

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of)
)
Information Privacy and Innovation in the) Docket No. 100402174-0175-01
Internet Economy)
) RIN 0660-XA12
)

COMMENTS OF AT&T INC.

David A. Gross
Scott D. Delacourt
Amy E. Worlton
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000
Counsel for AT&T Inc.

Paul K. Mancini
Bruce R. Byrd
Theodore R. Kingsley
AT&T INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3862

June 14, 2010

TABLE OF CONTENTS

	Page
INTRODUCTION	1
I. PROMOTING THE TRUST ENVIRONMENT	5
A. Consumer Control As The Foundation	5
B. The Importance of the Trust Environment.....	6
C. A New Privacy Framework Must Apply Consistently Across the Internet Ecosystem To Build an Effective Trust Environment	8
II. PROMOTING INNOVATION IN PRIVACY PROTECTION.....	10
A. Privacy-Enhancing Technologies and Business Practices Currently In Development Will Improve Consumer Privacy.....	10
B. The Federal Government, and the Department of Commerce Specifically, Have an Important Role in Promoting the Successful Development of Privacy-Enhancing Technologies.	12
III. DISPARATE LEGAL REGIMES REQUIRE HARMONIZATION AND CONSUMER-CENTRIC APPROACHES TO PRIVACY	15
IV. CONTINUING ACTIVE ENGAGEMENT ON INTERNATIONAL PRIVACY ISSUES	17
V. CONCLUSION.....	22

Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

In the Matter of)
)
Information Privacy and Innovation in the) Docket No. 100402174-0175-01
Internet Economy)
) RIN 0660-XA12
)

COMMENTS OF AT&T INC.

AT&T Inc., on behalf of itself and its affiliates, hereby submits these comments in response to the Department of Commerce (“DOC”) Notice of Inquiry (“NOI” or “Notice”) entitled “Information Privacy and Innovation in the Internet Economy.”¹ AT&T appreciates DOC’s ongoing focus on Internet policy, and privacy in particular. To maintain the pace of innovation on the Internet, both the government and the private sector must continue to find ways to strengthen consumer trust online, which will, in turn, increase Internet usage and adoption both domestically and internationally. AT&T is committed to working with the Internet Policy Task Force and other stakeholders to develop policies and tools that both protect consumer privacy and nurture investment and innovation, consistent with DOC’s objectives.

INTRODUCTION

DOC’s Notice is timely and important. Changes in technology, services and business models have fundamentally expanded the scope and magnitude of online data being collected and used in a wide variety of contexts. Consumers increasingly utilize the Internet for everyday transactions – banking, shopping, accessing electronic health records, engaging in job training and education. And consumers are taking advantage of new innovative services, such as cloud

¹ 75 Fed. Reg. 21,226, Notice of Inquiry (Apr. 23, 2010) (“NOI”).

computing social networking and location-based services, which generate entirely new categories of online information. In these contexts, consumers are choosing to share an unprecedented amount of personal information with trusted parties and each other. As opportunities for collection and use of consumer information will only increase, consumers must feel confident about the privacy and security of their data online.

Even where discrete user information may be anonymous on a stand-alone basis, a growing capability to accumulate and associate disparate data can be used to create a highly detailed, multi-dimensional view of an individual user that goes far beyond anything possible in the offline world. The explosion in both the amount and type of available information, and the potential to use that information in ways not apparent to consumers compels an equally multi-dimensional approach to privacy protection. Empowering individuals with up-to-date privacy tools to optimize their online experience is a cornerstone of that approach. Equally significant will be a change in thinking about individual privacy that must occur at all levels of the Internet ecosystem towards enabling users to meaningfully control how they present themselves in, interact with and experience their online environments.

Moreover, the Internet holds great promise as a platform for furthering important governmental objectives and delivering solutions for achieving the nation's health care, education and energy sustainability goals. For example, online services can increase transparency, accessibility, and civic engagement by enabling the delivery of government services and increasing the availability and accessibility of government information (both through easier access and reduced costs of making information available). In addition, online services will expand the availability of emerging solutions for healthcare IT and telemedicine, distance learning and modernization of the electric grid. These services raise the stakes for

consumers because of the amount of information that will be collected and shared online, as well as the sensitivity of the information. The full potential of these emerging services will only be realized if consumers trust that their privacy will be protected online.

