Statement of Leonard Cali

AT&T Senior Vice President Global Public Policy

Hearing: "Examining Safeguards for Consumer Data Privacy"

Before the United States Senate Committee on Commerce, Science, and Transportation

September 26, 2018

Thank you Chairman Thune, Ranking Member Nelson, and Members of the Committee.

I am Leonard Cali, Senior Vice President Global Public Policy for AT&T. AT&T has a 140-year heritage of innovation that includes eight Nobel Prizes and 15,000 patents and pending patents worldwide. We employ nearly 220,000 Americans, representing all 50 states. Over the past five years we've invested $135 billion in the United States, more than any other public company. Without doubt, we are deeply invested in our country, our communities, our employees and our customers.

Protecting our customers' privacy is a fundamental commitment at AT&T, and we understand the great responsibility that comes along with our customers' trust in allowing AT&T to collect and use their data. On behalf of AT&T, I thank you for this opportunity to participate in the critical discussion concerning the future of U.S. privacy regulation.

While we've all been talking about privacy for years, today we stand at a critical juncture in that discussion. Perhaps for the first time, there is widespread agreement among industry, policy makers and many consumer groups of the need for a new and comprehensive federal privacy law. This consensus is driven by a recognition that in today's data-driven world, it is more important than ever to maintain consumers' trust and give them control over their personal information. Consumers rightly expect that consistent privacy protections will apply regardless of which app, device, service or company is collecting and using their personal information.

However, there is an increasing risk that we will end up with a patchwork quilt of inconsistent privacy regulations at the federal and state level, which will only serve to confuse consumers and stifle innovation. And there is a risk that regulators will fail to strike the right balance in addressing privacy by importing the European Union's overly regulatory privacy regime.

Now is the time for decisive Congressional leadership to establish a thoughtful and balanced national privacy framework. AT&T strongly supports federal privacy legislation that both protects consumers and allows for innovation. Such legislation would not only ensure that

consumer privacy rights are protected, but it would also provide consistent rules of the road across competing websites, content, devices and applications.

Of course, there are differing views on what should be in a national privacy law. We expect that, and we will actively participate in discussions to reach consensus on a forward-looking framework. Fortunately, there is an emerging, wide-spread (and growing) consensus around basic privacy principles that should be the starting point for federal legislation.

Specifically, there is growing consensus that policy makers should design a national privacy law that builds upon the FTC's successful privacy framework and that*:*

- ✓ ***Establishes consistent nationwide privacy protections for consumers.*** Privacy protections should be based on the sensitivity and use of consumers' information, not by the type of entity collecting it. Legislation should preempt state privacy laws and provide consumers one set of consistent privacy protections, choices and controls.

- ✓ ***Avoids duplication and inconsistent requirements.*** To accomplish this, the federal privacy law can be overseen exclusively by the FTC, an agency with decades of experience regulating privacy practices.

- ✓ ***Respects customer privacy choices, requiring companies to be transparent about their privacy practices.*** Legislation should require companies to have a privacy policy that gives consumers clear and comprehensible information about the categories of data that are being collected, how consumer data is used and the types of third parties with whom data may be shared. Customers should have easy-to-understand privacy choices. Legislation should define sensitive and non-sensitive data and its appropriate treatment (e.g., opt-in/out) consistent with the FTC's established framework.

- ✓ ***Allows innovative, consumer-friendly uses of data that enhance their lives, subject to appropriate protections***. Strong privacy protections and innovation are not mutually exclusive goals. Legislation should affirmatively allow innovative uses of data, subject to effective safeguards. Consumers benefit from data-driven innovations that deliver high-quality services, reduce their costs, enhance their lives, and develop new, improved products.

- ✓ ***Requires companies to take reasonable steps to protect consumer data***. Data security and breach-notification legislation should establish a reasonable, flexible and consistent national framework.

- ✓ ***Supports collaborative public-private partnerships.*** Voluntary privacy programs and standards developed through public-private collaboration could serve as a safe harbor in legislation while enabling companies to adapt to rapidly changing technology and market developments. In particular, we welcome the Administration's efforts, though NTIA, to

work with stakeholders to establish a set of privacy principles that would provide an alternative to the European Union's prescriptive approach and be used in federal legislation.

AT&T is actively engaged with industry, consumer stakeholders and policymakers to build agreement around these principles, and we look forward to working with Congress to pass privacy legislation around them.

AT&T's Commitment to Customer Privacy

Protecting our customers' privacy and securing their information is a fundamental commitment at AT&T. Like you, we believe that consumers deserve strong privacy and security protections that give them control over how their information is used and shared, as well as confidence that their information will be protected.

We believe that customers should have choices and control about how their information is used by AT&T and shared with other companies. This includes opting in or out of some programs, setting privacy preferences, and unsubscribing from marketing emails and letters.

