STATEMENT OF DOROTHY ATTWOOD
SENIOR VICE PRESIDENT, PUBLIC POLICY & CHIEF PRIVACY OFFICER
AT&T INC.

BEFORE:

UNITED STATES SENATE
COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

HEARING: CONSUMER ONLINE PRIVACY

July 27, 2010

Thank you, Chairman Rockefeller and Ranking Member Hutchison, for providing AT&T with another opportunity to participate in a thoughtful examination of how consumer information is shared in the online world and what role those doing the sharing have in creating a comprehensive, consumer-centric approach to online privacy.

Background

For those of us who access the Internet – perhaps 2 billion people worldwide – the online possibilities are boundless. It is a venue for almost every type of human interaction or transaction. We can connect with old friends and meet new ones, purchase every imaginable good or service, find answers to almost every question, do business with our bank, exchange health information with our doctor, access libraries, get services from the government, communicate with political leaders, organize social events, mobilize a community, or facilitate disaster recovery. From love to money, we search for it on the Web.

Yet, for all that we already do on the Internet, we have only glimpsed the possibilities. Digital signals from the earthquake rubble of Haiti enabled relief workers to locate survivors, direct food and medicine delivery, and map transportation options to expedite emergency efforts. GPS data from wireless networks can be assembled to observe the flow of people, services, and cars so that urban planners can build more livable cities. Electric grids and other infrastructure

can be organized and managed for efficiency thanks to the instant exchange of information over broadband networks. Businesses can cut costs by storing data in the cloud or use Web data to create tailored services for their customers.

But these advances are not guaranteed. At its heart, beyond the computing power, software and backbone networks, the Internet runs on information shared willingly among its users. This sharing requires confidence and trust that the personal information we provide is safe from abuse and will be used in ways that we approve. Even in a digital world, most people continue to value their privacy – although they may approach their privacy differently from the way they did before the Internet entered our lives. Thus, the continued growth of the Internet, and the positive social and economic benefits of that growth, are dependent upon earning, maintaining and preserving the confidence and trust of Internet users worldwide that their information is being shared in the way they intend.

Online Privacy: Where We Started and What We've Learned

Two years ago when I appeared before this Committee, I articulated the four pillars of AT&T's approach to our customers' privacy: transparency, consumer control, privacy protection and consumer value – all designed to create and preserve our customers' trust. We urged then, and we continue to believe, that these principles can be the foundation of a consistent regime applicable to all entities in the online ecosystem that inspires trust in users worldwide. At the same time we have learned through practical experience that, as good as the various individual privacy efforts and consensus best practices are, more concerted activity is needed across the entire Internet ecosystem. Consumers have a consistent set of expectations about their privacy wherever they go online, regardless of which portals they enter and the number of places they visit. In light of this, there ought to be consistent standards to meet those expectations

throughout the Internet ecosystem. We are even more convinced today that the changing Internet marketplace requires a privacy regime that moves beyond the current patchwork of ad hoc practices for providing notice and obtaining consent to an interoperable framework – one in which a customer's consents and preferences are honored throughout the Internet ecosystem.

Transparency and Customer Control

Since I last testified before this Committee, AT&T and others in the industry have developed a variety of innovative solutions that are the essential steppingstones to the next phase in the evolution of online privacy practices. For example, last summer AT&T, through an open and inclusive roll-out process that specifically incorporated a 45-day preview period and comments from our customers, adopted a new, simplified, plain language privacy policy that applies to all AT&T services. Companies everywhere have come to the realization that privacy policies need to be readable and understandable, and we're especially proud of the way we have implemented transparency and control at the very outset of our customer relationship.

In consolidating 17 separate written company privacy policies into a single, unified, easy-to-understand AT&T privacy policy, we recognized that there was no reason for treating AT&T Mobility customer relationships different from AT&T U-Verse customer relationships or AT&T Long Distance customer relationships -- and on down the line. Our customer's privacy expectations are the same regardless of the nature, let alone legacy regulatory classifications, of the services they purchase from us. Our experience as the leading communications company in America with a diverse wireless, wireline, and video portfolio, combined with our experience as a major online advertiser, a website publisher, and Internet service provider, helped us to appreciate that customers not only want a clear understanding of how they can control the sharing of their personal information, but they want their expectations honored consistently

regardless of what they do or where they go online. Bottom line, our Internet users want their privacy to be respected, and regard the information they share as theirs to govern.

AT&T's Innovation Through Privacy By Design

AT&T has also emphasized bringing privacy-enhancing technologies to consumers through the roll out of new products, including the online advertising space, where we have actively improved our transparency as an advertiser and publisher. We apply these principles at the start of product development and strategy by embedding transparency and control features into the product itself, not as an add-on or afterthought. We have added an "advertising choices" link on our "YP.com" yellow pages website that explains how and where we use what consumers search for on YP.com to target ads to users elsewhere on the Internet. This link also explains to users how to opt-out as well as how to discover the "interest" category – or profile manager – that we have developed, and permits users to modify that profile. Essentially, we offer customers the ability to view and edit the interest categories that we have associated with them and a simple process for them to choose not to be targeted in this way.

