October 20, 2016

VIA ELECTRONIC FILING

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

Re: Ex Parte Letter Concerning Deviations from the FTC's Privacy Framework in the Chairman's Fact Sheet, *Proposed Rules for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106

Dear Ms. Dortch:

I write to express my concerns regarding the consumer welfare effects of the revised broadband privacy proposal summarized in a Fact Sheet[1] by Federal Communications Commission ("FCC") Chairman Tom Wheeler earlier this month. While the Fact Sheet appears to indicate that the Chairman's revised proposal includes some welcome changes from the initial broadband privacy NPRM adopted by the Commission this Spring,[2] it also raises a number of problematic issues that merit the Commission's attention before final rules are adopted.

While the Fact Sheet asserts that the Chairman's new proposal is "in harmony" with the privacy framework outlined by the Federal Trade Commission ("FTC") (as well as the Administration's proposed Consumer Privacy Bill of Rights), the purported changes in this regard are merely

---

[1] Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information (Oct. 6, 2016), *available at* https://www.fcc.gov/document/fact-sheet-broadband-consumer-privacy-proposal [hereinafter "Fact Sheet"].

[2] Notice of Proposed Rulemaking, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (Mar. 31, 2016), WC Docket No. 16-106, *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf [hereinafter "Initial Broadband Privacy NPRM"].

rhetorical, and do not, in fact, amount to a substantive alignment of the Chairman's proposed approach with that of the FTC.

- First, unlike the FTC's framework, the proposal described by the Fact Sheet ignores the crucial role of "context" in determining the appropriate level of consumer choice before affected companies may use consumer data, instead taking a rigid approach that would stifle innovation and harm consumers.

- Second, the Fact Sheet significantly expands the scope of information that would be considered "sensitive" well beyond that contemplated by the FTC, imposing onerous and unnecessary consumer consent obligations that would deter welfare-enhancing uses of data.

I agree with the Chairman that, if adopted, the FCC's rule should align with the FTC's. But the proposed rule reflected in the Fact Sheet does not. I urge the Commission to ensure that these important deviations from the FTC's framework are addressed before moving forward with adopting any broadband privacy rules.

I. The Chairman's Proposal Ignores the Central Role of Context in the FTC's Privacy Framework

The FTC's approach rightly acknowledges that the need for consumer choice is a function of *both* the *context* of the data collection and use, and the *sensitivity* of the data collected. For data usage consistent with "the context of the transaction or the company's relationship with the consumer," regardless of the sensitivity of the data involved, the FTC does not generally require choice (let alone affirmative consent) before a company collects or uses consumer data.[3] The sensitivity of the information is relevant only "[f]or practices requiring choice," meaning those that fall outside the context of the transaction.[4] For these uses, the FTC requires "affirmative express consent" (opt-in consent) only for uses of sensitive data.[5]

---

[3] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (Mar. 26, 2012) at 48, *available at* https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy [hereinafter "FTC Privacy Report"].

[4] *Id.* at 60.

[5] *Id.*

Despite its claims to the contrary, Chairman Wheeler's Fact Sheet ignores this critical component of the FTC's framework by focusing solely on the sensitivity of data, while completely overlooking the context in which it is used.

The Fact Sheet states that the Chairman's proposal "is calibrated to the sensitivity of the information…" because doing so is "in line with customer expectations."[6] But this is inconsistent with the FTC's approach. In fact, the FTC's framework explicitly *rejects* a "consumer expectations" standard: "Rather than relying solely upon the inherently subjective test of consumer expectations, the [FTC's] standard focuses on more objective factors related to the consumer's relationship with a business."[7]

Chairman Wheeler's "consumer expectations" framing is a transparent attempt to *claim* fealty to the FTC's well-developed standards while actually *implementing* a privacy regime that is flatly inconsistent with those standards.

Unlike Chairman Wheeler's proposal, the FTC's approach is an appropriately flexible one, aimed at balancing the immense benefits of information flows with sensible consumer protections. Thus it eschews an "inflexible list of specific practices" that would "risk[] undermining companies' incentives to innovate and develop new products and services…."[8]

Instead, the FTC's framework begins by establishing a sort of "safe harbor" for data use where its benefits may be presumed to exceed its costs and consumer consent may be inferred:

> Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer….[9]

To the limited extent that the proposal set forth in the Fact Sheet identifies any categories of uses from which it will infer consent, by contrast, it adopts the

---

[6] Fact Sheet at 2.

[7] FTC Privacy Report at 38.

[8] FTC Privacy Report at 38. Nevertheless, the FTC does identify certain "illustrative" categories of interactions that would "not typically require consumer choice," including "fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing…." *Id.* at 39.

