CENTER FOR DEMOCRACY & TECHNOLOGY

March 24, 2022

Via ECFS.

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: *Empowering Broadband Consumers Through Transparency*, CG Docket No. 22-2

Dear Ms. Dortch:

The Center for Democracy & Technology (CDT) respectfully submits this reply comment in response to the Notice of Proposed Rulemaking issued by the Commission, seeking public comment on the creation of labels to disclose information about broadband services offered by internet service providers (ISPs) to consumers.[1] CDT applauds the Commission's efforts to encourage competition and innovation in broadband service through transparency and urges the Commission to require ISPs to include specific information about their privacy practices in their consumer labels. As discussed below:

- ISPs' privacy practices necessitate the addition of easily-understood privacy disclosures to the consumer labels;
- The privacy disclosures should address the most harmful practices recently identified by the Federal Trade Commission; and,
- Requiring privacy disclosures is within the Commission's authority under the Communications Act and the Constitution.

[1] *Empowering Broadband Consumers Through Transparency*, CG Docket No. 22-2, Notice of Proposed Rulemaking, FCC 22-7 (2022).

CENTER FOR DEMOCRACY & TECHNOLOGY

ISPs' Privacy Practices Necessitate the Addition of Easily-Understood Privacy Disclosures to the Consumer Labels

Current ISP privacy practices overwhelm consumers. Simply providing consumers a link to a lengthy privacy policy is insufficient and fails to quickly and effectively allow consumers to grasp how ISPs collect, process, retain, and share their data.[2] CDT has long-advocated for robust data collection, sharing, and use limitations to lessen the burden on consumers and better protect their privacy.[3] As we continue to wait for comprehensive federal privacy legislation, more can be done to address privacy-invasive data practices. Disclosures on consumer broadband labels present one such opportunity.

ISPs collect and otherwise process extensive data about their customers. A 2021 Federal Trade Commission (FTC) staff report details troubling data practices by the country's largest providers.[4] The FTC found that many ISPs collect and share far more consumer data than consumers appreciate and expect. For example, ISPs are able to collect and then combine a host of individualized data about their customers across their products, including the websites customers visit, the shows they watch, the apps they use, details about home energy use, their real-time and historical location, internet search queries, and even the content of communications.[5]

---

[2] Ranking Digital Rights Comments at 2-4, *available at* https://ecfsapi.fcc.gov/file/10309205225941/Ranking%20Digital%20Rights_Comment%20on%20the%20FCC's%20NPRM%20for%20Broadband%20Consumer%20Labels.pdf.

[3] *See Generally* Ctr. Democracy & Tech., CDT Federal Baseline Privacy Legislation Discussion Draft (Dec. 2018), https://cdt.org/wp-content/uploads/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.

[4] Fed. Trade Comm'n, A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers (Oct. 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[5] *Id*. at 34.

Harmful ISP data practices do not end at over-collection. It also extends to secondary uses of data unrelated to the provision of services that the customer requested. For example, consumers may not appreciate that some ISPs log and retain data, like data associated with web browsing or television viewing history, to build and maintain behavioral profiles about consumers for better advertising targeting.[6] At least half of the ISPs the FTC examined engage in cross-device tracking, a practice that consumers will not necessarily understand and could even violate consumer expectations because people expect their devices will be kept separate.[7] Even more alarming are ISP practices around the collection, use, and sale of consumers' location information.[8] Location information can reveal personal information about peoples' health, faith, and sexual orientation. Moreover, in addition to location data, several ISPs also collected and shared consumer race and ethnicity data (or proxies for such data) for advertising purposes, and sold that data to unrelated businesses.[9] These practices can result in discrimination based on protected classes.[10]

Finally, ISPs employ practices that fail to provide consumers meaningful privacy choice, and instead steer consumers towards settings that permit greater data sharing.[11] Such practices primarily benefit companies, not consumers.[12] Even more troubling, the FTC concluded that it is difficult or near

[6] Fed. Trade Comm'n (2021), *supra* n. 3 at 35.
[7] *Id*. at 36.
[8] *Id*. at 36-37.
[9] *Id*. at 38.
[10] *Id*.
[11] *Id*. at 39.
[12] *See* Yoree Koh & Jessica Kuronen, *How Tech Giants Get You to Click This (and Not That)*, Wall St. J., (May 31, 2019), https://www.wsj.com/articles/how-tech-giants-get-you-to-click-this-and-not-that-11559315900.

impossible for consumers to meaningfully access their information held by ISPs.[13] This lack of information and meaningful control was often by design; according to the FTC, ISPs intentionally obfuscate their practices through broad terms, cumbersome procedures to exercise data rights, and a lack of meaningful access to data.[14] Such practices diminish consumer agency and prevent them from exercising basic access and control rights.[15]

Collecting, using, and retaining consumer data that is outside the scope of what is necessary to deliver the specific service people have requested can harm consumers.[16] These harms manifest in several ways, including identity theft, unwanted exposure, embarrassment, stigma, lack of autonomy, and chilling effects on expression and speech.[17]