We have also launched an advertisement-supported social networking "recommender" site that we call "Buzz.com." Buzz.com combines aspects of social networking with local search, so that users can search local listings for a restaurant or a doctor and get recommendations from people that users know as well as from other Buzz.com users in general. Because the site is based upon information sharing, users cannot join the site without first establishing their privacy preferences. We provide notice to our customers beyond the official notice in the general privacy policy through a separate link entitled "Things you should know about how your information is shared on buzz.com." Indeed, we call it what is – information sharing not privacy – and go the extra mile to explain the details of the information sharing that

takes place. Specifically, we give our customers a number of choices that permit them to control the scope and extent of that information sharing during the initial registration process. We explain the different levels of information sharing in plain language and make clear that "anonymous" postings may not always stay that way, so that customers are not surprised down the road.

We believe these new capabilities not only represent an example of an industry best practice but also demonstrate that technological innovations can and do occur when firms embrace privacy by design – that is, when they design their customer facing offerings in a way that provides both transparency and meaningful tools to control whether and how their information is shared. For example, providers of location-based services have demonstrated that functional integration of customer permissions can spur the acceptance of these new services. Indeed, location-based services continue to grow and incorporate consumer permission processes into the sign up and use of the service itself. Importantly, CTIA has established best practices and guidelines for entities that provide location based services, including mobile operators, device manufacturers and applications developers that encourage industry-wide adoption of robust permission-based approaches as well as further innovations in privacy enhancing technologies.

Ecosystem Evolution of Online Privacy

Other industry groups have likewise come together to make important progress in standardizing, clarifying and simplifying the user's understanding and control of how their online experience is used for targeted advertising. For example, the Internet Advertising Bureau has unified the presentation of the NAI opt-out tool, and adopted an icon that will be used throughout the industry to increase transparency. AT&T is helping to build on this momentum

by working with Better Advertising to trial inclusion of the icon in certain of its ads, and by participating with TRUSTe on its behavioral advertising pilot seal program, which is designed to give customers confidence that their privacy trust is well placed. All of these steps represent important progress toward an ecosystem-wide approach based on customer engagement and the ultimate goal of giving customers the tools necessary to manage their online identity in one place, at one time, so that their preferences are respected wherever they travel on the Internet.

Building on this progress, we believe the industry, which has innovation in its very DNA, should press even further and develop a trust framework that enables the "interoperability of permissions." With this framework, entities throughout the Internet ecosystem could cooperate in a "back-office" way to honor the information sharing preferences of the customer. Such an approach can be likened to the existing process in banking, where consumers initiating fund transactions are not involved in the details of when and how the automated clearing houses handle the actual money transfers, but have every confidence that their money goes when and where they intend.

Ground-breaking work on such a trust based ecosystem is already underway. For example, a draft White House report made public in June maps out a framework for "trusted identities in cyberspace" and suggests a "user-centric model" based around individual preferences. Private entities are working on user-centric identity management tools ("IDM tools") that give consumers the opportunity to decide how much of their identity to reveal, when and to whom. The two most prominent IDM tools, "OpenID" and "Information Cards" put the user in control of identity-based interactions and potentially provide a uniform user-driven approach to data collection and use. In addition, private companies are developing other technologies – browser controls, widgets and downloads – that will enable users to set and

manage their privacy preferences. Firefox, for example, offers consumers a browser add-on that protects and automatically updates opt-out settings, including flash cookie controls. Tracker Watcher, another browser add-on, offers users a way of identifying companies that track consumer online behaviors.

These tools have the potential to improve users' online experience and enhance privacy. For example, IDM tools have the potential to be used to establish privacy preferences, minimize the disclosure of personal, identifying information, enhance user choice about the nature and amount of data to be shared, and expand users' say regarding the timing and manner of updating and withdrawing data. Such tools also could provide websites with a secure, standardized means of authenticating users.

Conclusion

It is easy to misinterpret the ease with which personal information is shared to mean that those sharing information are unconcerned about privacy. We don't think that is accurate. Privacy is a more multi-dimensional idea on the Internet. It is not the inverse of security, but instead is about the creation and maintenance of an online identity – and consumers want control over how they present themselves online, and with whom and where they share information. We have seen time and again that users choosing to share their information is entirely different from companies choosing to share information about their users.

Policy makers and industry should work together to promote an Internet that promotes permission-based, user-driven sharing of information in a safe and secure environment. It is beyond question that consumer information is the bedrock of online advertising, and that online advertising fuels a great deal of the investment and innovation across a wide range of Internet activities, providing the revenue that enables consumers to continue to enjoy a myriad of free and

discounted services. Indeed, website publishers continue to make most of their money from advertising, which in turn funds the breadth and diversity of today's Internet content and information that is, in most cases, made available to consumers for free. At the same time, the lack of consumer trust in the Internet threatens to undermine the American economy. So we are back to the fundamental bedrock issue of how to preserve consumer confidence and trust in the Internet. Working together, government and industry must take the bold step of moving beyond a balkanized system of notice and consent regimes that seem more about the entities that are collecting consumer information than the rights of consumers in controlling that information. By doing so, we can maintain the consumer trust and confidence that will keep the economic engine of the Internet running through successive decades of innovation.