Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security With Respect to Their Data

FCC Chairman Tom Wheeler has circulated for consideration by the full Commission a Notice of Proposed Rulemaking (NPRM) to ensure consumers have the tools they need to make informed choices about how and whether their data is used and shared by their broadband providers. The proposal would apply the privacy requirements of the Communications Act to the most significant communications technology of today: broadband Internet access service. When consumers sign up for Internet service, they shouldn't have to sign away their right to privacy. The proposal will be voted on by the full Commission at the March 31 Open Meeting, and, if adopted, would be followed by a period of public comment.

Do Consumers Know What They Are Agreeing To When They Sign Up For Internet Service?

Every day, consumers hand over very personal information simply by using the residential or mobile broadband services they've paid for. Why? Because by carrying Internet traffic, ISPs can collect their customers' personal and private information to create detailed profiles about their lives.

- An ISP handles all of its customers' network traffic, which means it has an unobstructed view of all of their unencrypted online activity – the websites they visit, the applications they use. If customers have a mobile device, their provider can track their physical and online activities throughout the day in real time.
- Even when data is encrypted, broadband providers can still see the websites that a customer visits, how often they visit them, and the amount of time they spend on each website. Using this information, ISPs can piece together enormous amounts of information about their customers – including private information such as a chronic medical condition or financial problems.
- A consumer's relationship with her ISP is very different than the one she has with a website or app. Consumers can move instantaneously to a different website, search engine or application. But once they sign up for broadband service, consumers can scarcely avoid the network for which they are paying a monthly fee.

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

Consumers should have effective control over how their personal information is used and shared by their broadband service providers. Telephone networks have had clear, enforceable privacy rules for decades, but broadband networks currently do not. Chairman Wheeler's proposal to protect consumer privacy is built on three core principles – choice, transparency and security

- **Choice:** Consumers have the right to exercise meaningful and informed control over what personal data their broadband provider uses and under what circumstances it shares their personal information with third parties or affiliated companies.
- **Transparency**: Consumers deserve to know what information is being collected about them, how it's being used, and under what circumstances it will be shared with other entities. Broadband providers must provide accurate disclosures of their privacy practices in an easily understandable and accessible manner.
- **Security**: Broadband providers have a responsibility to protect consumer data, both as they carry it across their networks and wherever it is stored.

Chairman Wheeler's Proposal to Empower Consumers to Protect Their Privacy: It's Your Data

To provide the tools consumers need to make smart choices about protecting their information – and enforce the broadband provider's responsibility to do so – the Chairman's proposal separates the use and sharing of information into three categories, and proposes adoption of clear guidance for both ISPs and customers about the transparency, choice and security requirements for that information.

- **Consent Inherent in Customer Decision to Purchase ISP's Services:** Under the Chairman's proposal, **c**ustomer data necessary to provide broadband services and for marketing the type of broadband service purchased by a customer would require no additional customer consent beyond the creation of the customer-broadband provider relationship. For example, your data can be used to bill you for telecommunications services and ensure your email arrives at its destination, and a broadband provider may use the fact that a consumer is streaming a lot of data to suggest the customer may want to upgrade to another speed tier of service.
- **Opt-out:** Under the Chairman's proposal, broadband providers would be allowed to use customer data for the purposes of marketing other communications-related services and to share customer data with their affiliates that provide communications-related services for the purposes of marketing such services unless the customer affirmatively opts out.
- **Opt-in:** Under the Chairman's proposal, all other uses and sharing of consumer data would require express, affirmative "opt-in" consent from customers.

Your ISP's Duty to Keep Your Data Secure

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. The Chairman's proposal would put in place robust and flexible data security requirements for broadband providers, including an overarching data security standard.

- The proposal would require broadband providers to take reasonable steps to safeguard customer information from unauthorized use or disclosure.
- And, at a minimum, it would require broadband providers to adopt risk management practices; institute personnel training practices; adopt strong customer authentication requirements; to identify a senior manager responsible for data security; and take responsibility for use and protection of customer information when shared with third parties.

Data Breach & Consumers' Right to Know

Consumers have the right to know their data is being handled and maintained securely by their ISPs. They also have the 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. Specifically, in the event of a breach, providers would be required to notify:

- Affected customers of breaches of their data no later than 10 days after discovery.
- The Commission of any breach of customer data no later than 7 days after discovery.
- The Federal Bureau of Investigation and the U.S. Secret Service of breaches affecting more than 5,000 customers no later than 7 days after discovery of the breach.

It's about Permission and Protection, not Prohibition

- The Chairman's proposal does not prohibit ISPs from using or sharing customer data, for any purpose.
- It simply proposes that consumers have choices – either to opt out in some instances or to require that the ISP first obtain customers' permission before using and sharing the customer's data in others.

The Scope of the Chairman's Proposal Does Not Include

- The privacy practices of web sites, like Twitter or Facebook, over which the Federal Trade Commission has authority.
- Other types of services offered by a broadband provider, such as operation of a social media website.
- Issues such as government surveillance, encryption or law enforcement.

The Proposal Seeks Public Comment on Other Ways of Providing Consumers with Increased Choice, Security and Transparency

- While the Chairman's proposal sets forth a clear path forward towards final rules, the NPRM would also seek comment on additional or alternative paths to achieve pro-consumer, pro-privacy goals
- By seeking comment on a range of issues, the NPRM would ensure the development of a robust record upon which the Commission can rely in adopting final rules