Jacquelyne Flemming
AVP – External Affairs/
Federal Regulatory

AT&T Services, Inc.
1120 20th Street, NW.
Suite 1000
Washington, D.C. 20005
Phone: 202 457-3032
Fax: 202 457-3702

VIA ELECTRONIC SUBMISSION

June 28, 2016

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Reply Comments, Response to Initial Regulatory Flexibility Analysis; Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106.

Dear Ms. Dortch:

On June 24, 2016, James Talbot, Jeff Brueggeman, Jonathan Zimmerman, Gary Phillips and I from AT&T met with Matt DelNero, Lisa Hone, Sherwin Siy, David Brody and Melissa Kirkel from the Wireline Competition Bureau to discuss the Commission's broadband privacy proceeding. AT&T's outside counsel, Jonathan Nuechterlein of Sidley Austin LLP, also attended the meeting. During the meeting, we discussed comments filed in the proceeding by AT&T and others as reflected in the attached presentation.

Sincerely,

A Sensible Way Forward on Internet Privacy: Comments of AT&T Services, Inc.

Overview

- **For 20 years, the FTC has enforced a flexible online privacy regime that is technology-neutral and targets *harmful* practices but does not undermine the enormous *benefits* of data for the modern economy.**
  - "The beneficial uses of near-ubiquitous data collection . . . fuel an increasingly important set of economic activities" and any "policy focus on limiting data collection" would not strike "the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth)." (PCAST Big Data Report)
  - Privacy law should not "treat similar technologies within the communications sector differently," and thus "the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers" along with all other participants in the Internet ecosystem. (White House Privacy Report)
- **The FTC's approach turns on two key variables relevant to individually identifiable data:**
  - Is the information sensitive (e.g., health and financial information)?
  - Is it shared with third parties?
- **The industry proposal largely tracks the FTC's longstanding principles.**
- **The FTC's comments encourage the FCC to adopt those principles because:**
  - they reflect decades of experience and reflect basic cost-benefit considerations, and
  - different marketing or data-breach rules should not apply to different industry segments with respect to the same customer information.
- **The FCC should modify its proposed rules to address these concerns.**

AT&T

The Old CPNI Rules Do Not Fit the Internet Ecosystem

- **Myth No. 1 – It is appropriate to map the old CPNI rules designed for the legacy telephone network onto today's Internet ecosystem.**
- **In fact:**
  - The legacy telephone infrastructure was a closed system. The only commercial entities with access to CPNI were telecommunications carriers subject to Section 222.
  - The Internet is an *open* system characterized by the free flow of customer-specific information within a vast ecosystem of online companies subject to the FTC's more flexible regime. That information is the lifeblood of online commerce.
  - Keeping ISPs from using that information will not affect non-ISP actors and will do nothing to keep information private.

AT&T

ISPs Have No Unique Insight Into Customer Data

- **Myth No. 2: ISPs occupy a special position in viewing and synthesizing customer data.**
- **In fact:**
  - ISPs have an increasingly obstructed view of online activity.
    - "70% of global Internet traffic will be encrypted in 2016, with many networks expected to exceed 80%." Sandvine (June 2016).
    - Mobile broadband and Wi-Fi offload are becoming increasingly prevalent.
  - In contrast, large non-ISP platform providers (e.g., Android, Chrome, Facebook) have the best seats in the house.
  - Edge providers have broader and more detailed visibility into individuals' online activity.
    - Even individual websites work with data brokers and ad networks to pool information about individual users to create detailed profiles.
      - A single visit to WebMD's website will share a user's information with more than two dozen third-party entities. (Future of Privacy Forum comments at 9-10.)
- **Even parties that generally support stringent privacy regulation agree:**
  - "The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem . . . . [I]t is obvious that the more substantial privacy threats for consumers are not the ISPs." - EPIC comments at 16.

AT&T

The Proposed Marketing Restrictions Do Not Respect Context and Consumer Choice

AT&T

The Proposed Opt-In Requirement is Overly Broad

- **Under longstanding FTC guidance:**
  - No consent mechanism (even opt-out) is needed for any first-party advertising that does not involve the use of sensitive information.
  - Similarly flexible principles apply to third-party advertising that does not involve sensitive information or sharing with third parties. Most third-party advertising does not involve disclosing individually identifiable information to third-party advertisers .
- **The NPRM cites no persuasive rationale for requiring opt-in for either first- or third-party marketing that involves neither sensitive information nor sharing with third parties. That requirement is particularly indefensible given the wide availability of the same information to the rest of the Internet ecosystem under the FTC's more flexible rules.**
- **"[T]his approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer . . . ." (FTC Comments at 22-23.)**
  - The proposed rules would extend to a wide variety of nonsensitive information, including mere names and addresses (e-mail or IP).
  - Under a literal reading of these rules, an ISP would need to obtain opt-in consent before it could use its own customer list—simple names and email addresses—to email its customers promotional offers for discounted mobile devices or connected appliances.
  - As a result, ISPs would need to use more expensive, less efficient advertising (e.g., TV commercials rather than emails or direct mail) with no discernible privacy benefit to consumers.

