March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

Respectfully submitted,

Matthew M. Polka
President & CEO
American Cable Association

Steven K. Berry
President & CEO
Competitive Carriers Association

Meredith Attwell Baker
President & CEO
CTIA

Michael Powell
President & CEO
National Cable & Telecommunications Association

Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.[1] This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2)

[1] This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a "level playing field for companies;" and, most importantly, (3) create "a consistent set of expectations for consumers." To achieve this end, the FCC's policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC's Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU's stated goal of avoiding "duplicative, redundant or inconsistent oversight" by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC's approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC's framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
    - Providers' non-telecommunications services and products
    - Providers' non-telecommunications service provider affiliates
    - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC's policies, rules, and enforcement practices should conform to the FTC's longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC's commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama's Executive Orders 13563 and 13579, which require agencies to "adopt a regulation only upon a reasoned determination its benefits justify its costs" and "tailor its regulations to impose the least burden on society."
    - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
    - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.