AT&T agrees with DOC that a policy framework which protects consumer privacy and engenders consumer trust is the foundation for promoting continued innovation and the free flow of information on the Internet. The changing Internet marketplace requires a model of privacy protection that moves beyond notice and consent, and toward customer engagement and control. Indeed, as more and more of our personal and business lives are conducted electronically and online, consumers will be increasingly concerned about privacy issues and businesses must respond appropriately in order to achieve success in the marketplace.² Consistent with marketplace imperatives, privacy cannot be a “back-end” compliance consideration, but rather must be a foundational value under a “privacy-by-design” approach. For AT&T, such an approach means we are committed to integrating privacy as a feature into AT&T’s product design and various business models, and building capabilities for our customers to understand how information is used and to exercise meaningful control over their privacy. And in order for consumers truly to be in control of their information, *all* entities involved in the Internet will need to adopt this consumer control approach to privacy protection. The DOC must ensure that any policy framework is fully inclusive of all entities in the data collection and use value-chain.

Equally important is the development of innovative approaches and tools that allow consumers to effectively manage their privacy and control their personal information as they

² See, e.g., CMO Council, *Competitive Crunch and Convergence in the Commc 'ns Marketplace Fueling Increased Customer Churn, Testing Loyalty* (Aug. 3, 2009), available at <http://www.marketwire.com/press-release/Competitive-Crunch-Convergence-Communications-Marketplace-Fueling-Increased-Customer-1213143.htm> (last visited June 13, 2010) (discussing new challenges in customer retention in the communications industry).

navigate the Internet and the dizzying array of content and services that are available to them. As discussed further herein, AT&T and others in the industry have developed a variety of innovation solutions that can serve as a model for the next phase in the evolution of privacy practices. For example, last summer AT&T, through an open and inclusive process involving feedback from customers, adopted a new, simplified, plain language privacy policy that applies, with very limited exceptions, to all AT&T services. AT&T has also emphasized bringing privacy-enhancing technologies to consumers through its commitment to a “privacy-by-design” approach in the roll out of new products, including in the online advertising space. The Internet Policy Task Force should encourage and support such industry efforts to accelerate the paradigm shift toward deeper customer engagement in all aspects of the consumer Internet experience.

DOC and the Internet Policy Task Force have several key roles to play. First, they can foster the development of a national privacy framework that applies consistently to a wide variety of services and providers on the Internet. In performing this role, the Task Force should coordinate privacy-related activity across the Federal government and serve as a clearinghouse for ideas and innovative thinking regarding privacy issues. Second, both DOC and the Internet Policy Task Force should continue to promote and support private sector innovation in privacy protection and increasing consumer security as a means of furthering freedom of expression and the free flow of information. Third, they should provide leadership that helps to achieve national-level harmonization around consistent privacy standards and best practices while working to eliminate overly restrictive and inconsistent regulation that stifles innovation. Fourth, DOC is uniquely well-positioned to advance privacy standards and best practices internationally in an effort to promote greater global privacy harmonization and reduce barriers to commerce and innovation.

I. PROMOTING THE TRUST ENVIRONMENT

AT&T proposes a national privacy policy framework that is fundamentally rooted in the consumer's interest in controlling the integrity, use and dissemination of her identity in the online world. In turn, this consumer control focus will strengthen the trust environment on the Internet, which will be essential to unlocking its potential social, economic and cultural benefits. Enabling user control over information as a means to building trust should guide further policy making by all actors in the Internet ecosystem, including both public and private sector entities.

A. Consumer Control As The Foundation

As a matter of overarching policy, the privacy framework applicable to the online commercial ecosystem must start with a focus on consumer engagement and meaningful user control. AT&T has long held this position. In September 2008, for example, AT&T's Chief Privacy Officer, appearing in a hearing concerning online behavioral advertising, advocated a "consumer-focused" framework to the Senate Commerce Committee to "ensure[] that consumers have ultimate control over the use of their personal information."³ The approach outlined by AT&T at that time, based on engaging consumers and offering them transparency and control over the use of their information, provides the critical foundation for promoting a trust framework.

Innovative approaches to engaging consumers through increased transparency and control tools that have begun to emerge in the marketplace can serve as a model for the next

³ *Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech. and the Internet of the H. Comm. on Energy*, 111th Cong. (2009) (Written Statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T Inc. at pp. 1 and 5), available at http://energycommerce.house.gov/Press_111/20090423/testimony_attwood.pdf (last visited June 13, 2010); see also Comments of AT&T Inc., Federal Trade Commission Project No. P095416 (Nov. 6, 2009) available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00031.pdf> (last visited June 13, 2010).

phase in the evolution of privacy practices. AT&T sees that model as shifting the current focus from merely notifying consumers of data collection towards facilitating practices that promote the creation of value for consumers. This model would focus on ensuring that data practices are fully transparent (as opposed to merely disclosed) and that customers are engaged and have the opportunity to control their privacy and the use of their personal information.

