Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

Hearings on Competition and Consumer Protection in the 21st Century	)	Project No. P181201

COMMENTS OF AT&T SERVICES INC.

RESPONSE TO ISSUES 4 AND 5

David L. Lawson
James R. Wade
Robert C. Barber
AT&T SERVICES INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2121

Timothy J. Muris
Jonathan E. Nuechterlein
C. Frederick Beckner III
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

August 20, 2018

RESPONSE TO ISSUES 4 & 5:

"The intersection between privacy, big data, and competition," including "the benefits and costs of privacy laws."

1. The Commission's Privacy Framework Has Succeeded Because It Is Measured and Collaborative.

The Commission has exercised highly effective leadership in the development of U.S. privacy policy by wearing several different hats. In its most obvious role as "cop on the beat," the Commission "has brought over 500 enforcement actions protecting the privacy of consumer information."[1] Yet the Commission plays an equally effective role when engaging directly with industry and other stakeholders more informally—through workshops and reports, when analyzing the complex issues raised by commercial uses of consumer data, when representing U.S. interests in foreign proceedings, and when recommending best practices in privacy-related disclosures to consumers.[2]

The Commission has succeeded in these multiple roles because it recognizes that privacy debates often present complex trade-offs in need of balanced solutions.[3] The Commission has thus long supported a measured approach that protects consumers from genuine privacy abuses while recognizing that consumer information fuels the modern internet, enabling companies to

---

[1] FTC, *Privacy & Data Security Update: 2017*, at 2 (2018).

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

[3] There is broad bipartisan consensus on this point. *See* President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, at x-xi (May 2014) ("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)."); FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, at 2 (Mar. 2012) ("FTC 2012 Privacy Report") (noting that "the collection and use of consumer data has led to significant benefits in the form of new products and services").

offer consumers countless valuable services at deep discounts or for free. For example, the Commission has consistently opposed overbroad opt-in requirements for non-sensitive information, which foreclose productive uses of data without adequate justification.[4] This type of nuanced oversight is a key reason why the world's leading e-commerce companies, which have converted consumer data into trillions of dollars of consumer value, are headquartered in the United States rather than in foreign jurisdictions with more absolutist approaches.

Just as important, in developing the details of this framework, the Commission has properly relied on industry and multi-stakeholder processes rather than one-size-fits-all, top-down government regulation. One example is the process for determining what web-browsing data should be considered "sensitive" for notice-and-choice purposes. Companies typically rely on industry self-regulatory guidelines that preclude the use of categories of presumptively sensitive information—such as sensitive medical conditions—to target marketing at particular consumers.[5] These self-regulatory mechanisms are often superior to governmental mandates because, unlike prescriptive rules, multistakeholder processes provide the flexibility and speed necessary to address rapid technology and market changes.

[4] *See*, *e.g.*, FTC 2012 Privacy Report at 15-16; Comments of FTC Staff, FCC WC Docket No. 16-106, at 22 (May 27, 2016). Opt-in is an appropriate mechanism for sensitive consumer data, such as medical or financial information, that many consumers would not want to be shared. But compulsory opt-in mechanisms can present serious costs when applied broadly to nonsensitive information. In that context, when consumers fail to opt in, they often do so not by considered choice, but because they do not wish to take the time needed to make a choice and do not fully internalize the broader economic costs of that non-choice. *See*, *e.g.*, Joshua D. Wright, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy*, at 18-20 (May 27, 2016) (submitted by the United States Telecom Association in FCC WC Docket No. 16-106 and available at https://www.fcc.gov/ecfs/).

[5] *See, e.g.*, Digital Advertising Alliance, *Application of Self-Regulatory Principles to the Mobile Environment* (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf; Network Advertising Initiative Code of Conduct (2013), https://www.networkadvertising.org/2013_Principles.pdf.

2. Any Privacy Framework Should Promote Competitive Parity and National Consistency.

As AT&T discusses in its separate response to Issue 2, the Commission should pursue both competitive parity and regulatory predictability on all competition and consumer protection topics within its jurisdiction. Privacy and data security rules are a case in point. As discussed below, (1) there is no basis for subjecting ISPs to more onerous privacy restrictions than those applicable to leading online competitors such as Google and Facebook, and (2) the Commission should work with Congress to enact new legislation restoring predictability and national consistency to privacy oversight in the United States.

a. Any privacy framework should apply consistently to providers throughout the internet ecosystem.

As noted in our Issue 2 response, any privacy and data security framework should apply consistently to all internet companies, and there is no basis for imposing unusually stringent restrictions on ISPs in particular. That conclusion appears to be gaining some measure of consensus. For example, despite their many flaws, the recent privacy mandates issued by both the European Commission (the General Data Protection Regulation) and California (the California Consumer Privacy Act of 2018) at least avoid subjecting ISPs to more intrusive regulation than other internet companies. That said, calls for ISP-specific privacy restrictions remain stubbornly persistent in some quarters,[6] and they remain as baseless as before.