We keep customers' information safe using encryption or other appropriate security controls. All of our employees are subject to the AT&T Code of Business Conduct (COBC) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business - including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of our customers' records. We take this seriously. Any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action, including dismissal.

To the extent AT&T has records in its custody or control that are subject to a mandatory legal obligation to produce the records, AT&T will comply with that legal requirement. We ensure that government requests are valid, and that our responses comply with the law and our own policies. Although we comply with legitimate government requests for customer communications, we do so only to the extent required by law.

In addition, since 2014, AT&T has issued a Transparency Report that identifies the number and types of legal demands for customer information received in criminal, civil, and national security matters, as well as emergency situations. It also includes international demands related to global operations for customer information and website blocking. The Transparency Report is available in Spanish, to better inform our Mexican and Latin American customers.

AT&T is dedicated to being a leader in protecting customer privacy and providing our customers security, transparency, respect, choice and control.

The Need for Federal Privacy Legislation

For decades, the FTC's privacy regime has provided a predictable and technology neutral approach to privacy that focuses on customer transparency and consumer choice. The FTC's privacy framework has provided customers strong privacy protections, while allowing companies flexibility to innovate. By choosing this framework, as opposed to prescriptive requirements, the FTC has been able to keep pace with rapidly evolving technology and markets. Overly prescriptive prohibitions, in contrast, can limit the consumer benefits that come from innovation.

The FTC has also been an aggressive cop on the beat. It has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major internet and telecommunications companies.

As you know, in May 2018, the European Union's General Data Protection Regulation (GDPR) went into effect.[1] Some argued that the United States and other countries should quickly import GDPR. One month later, in June 2018, California enacted its Consumer Privacy Act of 2018 (AB 375), which applies to companies doing business in California. While the California law is different in many respects from GDPR, like GDPR, it applies its requirements to essentially all companies that collect data. We support uniform application of the law. However, also like GDPR, many of the California requirements are highly prescriptive, and ambiguities and errors in its language leave open serious questions about how it will be enforced and interpreted.[2] For both the California law and GDPR, there also remain serious questions about their ultimate impact on consumers, desirable new technologies like AI, and the marketplace.

But I am not here to provide Congress a laundry list of the possible negative implications of the California law. The more important point for Congress and this Committee to understand is that the passage of the California law and interest of other states in legislation raise the

[1] On the one hand, GDPR is a consistent framework, applicable to all companies that collect and use European sensitive data. On the other hand, it is still very much an open question how GDPR will be interpreted and enforced by European regulators. Even though AT&T does not offer consumer-facing services in Europe, we have spent significant time and resources ensuring our compliance with GDPR, having enhanced our documentation, procedures and technologies to ensure our compliance, where required.

[2] In particular, the law grants the state Attorney General broad rulemaking authority.

imminent risk that companies and consumers will soon face a patchwork of inconsistent state privacy laws. Indeed, twenty-six state privacy bills were introduced this year alone, and the passage of the California law will no doubt stimulate more state legislative action. Some states may follow the more-regulatory California/GDPR route, while other states may adopt a more flexible approach, similar to the FTC's framework. Regardless, what is certain is that future state privacy laws will differ in significant ways.

A patchwork of differing state privacy law will confuse consumers, providing them uneven protections and potentially forcing them to navigate a complicated menu of diverging state-specific privacy choices and controls. Imagine a customer trying to understand why she might be required to opt in to a particular privacy setting in Maryland, while being required to opt out of that setting in Virginia. Or why certain data is subject to heightened protections in Florida, but not South Dakota. And in a world where more and more communications and commerce occur on mobile devices, will legal requirements be determined by locations of those devices at any given time, the telephone numbers or IP addresses assigned to those devices, or the principal residences of the owners of those devices? While consumer protections often vary by state in our federal system, these variations make less sense when data moves freely, without regard to state borders and at the speed of a light. Consumers deserve a single set of privacy rules that they can understand and rely upon across the nation.

Further, while each state may adopt its own set of privacy permissions and restrictions, providers struggling with compliance may have no choice but to adopt the most restrictive elements of each state's law, given the impracticability of complying with multiple state rules when offering mobile and internet services that, by their nature, have no state boundaries. The result may be a more restrictive privacy framework than any state intended with less innovation, investment and consumer welfare than any state anticipated.

Differing privacy laws also raise business compliance costs. For example, compliance with the California law will require extensive changes to customer-facing policies and privacy controls, as well as internal systems and business processes. These challenges and resulting costs would be exponentially greater were states to adopt laws with different requirements.

As states adopt privacy laws that clash with the FTC's long-standing framework, the FTC's position as the nation's leading privacy regulator will inevitably be eroded. In short, federal legislation is necessary to codify a privacy law that builds on and strengthens the FTC's role as the nation's preeminent privacy "cop on the beat."

Conclusion

AT&T looks forward to working with this Committee and Congress 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.