James J.R. Talbot
Executive Director-
Senior Legal Counsel

AT&T Services, Inc.
1120 20th Street NW Ste. 1000
Washington, D.C. 20036

Phone: 202.457.3048
Fax: 202.463.8066
E-mail: jjtalbot@att.com

By ECFS

October 17, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth St., S.W.
Washington, D.C. 20554

Re: ***In the Matter of Protecting Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106***

Dear Ms. Dortch:

AT&T Services, Inc. ("AT&T") files this letter to address the following issues raised by the approach to broadband privacy described in the Fact Sheet released on October 6, 2016 in this proceeding.[1]

First-Party Marketing

The Commission should align its rules for first-party marketing with the FTC's determination that "most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice."[2] Contrary to the FTC's approach, the rules contemplated in the Fact Sheet would require broadband providers to obtain opt-out consent for virtually all first-party marketing uses of non-sensitive customer information, even if such marketing uses no customer information other than the customer's name and address. They also would require providers to obtain opt-out consent to use non-sensitive information for first-party marketing of bundled services that consumers commonly see in today's marketplace.

Nothing in Section 222 authorizes, much less compels, this blanket restriction. The Commission has consistently determined that a customer's name, address, and telephone number are "not CPNI" and may be freely used for marketing without approval.[3] Therefore, the

[1] AT&T does not hereby waive any legal claims it may have with regard to any rules the Commission may adopt in this proceeding.

[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 40 (Mar. 2012); *see also* Letter to Marlene H. Dortch, Secretary, FCC, from James Talbot, AT&T, WC Docket 16-106, October 4, 2016 ("AT&T October 4, 2016 Ex Parte").

[3] Order, *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 13 FCC Rcd. 12390, ¶ 9 (1998) ("1998 Bureau Order") (emphasis added); *see also id.* ("[U]nder section 222 and the Commission's rules, a carrier could contact all of its customers or all of its former customers, for marketing purposes, by using a customer list that contains each customer's name, address, and telephone number"); Order on Reconsideration and Petitions for Forbearance, *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 14 FCC Rcd. 14409, ¶¶ 146-47 (1999) ("1999 Order") (agreeing that "a customer's name, address, and telephone number are not CPNI" and adopting the 1998 Bureau Order's "reasoning and conclusions as [the Commission's] own").

customer consent provisions of Section 222(c)(1) do not even apply to this information.[4] The Commission has also determined that carriers need not obtain customer consent to market new products and services that are "reasonably understood by customers as within the existing service relationship."[5] These findings comport with the text of Section 222 and make abundant policy sense.[6] Applying them here would enable broadband providers to keep customers apprised of new products, services, and discounts in this highly dynamic marketplace.

An opt-out requirement for first-party marketing uses of non-sensitive information is especially unwarranted here given that other statutory provisions already protect customers from unwanted first-party marketing activities. The CAN-SPAM Act, 15 U.S.C. § 7701, et seq., requires, among other things, that companies provide consumers the ability to opt out of all "commercial" e-mails delivered to consumers. And the Telephone Consumer Protection Act, 47 U.S.C. § 227, and the Commission's implementing rules, 47 C.F.R. § 64.1200, require companies to obtain consumers' prior express consent before placing certain informational or marketing phone calls and text messages and also require companies to honor consumers' opt-out requests, including those requests made through the FTC's National Do Not Call Registry. There is no need for an additional, overlapping choice requirement that applies only to first-party marketing by broadband providers.

While the Commission should rationalize its first-party marketing rules with the FTC framework, and could use forbearance to do so, at a bare minimum any rules adopted in this proceeding should include the following provisions which are fully consistent with Section 222:

(a) A BIAS provider may use and share with its affiliates and vendors or agents acting on its behalf a customer's name, address, telephone number, and email address in order to market any product or service offered by the BIAS provider or its affiliates.

(b) A BIAS provider may use non-sensitive customer information and share such information with its affiliates and vendors or agents acting on its behalf to market products and services that use the BIAS provider's broadband network facilities or that the BIAS provider or its affiliates market with broadband Internet access service.

Web-Browsing and App Usage Data

The Commission also should align its rules for broadband providers with the FTC's recommendations by removing the blanket determination that all web browsing history and app usage is considered sensitive information. The Commission's current proposal would classify all web browsing and app usage history as per se sensitive and would thus categorically prohibit broadband providers from using any such information for marketing purposes without opt-in

[4] Section 222(h)(1)(B) expressly exempts subscriber list information from the definition of "customer proprietary network information" and thus from the scope of Section 222(c). *See* 1998 Bureau Order, ¶ 8. The Bureau Order also determined that a customer name, address and telephone number are not otherwise covered by the statutory definition of CPNI. *Id.*, ¶ 9 & n.18.

