Bruce R. Byrd
Vice President and
General Counsel-Washington
AT&T Services, Inc.
1133 21st Street NW – Suite 900
Washington, DC 20036

T: 202-463-4148
F: 202-463-8066
C: 202-286-2676
bruce.byrd@att.com

DRAFT – FOR DISCUSSION PURPOSES ONLY

December 21, 2009

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex P2)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Dear Sir/Madam:

Re: Comments of AT&T Inc. – Privacy Roundtables Project No. P095416

AT&T Inc., on behalf of itself and its affiliates ("AT&T"), respectfully submits these comments in connection with the Commission's planned second Privacy Roundtable.

The Commission's first roundtable, and the comments surrounding it, confirm that changes in technology and business models have fundamentally expanded the scope and magnitude of online data collected and used for commercial purposes. This paradigm shift not only poses great promise for the online environment, but also creates novel challenges to maintaining the sanctity of customer information and ensuring ultimate customer control over the Internet experience. As AT&T posited in the first round of comments, these challenges must be met with an equally novel policy and legal framework.

But law and policy are just components of a more comprehensive solution. Just as technology evolution is the catalyst for these tectonic shifts in the collection and use of online data, so too can technology innovation enable greater transparency and consumer control.[1] One particular form of emerging technology that could form the basis of truly enhanced consumer privacy online warrants the Commission's attention: user-centric identity management or "IDM." IDM tools have the potential to improve both the security and privacy of the Internet experience by allowing consumers to choose how much of their identity to reveal, when and to whom.

[1] As AT&T explained in its initial comments, the Internet advertising industry is already tapping helpful technologies. For instance, providing notice in or around ads themselves, as was incorporated into the IAB/DMA/ANA Self Regulatory Principles, can be seen as a way to make targeted advertising practices more transparent to users by giving them immediate, understandable and useful information about why they received certain types of ads and what options they have in response. The Future of Privacy Forum has garnered industry support and input for the development of possible ad label icons, and is testing these labels with consumers. TRUSTe is also looking at ways it can use ad labeling and the TRUSTe seal to increase transparency.

The two most prominent IDM tools are "OpenID" and "Information Cards." OpenID is a Web registration and single sign-on protocol that lets users register and log on to OpenID-enabled websites using their chosen OpenID identifier. With OpenID, a user can operate her own OpenID service (such as a blog), or she can use the services of a third-party OpenID provider (for example, most major Web portals, such as AOL, Google, and Yahoo!, now offer OpenID service). One key advantage of OpenID is that it requires no client-side software—it works with any standard Internet browser. OpenID is a community-developed open standard hosted by the non-profit OpenID Foundation.

Information Cards are a new approach to Internet-scale digital identity in which various aspects of a user's identity, whether self-created or established by third-party identity providers (e.g., employer, financial institution, school, government agency, etc.) are uniformly represented as visual "cards" in a software application called a card selector. Cards can contain information you may commonly share with a website, like name, address, interest information, etc., and can contain data relevant to advertisers and retailers, such as loyalty club membership information or interest profile information. The cards themselves may be stored on the same computer as the card selector, on a mobile device, or "in the cloud." Cards may be exchanged with websites using a variety of protocols and formats. All card selectors support at least the IMI protocol developed by the OASIS IMI TC 7, however, Information Cards are now being adapted to other protocols as well (including OpenID). Information Card technology is developed and promoted by the non-profit Information Card Foundation.

OpenID and Information Cards are often called "user-centric" or "user-driven" identity technologies because they can put the user in control of all identity-based interactions. The industry should therefore explore the potential of this technology to provide a uniform user-driven approach to data collection and use more generally, including with respect to the kinds of information generally valuable to advertisers. The potential benefits of such an approach are manifold:

- These tools offer websites a secure, standardized means of authenticating users.

- These tools also promise websites and advertisers a uniform way to access a user's privacy preferences, as well as other information about the user that would allow for personalization of the Internet experience.

- At the same time, users have the potential to control all identity-based interactions and the login becomes a "one-click" experience.

- And, most importantly, IDM can potentially increase consumer privacy by offering –
    - a single place to establish privacy preferences,
    - the ability to use pseudonyms,

- the possibility of minimum disclosure of personal, identifying information, and
- the promise of consumer choice regarding the nature and amount of data to be shared, when it will be shared, and the timing and manner of updating and withdrawing data.