The means for effective consumer engagement must be designed as an integral attribute of the online experience, providing demonstrable value to the customer. For example, consumers will be better served if there is transparency and choice regarding the collection and use of their information at the time it is collected and used.⁴ Consumers may decide to make their personal information available where they see the value of doing so and are confident about their ability to control its use. Moreover, Internet users clearly understand and accept that information will be collected in commercial relationships, and that the information will be used to offer goods and services that are of value to them. But as a general industry matter, consumers need more information about what data are collected, how personal information is used and shared, and how it is protected.

B. The Importance of the Trust Environment

The Internet holds the promise of stimulating historic progress, not only in economic and technological development, but also in the health care and financial sectors, energy independence, education, social connectivity and cultural production, and other areas. This promise is inextricably linked to a foundation of user trust in both the public and private sector online entities with whom users interact as well as in the safety and security of the Internet itself.

⁴ This does not mean that one privacy regime will be immediately supplanted by an entirely new one, as the use of straightforward and meaningful notice-and-consent systems can and will be appropriate in a variety of circumstances. However, more interactive forms of customer engagement must be part of the evolution of privacy practices.

Just as in the physical world, Internet users should have meaningful control over their transactional experiences. An online privacy paradigm that emphasizes user control will strengthen the foundational trust environment of the Internet.

Innovation on the Internet today depends on consumer participation and interaction. As a network, value is best created on the Internet through widespread use. Uninhibited use by consumers is the catalyst for social media, user-generated content, and the other exciting new developments in cultural production online. User confidence in the platform is essential to unlocking the potential of the platform for this cultural and economic growth and the other societal developments discussed above. This is because, in the words of Assistant Secretary of Commerce Lawrence Strickling, “[i]f users do not trust that their [personal information] is safe on the Internet, they won’t use it.”⁵

According to a study cited by the European Commission in its recently released Digital Agenda for Europe, among those Europeans who did not shop online in 2009, concerns about payment security and privacy were two of the most significant reasons why.⁶ In the United States, accounts of Internet businesses misusing or not protecting from unauthorized disclosure consumers’ personal information are nearly daily fare in the popular press,⁷ and have shaken the

⁵ See Lawrence E. Strickling, Assistant Secretary of Commerce for Commerce and Information, *The Internet: Evolving Responsibility for Preserving a First Amendment Miracle*, Remarks before the Media Institute (Feb. 24, 2010) available at http://www.ntia.doc.gov/presentations/2010/MediaInstitute_02242010.html (last visited June 13, 2010).

⁶ European Commission *Digital Agenda for Europe* at p. 12, Fig. 3 (May 19, 2010), available at http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf (last visited June 13, 2010).

⁷ See Alison Diana, *Google Wi-Fi Breach Spurs Calls for Investigation*, INFORMATIONWEEK (May 20, 2010), available at http://www.informationweek.com/news/infrastructure/WAN_optimization/showArticle.jhtml?articleID=224900497&subSection=Infrastructure (discussing Google’s collection of payload data from unsecured home Wi-Fi networks) (last visited June 13, 2010); Emily Steel and Jessica E.

foundation of the trust environment. In order to prevent these sorts of violations, and to encourage consumer confidence in the Internet, AT&T urges the adoption of a new privacy framework by public and private parties alike across the Internet space.⁸

Among the benefits of a strengthened trust environment is that it supports the use of the Internet as a platform for free expression. As Secretary of State Hillary Clinton explained in recent remarks on Internet freedom, “the more freely information flows, the stronger societies become.”⁹ This strength derives from the fact that “access to information helps citizens hold their own governments accountable, generates new ideas, [and] encourages creativity and entrepreneurship.”¹⁰ Strengthening the trust environment through increased consumer involvement with and control over privacy is essential to the free flow of information and free expression and increases the value and vitality of the Internet as a whole.

C. A New Privacy Framework Must Apply Consistently Across the Internet Ecosystem To Build an Effective Trust Environment.

For consumers truly to be in control of their information, *all* entities in the value chain, including advertisers, ad-supported products and services, ad networks, applications developers, search engines and ISPs, will need to adopt a focus on consumer engagement. Recent events have illustrated that privacy issues can arise anywhere in the value chain, particularly as online

Vascellaro, *Facebook, MySpace Confront Privacy Loophole*, WALL STREET JOURNAL B1 (May 21, 2010) (discussing unauthorized distribution of user information to advertisers by Facebook, MySpace, and other social-networking sites).

