



October 17, 2016

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

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

Dear Ms. Dortch,

On October 13, 2016, Catherine Hilke (Verizon), Michelle Rosenthal (T-Mobile), Matt Sullivan (Sprint), Jay Zimmerman (AT&T) and the undersigned of CTIA met separately with Stephanie Weiner of the Office of Chairman Wheeler, Matt DelNero and Lisa Hone of the Wireline Competition Bureau; Claude Aiken of the Office of Commissioner Clyburn; Amy Bender of the Office of Commissioner O’Rielly; Nick Degani, Alexandra McLeod, and Julia Palermo of the Office of Commissioner Pai; and Travis Litman and Jennifer Thompson of the Office of Commissioner Rosenworcel to discuss the above-referenced proceeding. During the meetings, CTIA and our member companies discussed several aspects of the proposed Order circulated by Chairman Wheeler, as described in the accompanying Fact Sheet,¹ including the importance of harmonization of privacy policy across the internet ecosystem; the strength of the three-prong test developed by the Federal Trade Commission (“FTC”) to guide ISP use of de-identified data; and the operational impact of the consent regime as outlined.

¹ Federal Communications Commission, Fact Sheet: Chairman Wheeler’s Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information (rel. Oct. 6, 2016), available at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/DOC-341633A1.pdf (“Fact Sheet”)



I. Sensitivity Framework

We expressed support for the decision to calibrate customer consent “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.”² Chairman Wheeler’s proposal retains the primary categories identified by the FTC Report as sensitive, i.e. information regarding children, financial and health information, Social Security Numbers, and precise geolocation data³ (assuming that “real-world location of a mobile phone or other device” replicates the FTC’s identification of “precise geolocation information” as a category). The qualifying adjective “precise,” which appears throughout the FTC Report⁴, is critical, because it distinguishes location information that is *sensitive* from location information that is not sensitive.

As FTC staff indicated in meetings that informed the final FTC Report, the phrase was intended to define information that could “pinpoint unique individuals in a precise location,” requiring a high level of specificity.⁵ In testimony following the release of the FTC Report, Jessica Rich, Director of the FTC Bureau of Consumer Protection, explained that this kind of precise geolocation information can be sensitive because it can reveal “intimately personal details about an individual,” such as whether someone has visited an AIDS clinic, a psychiatrist, or a prospective client.⁶ Thus, “precise geolocation

² Fact Sheet at 2.

³ FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers (Mar. 2012) (“FTC Report”), at 59, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁴ FTC Report at 8, 33, 58, and 59.

⁵ “Update on the FTC Privacy Rule and Its Impact on ‘Precise Geolocation Data,’” MAPPS, available at <http://www.mapps.org/blogpost/726441/145183/Update-on-the-FTC-Privacy-Rule-and-its-Impact-on-Precise-Geolocation-Data>. MAPPS is a national association of firms involved in surveying, spatial data, and geographic information systems.

⁶ Testimony of Jessica Rich, Director, FTC Bureau of Consumer Protection, The Location Privacy Protection Act of 2014: Hearing Before the Subcomm. for Privacy, Technology, and the Law (June 4, 2014) at 2, available at https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf.



information” attempts to capture information that allows someone to identify a particular location that an individual has visited with reasonable specificity.⁷

With respect to categories of sensitive information beyond those that the FTC identified in its Privacy Report, the Commission can take a much more tailored approach, which would achieve the Commission’s objectives while ensuring that consumers continue to benefit from new, innovative, and convenient products and services (and discounts) that depend on the use of such data. For instance, the Commission could adapt the FTC’s content-driven framework to the Commission’s proposal by clarifying that web browsing is sensitive to the extent that it includes information from the sensitive categories that the FTC identified.⁸

In addition to discussing the expanded categories that the Commission proposed, CTIA and the member companies raised questions regarding the scope of “financial information,” and cautioned against an over-inclusive approach that would classify certain data (e.g., payment history with the broadband provider) as sensitive information subject to opt-in consent. Member companies also sought assurances that the application of the sensitivity-based approach to certain types of data would not inadvertently restrict the scope of customer data that voice telecom providers can use to market to existing customers under the current CPNI rules.

⁷ See CTIA Comments at 135 (explaining how FTC jurisprudence and guidance and anti-stalking laws distinguish between precise geolocation information and less granular location information); AT&T Comments at 40 (distinguishing between precise geolocation data, on the one hand, and less granular location information that one can discern through cell tower triangulation and zip codes).

⁸ For instance, the Commission could adapt the FTC’s content-driven framework to the Commission’s proposal by clarifying that web browsing is sensitive to the extent that it includes content or information from the sensitive categories that the FTC identified. In fact, the FTC Comments in this proceeding further refine this approach by noting that only deep packet inspection for use of content, such as search terms or purchase history, should require opt-in consent. See Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 19-22, 35 (filed May 27, 2016).



II. De-Identification

CTIA and member companies expressed support for the proposed adoption of the FTC's three-part test for using and sharing de-identified information. The FTC's test, the first prong of which requires a company to take "reasonable measures" to ensure that data are de-identified, is designed to provide strong consumer protection even as technology evolves to enable new methods of data re-identification. It is not a prescriptive test, but rather outcome-based, allowing companies to adopt new de-identification methods, tools and technology to achieve "a reasonable level of justified confidence" that the data cannot reasonably be linkable.⁹

III. First-Party Marketing

We also discussed the importance of being able to infer consent to use non-sensitive and some sensitive customer information to market to, and communicate with customers about products and services that we offer. This approach is consistent with the approach to first-party marketing that both the FTC and the Obama Administration have taken. It is also consistent with the Commission's historical approach to carriers' use of customer proprietary network information ("CPNI") for marketing, allowing carriers to use CPNI to market to existing customers certain products and services that they would expect, given the nature of the underlying service and the relationship. The Commission should adapt this approach to the broadband context and allow ISPs to market "core" offerings, which may evolve over time as technology advances and markets continue to converge.

IV. Other Categories

Finally, we expressed support for the approach on data breach notification and data security outlined in the Fact Sheet. We noted that the implementation period should take into account the work that ISPs will have to do to modify their systems and internal processes to ensure compliance. This

⁹ FTC Report at 21.



work will likely include rewriting computer code, renegotiating contracts with vendors, training staff (both internal and consumer-facing), and so forth.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed in ECFS and provided to the Commission participants. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Maria L. Kirby

Maria L. Kirby
AVP, Regulatory Affairs &
Assoc. General Counsel
CTIA

Attachment

Cc: Claude Aiken
Amy Bender
Nick Degani
Matthew DelNero
Lisa Hone
Travis Litman
Alexandra McLeod
Julia Palermo
Jennifer Thompson
Stephanie Weiner