DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

NTIA Request for Comment: Developing the Administration's Approach to Consumer Privacy

Docket No: 180821780-8780-01

COMMENTS OF AT&T SERVICES INC.

David Chorzempa
Bob Barber
David Lawson
AT&T Services, Inc.
1120 20th Street, NW
Suite 800
Washington, DC 20036
(202) 463-4172

November 9, 2018

(Submitted by email to privacyrfc2018@ntia.doc.gov)
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW Room 4725
Washington, DC 20230
Attn: Privacy RFC, Washington DC 20230

INTRODUCTION AND SUMMARY

Protecting our customers' privacy is a fundamental commitment at AT&T.[1] We understand the great responsibility that comes along with our customers' trust in sharing their data with us. Our privacy program, therefore, is based on a set of core principles that explain our commitments to transparency, respect, choice and control, and security. These principles are reflected in the AT&T Code of Business Conduct,[2] as well as our privacy policies.[3]

AT&T has therefore long supported federal privacy legislation that, consistent with these principles, provides strong protections for consumers and a flexible, level playing field for companies seeking to compete and innovate. Privacy and innovation are not mutually exclusive goals and we welcome the Administration's leadership in carving out a nationwide privacy policy that strikes the proper balance.

We also echo the RFC's conclusion that the "[t]he time is ripe" for the Administration to assert leadership in shaping a nationwide privacy policy.[4] As the recent Congressional privacy hearings demonstrated, there is broad and growing consensus about the need for a federal privacy law. The need for a nationwide privacy policy is driven, in the first instance, by a recognition that in today's data-driven world, it is more important than ever to maintain consumers' trust and enhance their control over their personal information. A consistent, nationwide privacy law is also needed to avoid the growing risk of a patchwork quilt of inconsistent privacy regulations at the state and federal level.

AT&T also concurs with the RFC's adoption of an outcome-based privacy approach, which represents the most effective way to achieve a flexible, risk-based privacy framework.

---

[1] AT&T Services Inc. submits these comments on behalf of itself and the other affiliates of AT&T Inc.
[2] https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf
[3] As an example, see AT&T's communications privacy policy: https://about.att.com/sites/privacy_policy,
[4] RFC, at 2.

Rigid, prescriptive mandates can harm consumers, stifle innovation and be quickly outpaced by technology and market changes. Below, we provide comment on the RFC's proposed "outcomes," as well as its proposed high-level goals for federal action. In particular, we support the RFC's goals of establishing a federal privacy law that: harmonizes the regulatory landscape; maintains flexibility to innovate; applies comprehensively on a technology-neutral basis; is risk-based; and is enforced by the Federal Trade Commission (FTC), the nation's leading privacy regulator. AT&T looks forward to working with the Administration and other stakeholders in crafting a federal privacy law that furthers these goals.

Comments on the RFC's "Goals" for Federal Action

AT&T supports federal legislation aimed at creating a unified regulatory regime for privacy, data security, and breach notification, building on the standards developed by the FTC. We agree with the Administration that a federal privacy law should harmonize the regulatory landscape and apply consistently to all private organizations that collect, use and share consumer data for commercial purposes. In a connected world, where individuals use multiple devices and services from different providers, the most effective way to protect consumers is through one set of rules which apply to the collection and use of consumer data. Privacy regulations that apply to only one set of technologies or one segment of industry players will create customer confusion and distort competition.

To create a harmonized federal privacy law, the Administration's approach should be founded on the principle that federal privacy legislation will apply comprehensively across all sectors, unless there is a strong justification for maintaining an existing sectoral privacy law. In particular, adoption of a comprehensive federal privacy law would render unnecessary the privacy provisions contained in the federal Communications Act. These dated regulations,

applicable only to traditional "telecommunications services," fail to reflect the convergence that has taken place in the communications sector. Consumers communicate using a myriad of companies and services, including web-based messaging and calling services that often are not governed by the requirements of the Communications Act. Consumers deserve and expect one set of privacy protections for their communications and online services that is based on the nature of the data collected and how it is used. To the extent that other sector-specific regulations are retained, they should be carefully targeted at the uses of personal data that are unique to the pertinent sector. For example, it may be appropriate for health care institutions to apply special protections to a certain category of protected health information, but they should also be subject to the same rules governing collection and use of other personal data that apply to edge providers, communications companies, equipment manufacturers, retailers, and others.

Consistent with the Administration's goal of reducing duplicative and contrary privacy requirements, a unified regulator should oversee the national privacy framework. The FTC is the clear choice for an enforcement authority: it has proven itself to be an aggressive cop on the beat, bringing more than 500 enforcement actions for privacy and data security violations.

Similarly, the Administration should seek to avoid a patchwork of inconsistent state laws that regulate privacy and data security. Differing state rules will confuse consumers, providing them uneven protections and potentially forcing them to navigate a complicated menu of diverging state-specific privacy choices and controls. Because data flows freely among many types of companies every time a user connects to the internet, regulation at the state level could have far-reaching unintended consequences that could disrupt the operation of the internet that consumers have come to expect. Consequently, legislation should preempt state privacy laws and provide consumers one set of consistent privacy protections, choices and controls.

