BEN RAY LUJÁN
NEW MEXICO

498 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-6621

United States Senate
WASHINGTON, DC 20510-3105

COMMITTEES:
COMMERCE, SCIENCE, AND TRANSPORTATION
CHAIR, COMMUNICATIONS, MEDIA, AND BROADBAND
AGRICULTURE, NUTRITION, AND FORESTRY
HEALTH, EDUCATION, LABOR, AND PENSIONS
INDIAN AFFAIRS
BUDGET

March 10, 2022

John T. Stankey
Chief Executive Officer
AT&T
208 South Akard Street
Dallas, TX 75202

Dear Mr. Stankey:

I write seeking information about your company's use and collection of customer data, and to urge you to commit to making meaningful changes to ensure that you are meeting consumers' privacy expectations.

As an Internet Service Provider (ISP), you are responsible for connecting American consumers to critical services such as healthcare, employment, and education. Our constituents are dependent upon your services to meet their most important obligations, and this reliance has grown as a consequence of the pandemic. Americans expect ISPs to protect their data, and your customers deserve your highest respect for their privacy. Nevertheless, I have become aware that ISPs are collecting, using, retaining, sharing, and profiting from Americans' private and sensitive information in a manner that may not meet their privacy expectations. This trend is accelerating as the telecommunications industry evolves into vertically-integrated platforms that provide internet, cable, content, distribution, advertising and analytics—allowing ISPs to track consumers and their behaviors across various platforms and devices.

On October 21, 2021, the Federal Trade Commission (FTC) released a report titled, "*A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*." This report highlighted a number of alarming trends related to the collection and use of consumer data. Among these concerns are:

- ISPs are amassing large databases of sensitive data, including geolocation, web-browsing history, and app-usage information;[1]

- ISPs' amalgamation and use of such data can lead to detailed consumer profiles and classifications, including by demographic characteristics, such as race, ethnicity, gender, and sexuality;[2]

[1] "A Look At What ISPs Know About You." U.S. Federal Trade Commission, October 21, 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
[2] *Id.*

- Sensitive information is often used for advertising purposes, either by the ISP, a parent company, or an affiliated ad network in ways that are opaque to the consumer;[3]

- User access and control over data collected by ISPs is often "illusory" with problematic and confusing interfaces that minimize the user's effective control;[4] and

- Privacy challenges permeating the advertising ecosystem are amplified by ISPs because many have access to consumers' internet traffic, know the identity of their subscribers, and can track them across websites, services, devices, and geographic locations.[5]

After reviewing documents from AT&T and other large ISPs, the FTC determined that ISPs *"access and control a much larger and broader cache of consumer data than ever before, without having to explain fully their purposes for such collection and use, much less whether such collection and use is good for consumers*."[6]

Not only do these seemingly ubiquitous data collection practices violate users' basic expectation of privacy, but they also unnecessarily expose users to risk through security failures and data breaches. Breaches are fairly prevalent in the telecommunications industry; over the past decade, ISPs such as AT&T, Verizon, T-Mobile, Charter, and Cox have all suffered data breaches, exposing the personal and sensitive data of millions of American consumers.[7] With millions of customers across the United States, AT&T's data security policies, practices, and failures affect a significant number of Americans.

Allegations of potentially deceptive and predatory data practices on a national scale must be taken seriously. I request that you provide detailed responses to the following questions below regarding AT&T's data collection, use, retention, and sharing policies and practices, including the policies and practices of each of its affiliates and subsidiaries. More importantly, I hope that you will reform your policies and practices to bring them into alignment with the expectations of American consumers.

1. Does AT&T ask its customers, or consumers generally, for their affirmative consent before collecting and retaining user data? If so, where and how is this consent

---

[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Nguyen, Nicole. "Hackers Could Gain Complete Access To Spectrum Customers' Accounts Through A Security Flaw." *Buzzfeed News,* August 17, 2018. https://www.buzzfeednews.com/article/nicolenguyen/spectrum-time-warner-cable-security-flaw
* Fitzgerald, Drew and Robert McMillan. "T-Mobile Hacker Who Stole Data on 50 Million Customers." *Wall Street Journal,* August 27, 2021. https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105
* Hope, Alicia. "Hackers in AT&T Communications Data Breach Impersonated Company's Support Agent to Access Customer Information." *CPO Magazine*, December 23, 2021. https://www.cpomagazine.com/cyber-security/hackers-in-cox-communications-data-breach-impersonated-companys-support-agent-to-access-customer-information/

obtained? Please provide examples of reports given to consumers, screenshots of consent windows, and guidance documents

   a. Does AT&T train its employees on a duty of care related to customer privacy? Please provide any guidance documents provided to employees.

