

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
Public Notice #29, Comments)	GN Docket Nos.09-47, 09-51, 09-137
Sought on Privacy Issues Raised)	
By the Center for Democracy)	
And Technology)	

COMMENTS – NBP PUBLIC NOTICE #29

AT&T Inc., on behalf of its affiliates, submits these comments in response to the privacy issues raised by the Center for Democracy and Technology (“CDT”).

CDT raises a number of issues and questions that center on the use and protection of consumer information and privacy in the broadband context. As a threshold matter, AT&T has explained in numerous proceedings before this Commission and the Federal Trade Commission (“FTC”) that consumer privacy and data security must play a central role in the National Broadband Plan. Consumers increasingly rely on broadband services for everyday transactions – banking, shopping, accessing electronic health records, engaging in job training and education – and in these contexts choose to share an unprecedented amount of personal information with trusted parties. As opportunities for collection and use of consumer information will only increase, consumers must feel confident about the use and security of their data online. All stakeholders in the Internet ecosystem – search engines, application providers, network providers, advertisers, equipment providers, publishers, email providers, and others – accordingly must work together to develop and implement privacy policies that protect consumers, while ensuring that consumers continue to reap the benefits associated with the expansion of online services and technology innovation.

Similarly, all government agencies concerned about privacy must work together to develop a coordinated approach to oversight of online privacy. Today, there are multiple efforts underway across the federal government to examine online privacy. For example, in addition to this inquiry, the FTC is actively conducting workshops to explore various issues related to online privacy and the best way to protect consumers, NTIA has formed a team to examine online privacy, and OMB has solicited comment on how data collection and use with respect to government online services should be handled.

As a result of these multiple government efforts, there is significant work underway to better understand privacy issues in an evolving broadband marketplace. From a regulatory perspective, the FTC in particular has taken the helm¹ on these issues and has held and continues to hold workshops with consumer groups and industry stakeholders to understand the gamut of privacy issues involving the collection and use of consumer data online. At these workshops the FTC is exploring the privacy challenges posed by the vast array of 21st century technology and businesses that collect and use consumer data. These workshops build on the FTC's adoption of a self-regulatory model for online behavioral advertising, which focus on increasing transparency and consumer control.

In adopting this model in its February 2009 Staff Report on online targeted advertising practices, the FTC reaffirmed its support for self-regulation as the best means of addressing "evolving online business models"² and the explosion in the types, amounts, and uses of information these models have created. Therein, the FTC recognized that government can play a meaningful role in shaping public policy on these

¹ The Chairman of the FCC has recognized that the FCC has little jurisdiction over privacy issues. See BusinessWeek, "A Chat with FCC Chief Genachowski, FCC Chairman Julius Genachowski on broadband access, net neutrality, a spectrum gap, innovation, competition, and consumer empowerment," October 26, 2009.

² FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising*, at 23 n.51 (Feb. 2009).

privacy issues and appropriately provided the industry guidance in developing more effective models to ensure the safety and security of consumers navigating ad-supported Internet content. To that end, the FTC urged businesses to honor four principles: (1) transparency and consumer control, (2) security and limited retention, (3) affirmative express consent for new uses of data, and (4) affirmative express consent for collection of “sensitive” data, such as financial information.³

In response to the FTC’s self-regulatory guidelines, the industry took action. The Network Advertising Initiative, a cooperative of online advertising networks, issued modifications to their binding member rules governing notice and choice for consumers and retention and security of consumer data.⁴ Similarly, the Interactive Advertising Bureau, a trade group whose members are responsible for selling 86 percent of all online advertising in the United States, partnered with the Direct Marketing Association, Better Business Bureau, and other advertising groups to develop a “cross sector set of privacy principles for online behavioral advertising in order to respond to the challenge issued [by the FTC] for comprehensive industry self regulation.”⁵ In response to the heightened interest in privacy protection, individual companies have also proactively made changes to their privacy policies to better engage consumers and improve transparency and control. AT&T, for example, consistent with the FTC’s recommended privacy principles adopted the following four core principles which, if implemented across the Internet ecosystem, would significantly advance consumer privacy:

³ *Id.* at 45-47.

⁴ Network Advertising Initiative, *The NAI Releases the Updated 2008 NAI Principles*, http://www.networkadvertising.org/networks/principles_comments.asp.