[5] *Id.* ¶ 43; *see also id.* ¶ 45 (focusing on whether customers "expect that their service provider can and will offer these services along with the underlying telecommunications service").

[6] The Commission found that under Section 222(c)(1)(B) a service that is not currently provided to a customer can be considered "necessary to, or used in, provision of" a telecommunications service that is currently provided to that customer if these two services are "reasonably understood by customers as within the existing service relationship." *Id.*, ¶ 43.

consent. As Google and others have explained, that approach is unreasonably rigid and contradicts the more flexible regime applicable to the rest of the digital advertising ecosystem.[7]

Under the FTC's recommended approach, web browsing and app usage data should be considered sensitive only to the extent they are otherwise categorized as sensitive information. The FTC specified that sensitive information should include the content of communications and the traditional categories of sensitive data (*e.g.*, Social Security numbers and children's, financial, health and precise geolocation data).[8] Thus, for example, web browsing and app usage data that involves the content of a consumer's electronic health records or that could reveal information about someone's sensitive health condition should be considered sensitive. However, the fact that someone has accessed CNN.com or ESPN.com should not be considered sensitive, and companies should be free to use such non-sensitive web browsing and app usage data for marketing purposes so long as they obtain opt-out consent. There is no sound reason to subject broadband providers to a different set of rules than other Internet companies; indeed, as AT&T and others have explained, this would only confuse consumers and deny broadband providers the same opportunity other Internet companies have to participate in the fast-growing digital advertising market. It also would set a harmful precedent that would have far-reaching implications for the dynamic Internet economy. For these and other reasons, AT&T believes that any such restriction would be unlawful and at odds with the First Amendment.

Contrary to the claims of some commenters, the FCC's proposed broad restrictions in this area are not needed to prevent usage of the subset of web browsing and app usage data that is properly classified as sensitive. The premise of these commenters is that the process of differentiating between sensitive and non-sensitive information necessarily involves use of sensitive information, but that premise is factually wrong.

Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ("IAB") and other leading industry associations. This process involves correlating non-content web address or app information (*e.g.*, visit to a sports website) with a pre-established "white list" of permissible interest categories (*e.g.*, sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories. This approach is used today by broadband providers and other Internet companies that use similar web browsing and app usage information for marketing purposes. By limiting the information used for marketing to permissible categories (*e.g.*, sports lover), and not including sensitive categories such as those discussed above, a provider will avoid any use of sensitive information. Accordingly, the FCC should follow the FTC's recommended approach and limit the scope of the opt-in requirement to the specific sensitive information categories discussed above, which will include only a subset of web browsing and app usage information. The FCC should reject proposals to categorize all web browsing and app usage as sensitive information.

The Commission has ample statutory authority to adopt a sensitivity-based approach to the treatment of web browsing and app usage information. Section 222 requires opt-in consent (or "express prior authorization") only for automatic crash notification information and call location information.[9] As noted by Verizon, the Commission reasonably may apply a

[7] *See* Letter to Marlene Dortch, Secretary, FCC, from Austin Schlick, Google, WC Docket 16-106, October 3, 2016.
[8] *See* FTC Staff Comments at 20-22.
[9] *See* 47 U.S.C. § 222(f).

sensitivity-based approach to determine the type of consent for other approvals required by Section 222.[10]

De-Identified Information

The Commission should not categorically exclude from the definition of "de-identified information" any information that may be linked to a device as opposed to an individual. As an initial matter, the Commission lacks authority to impose that overbroad exclusion, as Section 222(c) authorizes it only to restrict uses of information that is "individually identifiable."[11] Further, as a logical matter, information poses a legitimate privacy interest only if a device is linked or linkable to an individual customer.[12] If a device cannot be linked to a specific individual (*e.g.*, by use of an anonymous identifier), information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules. For the same reasons, customer information that is otherwise subject to any rules that may be adopted should not include information that may be linked to a device as opposed to an individual.

Respectfully submitted,

/s/James J.R. Talbot
James Talbot
Executive Director – Senior Legal Counsel

cc: Matt DelNero, Wireline Competition Bureau
Lisa Hone, Wireline Competition Bureau

[10] *See* Letter to Marlene Dortch, Secretary, FCC, from William Johnson, Verizon, Jul. 5, 2016, WC Docket 16-106.
[11] *See* AT&T Comments at 67-68.
[12] *Id*. at 69.