2. What data does AT&T collect from its customers and consumers, and how does AT&T use that data?

   a. Please provide examples of any materials you provide to customers that explain to them their privacy rights and ability to opt out of data collection? Please provide any training materials to ISP employees and/or contractors on protecting customer privacy.

3. What is the process for a customer to opt-out of having their data collected, used, or sold across **all** AT&T products and services?

   a. Does AT&T train customer support personnel on how to instruct customers wishing to receive a report on their personal information or opt out of information collection? Please provide examples of guidance documents provided to personnel.

   b. What percent of your current customers complete all steps in this process?

   c. By completing this process, will your customers be able to opt out across all of their devices and services?

4. Does AT&T track and collect information regarding its customers' web-browsing history including URLs a user has visited, as well as associated metadata such as page title and time of visit? If so:

   a. Aside from any privacy choices AT&T provides to its customers and consumers, what external actions can consumers take to prevent AT&T from tracking their web-browsing activities?

   b. Does AT&T collect information about web-browsing activity when a user opts out of data collection through a browser-enabled Global Privacy Control? If so, please explain the reasons for doing so.

   c. Does AT&T collect information about its customers' web-browsing activities if they utilize a Virtual Private Network?

5. 47 U.S.C. 551 imposes obligations on "cable operators" to protect the personal information of subscribers to "cable services" and "other services" -- defined as any communication by wire or wireless. Please respond as follows:

   a. Are you a "cable operator," i.e., a provider of cable services, regardless of whether or not you also offer "other services" on a standalone basis?

   b. If yes, do you provide your subscribers with an annual report of personal information collected as required by Section 551(a). If so, please provide a sample copy of the most recent report, including the information collected and the purpose of such information collection.

c. If yes to question 5.a., do you require customers to waive their right to sue under 47 U.S.C. 551 and abide by mandatory arbitration instead?

d. Do you treat information obtained through a set-top-box or DRV as data subject to the protections of 47 U.S.C. 551. If not, why not? Do you distinguish between STB or DVRs that you rent to customers v. client-owned devices?

6. Does AT&T allow its customers and consumers to access and review all information collected about them?

    a. What does a typical report provided to customers or consumers look like?

    b. Does AT&T limit access rights based on the customer's or consumer's state of residence?

7. What steps do you take to comply with the Child Online Privacy Protection Act (COPPA)? Do you identify information collected from devices associated with children under 13?

    a. Do you co-mingle information collected on children's television programming viewing habits on a per-household basis -- either through STB or other means -- with information collected via broadband? If so, how do you treat this information related to requirements under COPPA?

8. What is the process by which a current or former AT&T customer or consumer can request that previously collected data be deleted?

    a. Does AT&T limit deletion rights based on the customer's or consumer's state of residence?

    b. How long does AT&T retain data collected by customers? Is this impacted if a user is no longer a AT&T customer?

    c. Does completing this process lead to AT&T and its affiliates retraining models that were created using or inferred from this data? If not, please describe what models remain in use and how long the data is continued to be used in those systems.

    d. Does completing this process lead to AT&T removing such data from backup storage? If not, please describe how long this data remains in backup storage.

9. Does AT&T sell or share any customer or consumer data with any affiliates or third parties, or provide products to third parties based on such data?

    a. What specific data does AT&T sell or share with any affiliates or third parties, and to what entity or entities?

    b. What steps, if any, does AT&T take to anonymize such data?

    c. What specific data does AT&T use to offer products to third parties based on such data?

    d. Does AT&T link Advertising IDs to individual devices? If so, how does AT&T ensure that third parties cannot link those Advertising IDs back to individual households or consumers?

e. Does AT&T offer customers a "Do Not Sell" or "Do Not Share" option, and if so, are such options available to all U.S. consumers?

10. Does AT&T or one of its affiliates share with, offer access to, or provide products to third parties based on data related to the race, ethnicity, gender, or sexuality of its customers? If so, please describe.
11. Please provide detailed information as to how AT&T collects and uses customer location, web-browsing, and app-usage data, and how long this sensitive data is retained.
    a. Does AT&T share with, offer access to, or provide products to third parties based on such data?
12. Does AT&T support legislation or formal rules that would set limits or standards on data retention, anonymization, distribution to third parties, and discrimination based upon users exercising control of their privacy? If so, please specify the rules or policies that AT&T supports.

More importantly, I request that AT&T thoroughly review its data collection, use, retention, and sharing policies and practices, and commit to making meaningful changes to ensure consumer expectations are met. If you are truly concerned about your customers' privacy, you will ensure that you collect your customers' personal and sensitive information with their informed consent.

I look forward to your response by April 27th, 2022 and thank you for your cooperation.

Sincerely,

Ben Ray Luján
United States Senator