The Administration's goals of harmonization and interoperability are related: by promoting a single federal framework for privacy, the Administration can demonstrate global leadership at a time when more of the United States' trading partners are adopting data protection laws. The United States' current, fragmented approach to privacy often gets lost in translation. Similarly, regulation of different privacy regimes by different federal agencies impedes companies in certain sectors from participating in the APEC Cross-Border Privacy Rules System, in which the FTC is the designated enforcement authority. Adoption of federal privacy legislation will provide U.S. trading partners with an alternative model, will help make the case for interoperability in those countries that have chosen their own approach, and will strengthen the APEC Cross-Border Privacy Rules System.[5]

Comments on Privacy Outcomes

AT&T supports the Administration's risk-based approach to privacy outcomes and believes it provides a roadmap for federal privacy legislation. This approach builds on the FTC's established privacy framework, which calibrates privacy protections and choices based on the sensitivity and use of consumer data, regardless of the company collecting the data or the technology used. The Administration should refine its framework by expressly recognizing that certain types of data collection and use may be subject to the consumer's implied consent, accompanied by proper notice. For example, AT&T uses network data not only to provide our voice, internet and video services, but also to improve network performance, to detect threats to network security, and to improve our products and services. The prevention of fraud and first-

[5] AT&T encourages the Administration to continue to promote interoperable cross-border privacy frameworks, based on industry best practices and providing risk-based accountability mechanisms. Agreements such as the APEC Cross-Border Privacy Rules (CBPR) System and the US-EU Privacy Shield are positive examples of frameworks that rely on internationally accepted data protection principles. We particularly welcome the United States-Mexico-Canada Agreement's chapter on Digital Trade and its promotion of the APEC CBPR System.

party marketing of services similarly fall into this category of uses.[6] In addition, the Administration should incorporate sensitivity and risk-management considerations directly into its privacy framework, particularly in the Transparency and Control outcomes.

AT&T also supports the Administration's goal of establishing a balanced privacy framework that provides legal clarity, protects consumer privacy, and allows companies to develop innovative new business models and technologies. As the Administration recognizes, the best way to achieve these goals is to establish a privacy framework that focuses on managing risk and protecting individuals from harm. For example, in its discussion of data minimization, the RFC recognizes that data collection, storage length, use, and sharing "should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm." However, the Administration also should include other relevant factors such as the benefits of responsible data use, the need to collect and use data for service delivery and other operational purposes, and legal requirements.

As the Administration recognizes, consumers benefit from responsible uses of data. Accordingly, legislation should affirmatively allow innovative uses of data, subject to effective safeguards. Rules and protections should be tailored to the sensitivity of the data and how it is used. For example, location data from mobile devices can provide valuable insights on traffic flows and use of public transportation when personally identifiable information is removed. Similarly, certain datasets can be used to train Artificial Intelligence and Machine Learning solutions, leading to innovations that reduce occupational hazards and inefficiencies.

AT&T also supports the RFC's proposed outcomes of Security, Risk Management, and Accountability. In particular, AT&T supports the Administration's position that data security

[6] FTC Report, *Protecting Consumer Privacy in An Era Of Rapid Change: Recommendations For Businesses and Policymakers*, (March 2012) (hereinafter, "2012 FTC Report"),at 36-48.

should be based on a reasonableness standard, calibrated to the level of risk. This is consistent with the FTC's approach to data security.[7] We agree that it is important for privacy legislation to include incentives for risk and outcome-based approaches.

The RFC also proposes outcomes of access and correction. ("Users should have qualified access [to] personal data that they have provided, and to rectify, complete, amend, or delete this data.")[8] The RFC makes clear that this access and ability to correct must be "reasonable given the context of the data flow" and "appropriate to the risk of privacy harm" (among other factors). In assessing reasonableness of any right to access or correction, the Administration should consider the costs, risks and benefits of any such requirements. The Administration should assess the actual benefit that access to data brings to consumers, the cybersecurity and fraud risks that any obligations might create, and the operational and compliance costs to businesses. Consistent with the reasonableness standard that the Administration recognizes, any access requirement should avoid requiring organizations to collect additional information from users to identify them or to catalogue, link, and retain data for longer than they would otherwise do. Any access requirement also must address verification, security and liability concerns related to providing access to users' personal information.

A U.S. privacy law should include a role for industry voluntary efforts, best practice codes, and multi-stakeholder initiatives, all of which drive privacy protections in ways that make sense for the providers and consumers of covered technologies. Voluntary privacy programs and standards developed through public-private collaboration could serve as safe harbors in legislation while enabling companies to adapt to rapidly changing technology and market

[7] 2012 FTC Report, 24-26.
[8] RFC, at 8.

developments. The NTIA's work to develop voluntary privacy guidelines has added value in the past and provides an example of the type of work that should be encouraged.

Privacy legislation should also recognize that governance practices such as the appointment of a Chief Privacy Officer, data governance policies, and the performance of privacy impact assessments represent good practices. The existence of such practices could serve as a tool to validate compliance with privacy law and policies and should be mitigating factors in any investigation into a company.

Conclusion

AT&T looks forward to working with the Administration and NTIA to establish a nationwide set of privacy protections that, consistent with the principles outlined above, provide consumers with strong and uniform safeguards and strengthen the FTC's position as the nation's leading privacy regulator.

Respectfully submitted,

/s/David Chorzempa

David Chorzempa
Bob Barber
David Lawson
AT&T Services, Inc.
1120 20th Street, NW
Suite 800
Washington, DC 20036
(202) 463-4172

November 9, 2018