**FACT SHEET: CHAIRMAN WHEELER'S PROPOSAL TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION**

*FCC Chairman Tom Wheeler has circulated to his fellow Commissioners a proposed Order to give consumers the tools they need to choose how their Internet service provider (ISP) uses and shares their personal data. Building on widely accepted privacy principles, the rules would 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, if adopted, would not prohibit ISPs from using or sharing their customers' information – they would simply require ISPs to put their customers in the driver's seat when it comes to those decisions.*

*The approach the Chairman is recommending reflects extensive public comments received in response to the comprehensive proposal adopted by the Commission in March, including input from the Federal Trade Commission. The full Commission will vote on the proposed Order at the FCC's October 27 Open Meeting.*

**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 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, if adopted, would 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 Notification: ISPs Must Tell Customers about the Collection, Use & Sharing of Their Information**

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

- 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 Chairman's proposal directs the Commission's Consumer Advisory Committee (CAC) to develop a proposed standardized privacy notice format that is voluntary and would serve as a 'safe-harbor' for those providers who choose to adopt it.

**Increased Consumer Choice: Personal Information Use 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 would be required to obtain "opt-in" consent to use sensitive information** ISPs would have to obtain affirmative permission from consumers — opt-in consent — to use and share sensitive information. The proposed Order specifies a category of information that would be considered "sensitive," including:

    - **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 communications**

- **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 used to market an alarm system — would be considered non-sensitive and the use of sharing of that information would be subject to opt-out, consistent with customer expectations.

- **Exceptions to the Consent Requirements:** Customer consent is inferred for certain purposes spelled out in the statute — the provision of broadband service, or billing and collection for example.

**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 proposed rules would allow ISPs to use and share properly de-identified information outside the consent regime required for other consumer data. However, we also recognize that ISPs may have the incentive and, increasingly, the technical ability to easily re-identify consumer 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-prong 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 rules, if adopted, would prohibit "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 would require heightened disclosure for plans that provide discounts or other incentives in exchange for a consumer's express affirmative consent to the use and sharing of their personal information. The Commission would 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, if adopted, will require ISPs to take reasonable measures to protect customer data.

The rules would require that an ISP's practices be appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, and the size of the provider and technical feasibility. Recognizing that data security is a dynamic and innovative arena, the Order would not provide a check-list of required data security activities. The Order would, 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 Chairman's proposal includes common-sense data breach notification requirements. The requirement would be triggered from an ISP's determination that an

unauthorized disclosure of a customer's personal information has occurred, unless the ISP establishes 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 discovery;
- The Commission of any breach of customer data no later than 7 business days after discovery; and
- The Federal Bureau of Investigation and the U.S. Secret Service of breaches affecting more than 5,000 customers no later than 7 business days after discovery of the breach.

**What the Chairman's Proposed 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.

###