AT&T

The Proposed Opt-In Requirement is Overly Broad (continued)

- **Public Knowledge argues that basing consent requirements on the sensitivity of data would "necessarily requir[e] manual inspection of each packet" to "determine whether sensitive information is present in any given communications." That is incorrect.**
- **The concern can logically apply only to uses of communications content, which constitutes a tiny subset of the information the proposed rules would restrict ISPs from using.**
  - Would not apply to use of customer names and email addresses.
  - Would not apply to use of visits to espn.com to market sports-related products.
- **In any event, this "inspection" concern rests on a misunderstanding of how content and other information is used for ad targeting throughout the internet ecosystem.**

AT&T

The Harmful Consequences of Overly Broad Opt-In Rules

- **By creating a default rule against productive data uses, overbroad opt-in requirements impose substantial costs, suppress productive economic activity, and harm consumers. They are not a more consumer-friendly version of opt-out.**
- **If opt-in became a widespread requirement, applicable even to nonsensitive data, it would undermine the economic premise of the modern Internet. The same economic dynamic applies to ISPs.**
  - The market price of broadband service depends in part on what collateral revenues an ISP can earn: either revenues for additional services by the ISP or its affiliates or revenues from third-party advertising.
  - Any consent requirement that hamstrings an ISP's efforts to pursue either type of collateral revenues will impose upward pressure on broadband prices and diminish broadband adoption.
- **Any substantial departure from the notice-and-consent rules applicable to the rest of the online ecosystem would confuse consumers about who may use their data and on what terms.**
- **The proposed marketing restrictions would irrationally protect market incumbents (e.g., Google and Facebook) against competition from new entrants (ISPs) in the digital advertising market.**

AT&T

The Proposed Opt-In Rules Would Violate the APA and the First Amendment

- **The proposed opt-In rules would violate the APA and the First Amendment.**
- **The proposed rules would violate all three prongs of the *Central Hudson* analysis.**
- ***US West* is controlling and *NCTA* is not:**
  - The focus in *NCTA* was on sharing with third parties, not on mere uses of information.
  - *NCTA* involved the closed telephone system – not the information-rich Internet ecosystem – and thus presented no underbreadth concerns.

AT&T

The Proposed Rules Negate The Benefits Of Non-Aggregate De-Identified Data

AT&T

A Sensible Way Forward on Aggregate and Non-Aggregate De-Identified Data

- Businesses, research institutions, and governmental bodies use AT&T de-identified data to produce enormous social and economic benefits.
- There is no legal or policy basis for applying different rules to non-aggregate de-identified data.
- There is no legal or policy basis for subjecting de-identified data to notice-and-consent requirements.
- The proposed de-identification rules should be revised so they are workable in practice.

AT&T

The Proposed Data-Security And Data Breach Rules Would Be Counterproductive And Impose Needless And Substantial Costs

AT&T

A Sensible Way Forward on Data Security and Data Breach Notifications

- ISPs should not be subject to strict liability for ensuring security and should simply be required to ensure the "reasonable" security, confidentiality, and integrity of customer proprietary information (FTC staff comments).
- ISPs should not be required to "promptly remedy any" security concern regardless of cost, data sensitivity, or risk of breach.
- The rules should include a "risk of harm" requirement in connection with breach notification obligations.

AT&T

The Harmful Effects of the Proposed Data Security and Breach Rules

- **The proposed reporting requirements do not provide sufficient time for ISPs to investigate suspected breaches (FTC Staff comments).**
  - The proposal to require notification within 7-10 days of "discovery" of a data breach should be eliminated.
- **The proposed reporting requirements will lead to excessive notice updates to customers and notice fatigue.**
  - Reporting requirements should not apply to "any" customer proprietary information or require separate reports by agents of ISPs (FTC Staff comments).
  - Reporting requirements should not apply to unsuccessful attempts to access customer PI or conduct that "might reasonably lead to" a data breach.

AT&T

Summary: The Optimal Path Forward

- Maintain a technology neutral privacy framework for online data that is consistent with the FTC's well-established approach.
- Adopt notice-and-consent rules consistent with those governing the rest of the online ecosystem.
- Revise the proposed de-identification rules so they are workable in practice
- Revise the proposed data security rules to require ISPs to ensure the "reasonable" security, confidentiality, and integrity of customer proprietary information
- Revise the proposed breach reporting requirements to provide sufficient time for ISPs to investigate suspected breaches and avoid notice fatigue

AT&T