Indeed, as the Commission moves toward conducting more of its own business on the web, it might explore the implementation of Information Card, OpenID or similar user-centric IDM technologies at Commission sites. In doing so, the Commission would provide momentum for the development and deployment of these technologies by private industry.

Further in the realm of game-changing technology innovations, we encourage the Commission to focus attention on the benefits and implications of cloud computing. While the term "cloud computing" has been used in various contexts to describe a variety of different services and capabilities, AT&T understands that term generally to refer to business models under which the provision of data storage, processing, and related functions are performed by a network operator inside a network, rather than by end users inside their customer premises equipment on the "edges" of the network. Although this approach is not new – AT&T and others have been providing such network-based managed services for years – cloud computing has been growing in importance in recent years, in large part because of the widespread deployment of reliable broadband services to consumers and businesses. Both businesses and consumers are increasingly choosing to obtain computing functions remotely rather than purchasing, managing and maintaining additional computer hardware and software themselves. Many customers are finding that cloud computing has the potential to improve the efficiency of businesses, as well as to meet other core objectives such as to enhance the delivery of health care and other services, to improve the environment, and to benefit consumers and the nation in myriad other ways.

For many customers, cloud computing can offer a number of advantages over reliance on on-site computers, as is evidenced by increasing consumer adoption of cloud-based services, but, at a minimum, it provides another choice in an expanding digital ecosystem for how users access, manipulate, utilize and personalize data services. Cloud computing relies on large-scale, shared computing resources, which means that it can be dynamically provided on demand and is quickly scalable. It relieves customers of the need to purchase extensive computing equipment and to manage the complexities of computer technology; indeed, economies of scale within the network can often allow cloud computing providers to offer much more powerful and flexible computer functions more cheaply than if the end-user were to attempt to piece together such computer resources on its own. Cloud computing also transfers much of the burden of ensuring reliability and security to the network cloud provider; services like anti-virus protection installed on customer premises equipment become a last line of defense, rather than the only line of defense. And, cloud computing is typically accessible anywhere on the globe from any device with the appropriate type of connection (such as Internet access).

Notably, network providers are only a subset of the companies in the Internet ecosystem that offer cloud computing services. Today, companies like Google, Amazon, Microsoft, and Yahoo! provide cloud computing services over their own integrated, managed, and interconnected *networks* of routers, servers and links. Indeed, some, like Google, operate such computing networks on a massive scale that rivals the carriers' networks. One recent study found that 30 "hyper giant" companies, including Google and Microsoft account for 30 percent of all Internet traffic globally.[2]

Thus, cloud computing is changing in dramatic ways the manner in which the full range of Internet consumers access computing capabilities, but it also raises new challenges for ensuring privacy and security. As in all Internet contexts, cloud providers must strive for appropriate transparency of their practices on collection, storage, and use of data (*e.g.*, whether the cloud provider retains data after the customer no longer purchases the service or uses the data for advertising purposes), customer control of data stored in the cloud (*e.g.*, giving the customer the option to remove data and control its use), and security. Cloud services present unique challenges, however, because the data is not under the direct control of the user, and cloud resources, whether processing or storage, are not restricted by national boundaries. There are a number of industry self-regulatory initiatives under way that have begun to develop the best practices necessary to ensure a responsible, secure, open and interoperable marketplace.[3] Nonetheless, the confluence of the growing use of cloud computing, the widespread availability of such services from varied players in the Internet and broadband realm, and the unique privacy implications of the technology calls for a sustained commitment by industry and regulators to employ a holistic privacy framework that protects consumer interests and encourages innovation.

AT&T appreciates the Commission's willingness to open a dialogue on these issues, and it looks forward to participating in the second Roundtable discussion.

Sincerely,

_____/S/_____

Bruce R. Byrd

---

[2] *See* Arbor Networks, "Two Year Study of Global Internet Traffic Will Be Presented at NANOG47," www.arbornetworks.com (October 13, 2009) ("Out of the 40,000 routed end sites in the Internet, 30 large companies – 'hyper giants' like Limelight, Facebook, Google, Microsoft, and You Tube – now generate and consume a disproportionate 30% of all Internet traffic").

[3] These include the Open Cloud Manifesto (signed by AT&T and many others), the Cloud Computing Interoperability Forum ("CCIF"), and the Enterprise Cloud Buyers Council.