⁵ Interactive Advertising Bureau, Press Release, Key Advertising Groups Committed to Strong Industry Self-Regulation and the Development of Privacy Guidelines for Online Behavioral Advertising Data Use and collection (Feb., 12, 2009).

- (1) Transparency: Consumers must have full and complete notice of what information will be used, and how it will be protected.
- (2) Consumer Control: Consumers must have easily understood tools that will allow them to exercise meaningful consent. Consumer information should not be used for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of his/her information.
- (3) Privacy Protection: The privacy of consumers and their personal information must be vigorously protected, and sufficient technology must be deployed to guard against unauthorized access to consumer information.
- (4) Consumer Value: Collection and use of consumer data should be designed to increase consumer value, both by offering better and more innovative services and by allowing users to more fully customize and differentiate their Internet experience.

In short, regulators and industry stakeholders recognize that basic consumer privacy protections must play a key role in the development of broadband services, and that the evolution of online business models calls for a concurrent evolution in approaches to privacy protection, away from traditional models of notice and consent to a model that focuses on customer engagement in the use and sharing of their information. For its part, the Commission should ensure that the National Broadband Plan endorses the work that the FTC, other agencies and industry are doing, and encourages commitment on behalf of all internet-related industries to practices that will enhance consumer privacy and increase consumers' understanding about and control over use of their personal data online.

Below, AT&T generally responds to issues raised by CDT in the following areas: (1) Meeting Consumer Expectations of Privacy, (2) Building Privacy by Design, and (3) Third-Party Applications.

Meeting Consumer Expectations of Privacy

CDT asks what principles should be considered by the Commission and industry to meet consumer expectations of privacy.⁶

As more and more of our personal and business lives are conducted electronically and online, consumers have made it quite clear that privacy issues are important to them, and could well be a key determinant of success in the marketplace.⁷ For its part, the Commission can use the National Broadband Plan as a vehicle to encourage industry multi-stakeholder collaboration in the development and implementation of a self-regulatory model that employs the above-articulated four core privacy principles. Just as certain segments of the Internet ecosystem – namely the online advertising industry – have begun to implement these key privacy principles, *all* industry segments that collect and use consumer data online must follow suit and establish best practices regarding consumer privacy.

Building Privacy by Design

CDT asks whether there are ways to further “promote the development of technologies that protect privacy as they also utilize data.”⁸ The answer is obviously yes. As we noted in our comments to the FTC, more interactive forms of customer engagement must be part of the evolution of privacy practices – and, in order to be effective, those tools must be designed as an integral attribute of the online experience, providing demonstrable value to the customer.⁹

⁶ CDT Letter at 2.

⁷ *See, e.g.*, Reuters, Competitive Crunch and Convergence in Communications Marketplace Fueling Increased Customer Churn, Testing Loyalty (August 3, 2009), www.reuters.com.

⁸ *Id.*

⁹ Comments of AT&T Inc. – Privacy Roundtables Project No. P095416, filed November 9, 2009.

That evolution is well underway. Today, there are a number of technologies – browser controls, widgets and downloads – that offer consumers the ability 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.¹⁰ Tracker Watcher, another browser add-on, offers consumers a way of identifying companies that track consumer online behaviors.¹¹ Further, a two-click opt-out wizard is available to consumers that allows them to “opt-out completely or selectively from up to 106 networks based on their policy preferences.”¹² These technologies provide numerous privacy benefits to consumers, but alone are not sufficient to give consumers the tools they need to set and manage their privacy preferences.

AT&T fully supports the further development of user-centric identity management tools (“IDM tools”). IDM tools are an emerging technology that can enhance consumer privacy online by giving consumers the ability to determine how much of their identity to reveal, when and to whom. As AT&T detailed in its December 21, 2009 comments to the FTC’s Privacy Roundtables Project,¹³ the two most prominent IDM tools, “OpenID”¹⁴ and “Information Cards”¹⁵ put the user in control of all identity-based

¹⁰ PrivacyChoice.org Comments, “Analysis of Ad-Targeting Privacy Policies and Practices,” Federal Trade Commission Exploring Privacy Roundtable Series, December 4, 2009.

¹¹ *Id.*

¹² *Id.*

¹³ Comments of AT&T Inc. – Privacy Roundtables Project No. P095416, filed Dec. 21, 2009.