[9] *Id.* at 48. The framework also infers consent when practices "are required or specifically authorized by law." *Id.*

"inflexible" approach that the FTC was expressly trying to avoid: a mechanical, "bright-line standard that freezes in place current practices and potentially could harm innovation and restrict the development of new business models."[10]

Not only does the Fact Sheet limit inferred consent to a narrow set of specific "purposes spelled out in the statute — the provision of broadband service, or billing and collection for example,"[11] but these appear to contemplate a much smaller scope of activity than even the FTC's *illustrative* examples. Because the proposal is not public, however, we do not know for certain what, if any, additional uses beyond "provision…, billing and collection" might merit inferred consent.[12]

What is certain, however, is that the Chairman's proposal does not likely heed the FTC's call for humility and flexibility regarding the application of privacy rules to ISPs (and other Internet platforms):

---

[10] *Id.* at 36.

[11] Fact Sheet at 2. *See also* 47 U.S. Code §§ 222(c)(1) & (d).

[12] Although, regardless, the scope is needlessly rigid, it is not clear is whether this latest iteration of the Chairman's proposal treats *only* the specific exceptions listed in § 222(d) and one or two other places in the statute as "spelled out in the statute," or whether it also includes (as did the Initial NPRM) the relatively open-ended language of § 222(c)(1) referring to activities "necessary to, or used in, the provision of" broadband service. *See* Initial Broadband Privacy NPRM at ¶ 113. If it does, and depending on how narrowly it is interpreted by the Chairman, this language may describe a substantial set of practices in which consent may be inferred, thus softening somewhat the Fact Sheet's apparent and overly restrictive standard.

Importantly, the FTC identifies most first-party marketing as a use "consistent with the context of the transaction," and thus not requiring consent. The FTC does note that companies should enable opt-in consent for the use of *sensitive data* in first-party marketing — but, for the FTC, even this limitation is flexible. The FTC Privacy Report notes that "the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information," for example. FTC Privacy Report at 46-47 (emphasis in original).

Moreover, and tellingly, the FTC notes a specific exception from inferred consent for ISPs *using deep packet inspection* for marketing purposes — although, even then, it recommends only some opportunity for choice, and not necessarily affirmative consent. FTC Privacy Report at 40-41 & 56. The implication is clear, however: ISPs' first-party marketing that does *not* use deep packet inspection does *not* automatically trigger a choice obligation under the FTC's framework. The same is seemingly not true of the Chairman's proposal.

> These are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data.[13]

2. The Chairman's Proposal Moves Far Beyond the FTC's Definition of "Sensitive" Information Requiring "Opt-in" Consent

Chairman Wheeler's Fact Sheet also contemplates a significant expansion of what constitutes "sensitive" information requiring "opt-in" consent, well beyond what the FTC's framework embodies (and well beyond what the statute authorizes). As a result, the proposal would require opt-in consent — which is significantly more restrictive than opt-out — for virtually all uses of sensitive data, without justification or corresponding consumer benefit.

As noted, under the FTC's regime, the sensitivity of data matters essentially only for transactions inconsistent with context. But the FTC's approach contemplates a further distinction, between data uses that require "express affirmative" (opt-in) consent and those that do not (requiring only "other protections" short of opt-in consent[14] — *e.g.*, opt-out). In the FTC's framework, it is *this* distinction that generally turns on the sensitivity of the data involved.

Because the distinction is so important — because opt-in consent is much more likely to staunch data flows — the FTC goes to great pains to provide guidance as to what data should be considered sensitive, and to cabin the scope of activities requiring opt-in consent. Thus, the FTC agrees that "information about children, financial and health information, Social Security numbers, and precise geolocation data [should be treated as] sensitive."[15] Beyond those instances, however, the FTC does not consider any other type of data as inherently sensitive.[16]

By contrast, and without explanation, Chairman Wheeler's Fact Sheet adds to this list several additional categories of information. In particular, it designates

---

[13] *Id.* at 56.

[14] *Id.* at 60.

[15] *Id.* at 59.

[16] It should be noted that the FTC Privacy Report would also impose an opt-in requirement when companies adopt "material retroactive changes to privacy representations." *Id.* at 57-58.

"web browsing history," "app usage history," and "the content of communications" as sensitive data.[17]

Treatment of these categories of information as sensitive and requiring opt-in consent is flatly inconsistent with the FTC's approach. If adopted, such rules would deter consumer-welfare-enhancing uses of data.

It is telling that when the FTC sought public input on its own privacy framework, *only a single commenter* would have "characterized as sensitive information about consumers' online communications or reading and viewing habits."[18] The FTC explicitly rejected this suggestion.

Instead, the FTC treats web browsing history as information that raises "special concerns," often requiring some form of consumer *choice*, but not as sensitive information requiring *opt-in consent*.[19] Similarly, nothing in the FTC Privacy Report (or elsewhere) suggests that "app usage history" or "the content of communications" should necessarily be treated as sensitive or encumbered by opt-in requirements.

In fact, to the extent that the FTC has supported the use of do not track (DNT) mechanisms (for both web browsing,[20] as well as app usage[21]) in order to provide consumers some choice regarding use of their web browsing and app usage histories, it recommends DNT only in the form of consumer *opt-out*, not opt-in, and only when inconsistent with context.[22]

---

[17] Fact Sheet at 2.