Greater transparency into overbroad data collection practices better equips consumers to confront and prevent these harms. Labels with clear information about ISPs' privacy practices empower consumers to select a provider with full information about the broadband service they are purchasing. Transparency benefits consumers even when they have limited choice in providers by enabling them to exercise control over their data. Transparency into ISP data practices helps alert consumers to examine and change privacy settings or online behaviors, and can deter providers from engaging in practices that consumers dislike. Finally, more transparency provides a basis for regulators,

[13] Fed. Trade Comm'n (2021), *supra* n. 3 at 30.
[14] *Id.* at 26-31.
[15] *See generally*, Ctr. Democracy & Tech., CDT Baseline Individual Rights One Pager, (Jan. 2019), https://cdt.org/wp-content/uploads/2019/01/2019-01-30-CDT-Baseline-Individual-Rights-One-Pager-2.pdf.
[16] *See* Access Now, *Data Minimization: Key to Protecting Privacy and Reducing Harm* (2021), https://www.accessnow.org/data-minimization-guide/.
[17] *Id*.

like the FTC, to prevent unfair and deceptive trade practices when ISPs fail to adhere to their disclosures.

The Privacy Disclosures Should Address the Most Harmful Practices Recently Identified by the Federal Trade Commission

The Commission should require ISPs to disclose key information that is particularly relevant to the types of troubling data practices identified in the FTC report. Clear standardized information about privacy practices in labels allows consumers to quickly digest key information without having to navigate through densely-worded, lengthy external privacy policies. This approach allows consumers to easily identify items and compare and contrast how each provider addresses consumer data. In particular, we recommend the Commission consider the addition of the following information to consumer broadband labels to avoid deception to consumers.

- Labels should include information about the types of consumer data that is collected. These standardized sections can identify specific categories of collected information such as:
    - Subscriber information,
    - Browsing history,
    - App usage,
    - Location, and
    - Does the ISP collect or purchase any of this data about customers from third parties?

- Labels should also disclose the purposes for which consumer data is used outside of providing the requested broadband service. These standardized sections can identify specific uses for collected consumer data such as:
    - Target advertising,
    - User profiling,
    - Algorithmic training, and
    - Sale or sharing to data brokers/ third parties that are not law enforcement entities.
- Labels should disclose ISP data retention practices. These standardized sections can identify specific retention practices such as:
    - How long data about consumers is retained,
    - If any anonymized or deidentified consumer data is retained,
    - When, if ever, consumer data is deleted?

Finally, labels should clearly tell users about their affirmative rights. This includes disclosures about and direct links to consumers' ability to access, correct, move, and delete their data. Moreover, labels should inform consumers about what choices they have about the collection and use of their data, including the ability to limit sharing with third parties.

Requiring ISP privacy disclosures in broadband labels provides consumers with critical data points to consider, evaluate, and weigh how ISPs treat consumers' personal information, and it will help provide much needed sunlight on ISP privacy practices beyond dense and lengthy privacy policies that consumers may not fully review or comprehend. Finally, greater transparency may cause ISPs to rethink and cease to use some of the more egregious data practices discussed above.

Requiring Privacy Disclosures Is Within the Commission's Authority Under the Communications Act and the First Amendment

The Commission has the legal authority to require privacy disclosures in its broadband labels to meet the Communications Act's requirement that it report on "market practices" within the communications marketplace. Further, because the disclosures avoid consumer deception and fit within long-established, uncontroversial frameworks for transparency regarding privacy practices, the First Amendment is no bar to narrowly tailored disclosures.

The Communications Act grants sufficient latitude to the Commission to require ISPs to disclose their "market practices," including privacy practices. Section 13 of the Communications Act, as amended, requires the Commission to publish a biennial report on the "state of the communications marketplace."[18] The report must include ISPs and assess whether "marketplace practices pose a barrier to competitive entry into the communications marketplace."[19] The Act, however, "does not specify precisely how [the Commission] should obtain and analyze information for purposes of its reports," and it may reasonably be interpreted as "including within it direct authority to collect evidence to prove that such barriers exist."[20] Based on this reading of the Act, the D.C. Circuit has affirmed the Commission's current "transparency rule,"[21] which requires ISPs to "publicly disclose accurate information" regarding their "commercial terms,"[22] including privacy practices.[23]

[18] Consolidated Appropriations Act, 2018, sec. 401, § 13(a), 132 Stat. 1087-88 (2018) (codified at 47 U.S.C. § 163).
[19] *Id.*, § 13(b)(3).
[20] Mozilla Corp. v. FCC, 940 F.3d 1, 47 (2019)
[21] *Id.*
[22] 47 C.F.R. § 8.1(a).
[23] *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311, 442, para. 213 (2018).