¹⁴ 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 his/her own OpenID service (such as a blog), or he/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.

interactions and potentially provide a uniform user-driven approach to data collection and use, including the kinds of information generally valuable to advertisers. Continued industry development and exploration of these and other user-driven identity technologies could potentially have numerous benefits for consumers and industry stakeholders:

- Could offer users the ability to control all identity-based interactions and the login becomes a one-click experience.
- Could offer consumers enhanced consumer privacy by providing
 - 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.
- Could offer websites a secure, standardized means of authenticating users.
- Could offer 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.

Because of the potential value of these technologies to the consumer online experience, the National Broadband Plan should encourage the use and further development of these technologies by the industry. Further, the Plan should recommend that government agencies lead by example and develop best practices for incorporating

¹⁵ 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.

privacy by design principles in the design of their online services. In this regard, the Broadband Plan should endorse the Obama Administration's Open Government Initiative for government online services.¹⁶ Through that initiative, the government and industry could encourage digital identity providers¹⁷ to further enhance IDM tools to allow consumers to access and interact with government content using the log-in and other personal information they have provided to digital identity providers. Enabling consumers to control the collection and use of their personal data in this manner, particularly as they navigate multiple government websites, would materially advance consumer privacy objectives and hopefully spur other website providers to follow suit.

Third Party Applications

CDT asks whether platform providers should be liable for the privacy and security violations of third-party application providers.¹⁸

The rise in popularity and use of third-party application platforms has brought unprecedented innovation and new entrants to the software development and online market place. With the mere click of a button, consumers can now access multiple third-party applications via a single retail distribution platform. This explosion of new application products and increased consumer use thereof naturally has raised questions about the access and use of consumer personal data by these applications and the privacy and security thereof.

Greater regulation of platform providers however is not the solution to these concerns. Regulators should rely on existing consumer protection laws,¹⁹ *not platform*

¹⁶ <http://few.com/Articles/2009/09/09/Open-identity-groups-collaborate-with-federal-agencies.aspx?>

¹⁷ Yahoo, Google and PayPal are just a few identity providers that use OpenID and Information Card technologies.

¹⁸ CDT Letter at 3.

¹⁹ These laws, for example, include applicable product liability regulations.

providers, to regulate the privacy and security of third-party applications. In this regard, application developers, like other product manufacturers in the retail environment, would be responsible for the quality of their products, which would include ensuring that their applications employ adequate consumer privacy and security standards. Importantly, applying consumer protection laws in the Internet ecosystem would not insulate platform providers from liability. Under existing consumer protection laws, where platform providers, like other retailers and distributors, sell or distribute third-party applications that they know do not meet some minimum, reasonable standard of consumer privacy and security, they would be held responsible. The existing status quo thus represents a “middle ground” by ensuring that consumer privacy interests are protected and that the *appropriate* industry stakeholder is held responsible when violations occur.

Moreover, to assign responsibility for violations of consumer privacy to one industry segment would ignore the fact that consumers can access third-party applications in a number of ways. Consumers, for example, can access a myriad of applications that use location-based technology in the App Store on iPhone or access the very same applications directly from the application provider through a browser. Any solution that would impose privacy or security regulation on only one industry stakeholder therefore would not produce the intended result.

Nonetheless, it would be prudent for the industry to better define minimum privacy standards regarding the collection and use of customer data. Such efforts have begun in certain segments of the industry – for example, as previously noted, online behavioral advertising groups and coalitions have developed standard consumer privacy principles. Additionally, the Cellular Telecommunications Industry Association has developed location-based services best practices and guidelines, which incorporate key privacy principles.²⁰ Other industry segments should follow suit. Minimum consumer privacy

²⁰ http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf

standards across the industry that embrace the principles of transparency, consumer control, security, and consumer value would go a long way in ensuring the privacy and security of consumer data. The National Broadband Plan can further such an objective by encouraging all platform and application providers, and indeed all stakeholders in the Internet value chain, to work together to address core consumer privacy issues through the development of minimum best practices.

Conclusion

For the foregoing reasons, the Commission should use the National Broadband Plan as a vehicle to encourage the industry to take the measures outlined herein to further protect consumer privacy.

Respectfully Submitted,

/s/ Davida Grant

Davida Grant
Gary Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street NW
Suite 1000
Washington, D.C. 20036
(202) 457-3045 – phone
(202) 457-3073 – facsimile

January 22, 2010