subject to opt-out consent, consistent with customer expectations.

- **Exceptions to the Consent Requirements:** Customer consent is inferred for certain purposes, including:

    - Use and sharing of non-sensitive information to provide and market services and equipment typically marketed with the broadband service subscribed to by the customer.
    - To provide the broadband service, and bill and collect for the service.
    - To protect the broadband provider and its customers from fraudulent use of the provider's network.

Implements Strong Protections for De-identified Information
The use and sharing of de-identified information, that is, data that have been altered so they are no longer associated with individual consumers or devices, can present fewer privacy concerns than other types of consumer data. The rules allow ISPs to use and share properly de-identified information outside the consent regime required for other customer data. However, we also recognize that ISPs may have the incentive and, increasingly, the technical ability to easily re-identify customer information.

As such, if an ISP wants to rely on de-identification in its use or sharing of information outside of the new consent framework, it must meet the strong, three-part test first articulated by the FTC in 2012 to ensure consumer information is not re-identified. ISPs must:

- Alter the customer information so that it can't be reasonably linked to a specific individual or device.
- Publicly commit to maintain and use information in an unidentifiable format and to not attempt to re-identify the data.
- Contractually prohibit the re-identification of shared information.

Prohibits "Take-It-or-Leave-It" Offers

The Order prohibits "take-it-or-leave-it" offers, meaning that an ISP can't refuse to serve customers who don't consent to the use and sharing of their information for commercial purposes.

Heightens Consumer Protections for Financial Incentives

Recognizing that so-called "pay for privacy" offerings raise unique considerations, the rules require heightened disclosure for plans that provide discounts or other incentives in exchange for a customer's express affirmative consent to the use and sharing of their personal information. The Commission will determine on a case-by-case basis the legitimacy of programs that relate service price to privacy protections. Consumers should not be forced to choose between paying inflated prices and maintaining their privacy.

Strengthens Protection of Customer Information

Strong security protections are crucial to protecting consumers' data from breaches and other vulnerabilities that undermine consumer trust and can put their health, financial, and other sensitive personal information at risk. Consistent with FTC data security requirements and the NIST cyber-security framework, the rules require ISPs to take reasonable measures to protect customer data.

The rules require that an ISP's practices be appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility. Recognizing that data security is a dynamic and innovative arena, the Order does not provide a check-list of required data security activities. The Order does, however, provide guidelines about steps ISPs should consider taking to develop reasonable data security practices, such as to:

- Implement up-to-date and relevant industry best practices, including available guidance on how to manage security risks responsibly.
- Provide appropriate accountability and oversight of its security practices.
- Implement robust customer authentication tools.
- Properly dispose of data consistent with FTC best practices and the Consumer Privacy Bill of Rights.

Includes Common-Sense Data Breach Rules That Protect Consumers' Right to Know

Consumers have a right to know when their data has been compromised. In order to encourage ISPs to protect the confidentiality of customer data, and to give consumers and law enforcement notice of failures to protect such information, the rules include common-sense data breach notification requirements. The requirement is triggered by an ISP's determination that an unauthorized disclosure of a customer's personal information has occurred, unless the ISP determines that no harm is reasonably likely to occur.

Specifically, in the event of a reportable breach, providers would be required to notify:

- Affected customers of breaches of their data as soon as possible, but no later than 30 days after reasonable determination of a breach.
- The Commission, the Federal Bureau of Investigation, and the U.S. Secret Service of breaches affecting 5,000 or more customers no later than 7 business days after reasonable determination of the breach.
- The Commission at the same time as customers are first notified of breaches affecting fewer than 5,000 customers.

Harmonization of Broadband and Voice Rules

The new rules also apply to voice services and treat call-detail record information as sensitive information in the context of voice services. By harmonizing the rules that apply to broadband and voice services, the Commission is providing clear and consistent privacy and data security protections for customers of all telecommunications services.

Dispute Resolution

Today's Order reaffirms the right of broadband and voice customers to use the Commission's informal dispute resolution process. In addition, it expresses concern about the impact on consumers from the use of mandatory arbitration agreements. The Commission intends to proceed with a rulemaking in February 2017 to address mandatory arbitration requirements in contracts for communications services.

Implementation Timeline

The Order gives providers sufficient time to implement the changes required by the rules, while adopting an implementation timeline calibrated to ensure that consumers receive the benefit of the new rules as quickly as possible.

- The data security requirements will go into effect 90 days after publication of the summary of the Order in the Federal Register.
- The data breach notification requirements will become effective approximately 6 months after publication of the summary of the Order in the Federal Register.
- The Notice and Choice requirements will become effective approximately 12 months after publication of the summary of the Order in the Federal Register. Small providers will have an additional 12 months to come into compliance.

What the Rules Do NOT Do:

- Do not regulate the privacy practices of websites or apps, like Twitter or Facebook, over which the Federal Trade Commission has authority.
- Do not regulate other services of broadband providers, such as operation of a social media website.
- Do not address issues such as government surveillance, encryption or law enforcement.

###