For many years, FCC-focused interest groups have sought to justify such asymmetric regulation on the premise that ISPs have greater visibility into online user behavior than so-called "edge" providers such as Google and Facebook. That premise stands reality on its head.

[6] *See*, *e.g.*, Salome Viljoen, *Facebook's Surveillance Is Nothing Compared with Comcast, AT&T and Verizon*, The Guardian (Apr. 6, 2018); Karl Bode, *Given Facebook's Privacy Backlash, Why Aren't We Angrier with the Broadband Industry?*, Motherboard (Mar 20, 2018).

First, the now-pervasive use of encryption blinds ISPs but *not* the operators of browsers, operating systems, and social networks to most of a given user's online activities.[7] Those "edge" providers also typically have continuous visibility into a user's activities, whereas any given user typically shifts from one ISP to another (home, cellular, office) during the course of a day.[8] As University of Pennsylvania Professor Michael Kearns explains, the leading edge providers' "combination of data volume, diversity, intimacy and [predictive] modeling provides insights about consumers … that are historically unrivaled and are still rapidly expanding," whereas data gleaned by ISPs are "more limited" and "in many ways less comprehensive and valuable."[9] It also makes no sense to defend ISP-specific privacy burdens on the theory that ISPs face less retail competition and thus less accountability to end users than edge platform providers do. If anything, it is easier to switch from one mobile provider to another than from one operating system to another—a choice that requires abandoning one's smartphone and all its apps.

Indeed, saddling ISPs with special privacy-related burdens would be affirmatively anticompetitive because it would disable them from bringing much-needed competition to leading online companies. Information is a crucial competitive advantage in many markets, from

[7] *See* Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Geo. Tech. Inst. for Info. Sec. & Privacy, May 2016). According to Google's most recent Transparency Report providing a snapshot of HTTP encryption on the web, 85% of web pages downloaded in the U.S. using Chrome (which is the most popular web browser) are encrypted. *See* Google, *HTTPS Encryption on the Web*, https://transparencyreport.google.com/https/overview?hl=en (last viewed Aug. 16, 2018).

[8] *See*, *e.g.*, Comments of the Electronic Privacy Information Center, FCC WC Docket No. 16-106, at 16 (filed July 17, 2016) (available at https://www.fcc.gov/ecfs/) ("Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. … [I]t is obvious that the more substantial privacy threats for consumers are not the ISPs.").

[9] Michael Kearns, *Data Intimacy, Machine Learning, and Consumer Privacy*, at 2 (Penn. Law/CTIC 2018), https://www.law.upenn.edu/live/files/7952-kearns-finalpdf.

digital advertising to streaming video.[10] Restricting ISPs' ability to access, collect, and use data in responsible ways could only enhance the market power of the online companies that have converted their unrivaled stores of consumer data into dominance of various online markets. AT&T's objective is not to limit the ability of those companies to continue collecting and using such data (assuming they do so in a responsible manner). But the Commission should ensure that potential rivals, including ISPs, can compete with those data incumbents by making productive and responsible use of consumer information on a level playing field.

b. The need for a unified national privacy framework.

As the Commission is aware, the California legislature recently enacted the California Consumer Privacy Act of 2018, which is scheduled to take effect in 2020. Unless it is substantially amended, this new statute will subject companies to more stringent privacy restrictions than any other U.S. law, past or present.[11] The California legislation and similar initiatives in other states threaten to create a highly problematic patchwork quilt of privacy regulation. Internet communications are by nature geography-agnostic, and providers cannot feasibly tailor online services to the disparate rules of many different U.S. jurisdictions. As a result, balkanized state-by-state privacy regulation would lead all providers to tailor their practices nationwide to the most restrictive elements of the various state laws, irrespective of the balance that any given state may have struck between restrictions and permissions, and no matter how oblivious those laws may be to a careful cost-benefit analysis.

[10] *See* AT&T Response to Issue 2 (discussing importance of consumer data in media markets).

[11] *See*, *e.g.*, Sidley Austin LLP, *California Enacts Broad Privacy Laws Modeled on GDPR* (June 29, 2018), https://www.sidley.com/en/insights/newsupdates/2018/06/california-enacts-broad-privacy-laws-modeled-on-gdpr.

For that reason, these laws may well violate the dormant Commerce Clause, which requires states to balance their regulatory interests against the burden on interstate commerce and prohibits them from regulating activity occurring "wholly outside of the State's borders."[12] But the federal government should not await the outcome of multiyear litigation to restore consistency and predictability to the U.S. privacy framework. Instead, as AT&T and others have proposed, the Commission should work with Congress to enact federal legislation that reinforces the Commission's leadership role in this area and ensures national consistency in privacy policy.

[12] *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989); *see Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 180 (S.D.N.Y. 1997); *see also Am. Booksellers Found. v. Dean*, 342 F.3d 96, 103 (2d Cir. 2003); *ACLU v. Johnson*, 194 F.3d 1149, 1160-61 (10th Cir. 1999).