[18] FTC Privacy Report at 59. (citing to Comment of Electronic Frontier Foundation, cmt. #00400, at 7).

[19] Such usage is discussed not in the section of the Report on "Practices Requiring Affirmative Express Consent," IV.C.2.e, but rather in the section on "Large Platform Providers That Can Comprehensively Collect Data Across the Internet Present Special Concerns," IV.C.2.d. *See id.* at 41.

[20] *Id.* at 52-55.

[21] *See* FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency (2013) at 20-21, *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [hereinafter "FTC Staff Mobile Privacy Report"].

[22] FTC Privacy Report at 53 ("[A]n effective Do Not Track system should… [enable consumers to] opt out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction…"); FTC Staff Mobile Privacy Report at 21 (adopting the DNT standards described in the FTC Privacy Report).

Moreover, by treating virtually *all* useful information accessible by ISPs as "sensitive,"[23] and by making the sensitivity of data the primary determinant for opt-in consent, the Chairman's proposal would dramatically expand the constraints on data collection and usage for ISPs well beyond those espoused by the FTC —without any evidence of a corresponding benefit. "'Opt-in' offers no greater privacy protection than allowing consumers to 'opt-out'…, yet it imposes significantly higher costs on consumers, businesses, and the economy."[24] Not surprisingly, these effects fall disproportionately on the relatively poor and the less technology-literate.[25]

> By adopting a default rule that stops the free flow of information, "opt-in" impedes economic growth by raising the costs of providing services and… decreasing the range of products and services available to consumers…. "Opt-in" reduces competition and raises prices…. [And] "opt-in" systems… [are] contrary to consumer expectations.[26]

What's more, because the Chairman's proposal would impose these inappropriate and costly restrictions only on ISPs, it would create a barrier to competition by ISPs in other platform markets, without offering a defensible consumer protection rationale to justify either the disparate treatment or the restriction on competition.[27]

---

[23] The Fact Sheet notes that "[a]ll other individually identifiable customer information — for example, service tier information used to market an alarm system — would be considered non-sensitive and the use of sharing of [sic] that information would be subject to opt-out, consistent with customer expectations." It is difficult to conceive of what relevant data accessible by ISPs *other* than "service tier information" would fall outside of the Chairman's enumerated categories of sensitive data, however.

[24] Fred H. Cate and Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* at 1, *available at* http://home.uchicago.edu/~mferzige/fallacyofoptin.pdf.

[25] *See, e.g.,* Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REPORT 31, 38 (2002); Nicklas Lundblad and Betsy Masiello, *Opt-in Dystopias*, SCRIPTED, § 5.1 (2010), *available at* http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

[26] *Protecting Privacy in the New Millennium, supra* note 24 at 2.

[27] *See, e.g.,* Comments of the International Center for Law & Economics and Scholars of Law & Economics, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (May 27, 2016) at 12-20, *available at* https://www.fcc.gov/ecfs/filing/60001975214/document/60002081125.

Nor is this result required by the statute. Seemingly, even for those uses of information that the statute specifically authorizes only "with the approval of the customer," it requires opt-in consent only for disclosure of proprietary information to third-parties. The basic rule in § 222(c)(1) is that disclosure or use is limited "[e]xcept as required by law **or with the approval of the customer**"

———————

The Fact Sheet is correct insofar as it suggests that the FCC *should* in fact conform its privacy rules to those established by the FTC, an agency that has a long history of addressing consumer privacy concerns, including in the context of Internet practices and online data. Unfortunately, the reality of the Fact Sheet simply does not conform to its rhetoric. And, sadly, we have only the terse and ambiguous Fact Sheet from which to judge the Chairman's proposal, as he has refused to make his revised proposal available outside the Commission — despite the apparently crucial changes embodied in the Fact Sheet.

In light of these defects, I urge the Commission to refrain from adopting the regime set forth by the Chairman in his Fact Sheet, and to ensure that these significant deviations from the FTC's well-accepted framework are addressed before moving forward.

Respectfully submitted,

Geoffrey A. Manne
Executive Director
International Center for Law & Economics
3333 NE Sandy Blvd., Suite 207
Portland, OR 97232

(emphasis added). But "approval of the customer" is not necessarily "affirmative express consent," and can be effected by notice and *non-choice — i.e.*, by an informed consumer's decision not to opt-out. By contrast, § 222(c)(2) requires that "[a] telecommunications carrier shall **disclose** customer proprietary network information, **upon affirmative written request by the customer**, to any person designated by the customer" (emphasis added). Although this is couched in terms of a provider's obligation to share information when a customer requests it, it also indicates that Congress was fully cognizant of the different degrees of consumer consent, and saw fit to impose a heightened, affirmative consent standard only in the case of disclosure, rather than first-party use.