Further, carefully circumscribed privacy disclosures are consistent with the First Amendment. "Voluntary advertising" and "product labeling at the point of sale"[24] may be required to "appear in such a form, or include such additional information, warnings, and disclaimers, as are necessary to prevent its being deceptive" for consumers.[25] Commercial speech is protected by the First Amendment,[26] but disclosures to remedy deceptions withstand constitutional scrutiny "as long as [the] disclosure requirements are reasonably related to the State's interest in preventing deception of consumers,"[27] the mandated disclosures require only "purely factual and uncontroversial information about the terms under which . . . services will be available," and they are not unduly burdensome.[28] Under that standard, the Supreme Court and the Courts of Appeals have upheld mandates that attorney advertising disclose costs to clients,[29] that debt relief agencies disclose that their services may involve bankruptcy,[30] and that labels on meat disclose the country of origin.[31]

Circumscribed disclosures of ISPs' privacy practices meet those requirements. Privacy disclosures would help consumers avoid deception by understanding a material aspect of the terms of the services they are purchasing. As the FTC's report demonstrates, consumers often lack that information, in part due to a lack of transparency by ISPs. ISPs' privacy practices are a material term in

[24] Nat'l Ass'n of Mfrs. v. SEC, 800 F.3d 518, 522, 523-24 nn.13-14 (D.C. Cir. 2015) ("NAM") (citing Am. Meat Inst. v. United States Dep't of Agric., 760 F.3d 18, 23 (D.C. Cir. 2014) (en banc) ("AMI")).

[25] 44 Liquormart v. Rhode Island, 517 U.S. 484, 498 (1996) (quoting Virginia Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 772 n.4 (1976)).

[26] Zauderer v. Office of Disciplinary Counsel of Supreme Court, 471 U.S. 626, 637, 651 (1985).

[27] *Id.* at 651.

[28] Nat'l Inst. of Family & Life Advocates v. Becerra, 138 S. Ct. 2361, 2372 (2018) (quoting *Zauderer*, 471 U.S. at 651).

[29] *Zauderer*, 471 U.S. at 651.

[30] Milavetz, Gallop & Milavetz, P.A. v. United States, 559 U.S. 229, 252-53 (2010).

[31] *AMI*, 760 F.3d at, 27.

the offer of broadband service — for example, one Pew Research survey revealed that 81 percent of Americans believe that the risks of companies collecting their personal data outweigh the benefits; yet, 59 percent have "little/no understanding" about what companies do with the data collected.[32] The FTC has likewise determined that companies' misrepresentations about how they "collect, use, and share consumer data" may be material to consumers and constitute a deceptive act or practice under the FTC Act.[33]

Similarly, the disclosures would be "factual and uncontroversial." Under this requirement, mandatory disclosures must be "factual and non-ideological."[34] Mandatory disclosures "may not compel affirmance of a belief with which the speaker disagrees"[35] so as to prevent the person subject to disclosures from opting to "convey [their] 'message' through 'silence.'"[36] For example, the D.C. Circuit invalidated mandatory labeling of minerals as "[not] conflict-free" because it amounted to an "assessment of moral responsibility."[37] In contrast, the D.C. Circuit found a country-of-origin label for meat products "uncontroversial" because it allowed producers to select between the terms

[32] Brooke Auxier, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[33] *Restoring Internet Freedom*, WC Docket No. 17-108, Comment of the Staff of the Federal Trade Commission, at 3-4 (2017), *available at* https://www.ftc.gov/legal-library/browse/advocacy-filings/comment-staff-bureau-consumer-protection-bureau- competition-bureau-economics-federal-trade; *accord Developing the Administration's Approach to Consumer Privacy*, Docket No. 180821780–8780–01, FTC Staff Comment, at 14-15 (2018), *available at* https://www.ftc.gov/legal-library/ browse/advocacy-filings/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy.

[34] *NAM*, 800 F.3d at 530.

[35] *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557, 573 (1995)

[36] *NAM*, 800 F.3d at 530 (citing *Hurley*, 515 U.S. at 573).

[37] *Id.* (alteration in original).

"slaughter" and "harvested," of which, only the former "might convey a certain innuendo."[38] Although privacy practices continue to evolve, the components of the data lifecycle — including collection, use, and disclosure — have been well defined for over forty years, as have the corresponding principles of transparency around those practices.[39] The disclosures here would be limited to the factual disclosure of ISPs' own practice within that established framework and would not constitute a message or assessment of ISPs' practices that would preclude an ISP from otherwise explaining or defending them.

CDT supports the Commission's efforts to foster competition and innovation in broadband service through transparency and encourages the Commission to adopt easily understood privacy disclosures in its labels.

Sincerely,

Andrew Crawford
Senior Counsel, Privacy & Data, CDT

Cody Venzke
Senior Counsel, Equity in Civic Technology, CDT

[38] *AMI*, 760 F.3d at 27.

[39] *See* CDT, *Privacy Recommendations for the National Broadband Plan* (Jan. 25, 2010), https://cdt.org/insights/privacy-recommendations-for-the-national-broadband-plan/; FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace (2000), *available at* https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission; U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), *available at* https://aspe.hhs.gov/reports/records-computers-rights-citizens.