⁸ AT&T has also recently experienced a security breach with its iPad product. See Nick Bilton, “AT&T Explains iPad Security Breach” NYTIMES.COM - BITS BLOG, <http://bits.blogs.nytimes.com/2010/06/13/att-explains-ipad-security-breach/> (June 13, 2010).

⁹ Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom*, The Newseum, Washington, D.C. (Jan. 21, 2010) available at <http://www.state.gov/secretary/rm/2010/01/135519.htm> (Clinton Internet Freedom Remarks) (last visited June 13, 2010).

¹⁰ *Id.*

services continue to evolve so rapidly. For example, both Google and Facebook are in the news lately for information collection and product design decisions that have attracted public scrutiny and eroded consumer confidence. In Google's case, the recent controversy involved its introduction of a social networking service integrated with its popular webmail platform that pre-populated and shared a contacts list semi-publicly, without clear consent from users.¹¹ For Facebook, concerns have been raised regarding potentially personally identifiable information transmitted without user consent to advertisers.¹² This approach of acting first and considering privacy impacts later has the effect of weakening consumer confidence in the online ecosystem and causing consumer frustration about the complexities of managing their privacy and personal information online.

Appropriate collection and use of personal information is essential to many of the developing social benefits of the Internet. For example, Internet-enabled health care services will rely upon access to accurate personal medical history details. However, to be effective in supporting the trust framework in a way that will give consumers sufficient confidence to allow the use of information in these ways, the consumer control approach to privacy must be ubiquitous. A regime that applies only to one set of actors will not protect consumers. As is illustrated in the examples above, frequently the entities pushing the envelope on the aggressive uses of data and customer information are the least regulated. In addition, an underinclusive privacy regime will arbitrarily favor one business model or technology over another by placing

¹¹ See Miguel Helft, *Critics Say Google Invades Privacy With New Service*, N.Y. TIMES, Feb. 13, 2010, at B1 available at <http://www.nytimes.com/2010/02/13/technology/internet/13google.html> (last visited June 13, 2010)

¹² See Steel and Vascellaro, *supra*, note 6.

all the costs of protecting consumers on certain sectors, while others are allowed to commercially exploit consumers' information without serious restriction.

II. PROMOTING INNOVATION IN PRIVACY PROTECTION

The Federal government, and DOC specifically, should continue to champion policies in which privacy and innovation are mutually reinforcing. In many areas, U.S. policy to date has fostered the efficient deployment of new technologies while remaining neutral as to their specific design. This same approach should be used here to encourage the innovation in privacy-enhancing technologies that is already well underway by the private sector. As discussed in more detail below, DOC can work to encourage the development of identity management standards, promote the development of privacy control tools that consumers can understand and adopt, collaborate with stakeholders to develop best practices for privacy and security safeguards, and support positive international developments in this area. Additionally, DOC can encourage the Federal government to lead by example in this area by developing and implementing best practices in government Internet activities and employing consumer-centric privacy protections in its own offerings of online services.

A. Privacy-Enhancing Technologies and Business Practices Currently In Development Will Improve Consumer Privacy.

The *Notice* requests information regarding ongoing efforts to develop privacy-enhancing technologies and specifically efforts towards increasing notice to consumers and anonymized browsing.¹³ Further development of privacy-enhancing technologies and business practices should be encouraged to build the capability to give consumers information about how and what data is collected and used, and to track the sharing of personal data as it occurs. With improved tools, consumers will be better-positioned to make informed choices about protecting their own

¹³ See NOI, 75 Fed. Reg. at 21,231.

privacy.

AT&T has already begun this transition in its own practices. Last year we developed and published an updated, consolidated and streamlined privacy policy that applies (with very limited exceptions) across all of AT&T's business units and services. Customer feedback helped shape this new policy, and contributed to our emphasis on a consumer-centric, plain-language presentation that clearly explains to users what data we collect, how we collect it, and how we use it. Our rollout included video explanations of our policy highlights, as well as a 45-day preview period for customer feedback. Based on that customer feedback, we made additional changes to the policy – including adding definitions and specifically confirming that we do not sell, give or “rent” personal information to marketing companies – before posting the final version.¹⁴

AT&T has also emphasized bringing privacy-enhancing technologies to consumers. For example, in connection with targeted advertising with data from yellowpages.com, 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 believe these new capabilities not only represent best practice in this area, but also are a step towards an ecosystem-wide approach based on customer engagement.

Several technologies identified in the *Notice* would improve transparency and give consumers greater control over personal data. For example, anonymized browsing helps prevent

¹⁴ The principles that underlie this updated policy include: We will protect your privacy and keep your personal information safe; we will not sell your personal information to anyone, for any purpose; we will fully disclose our privacy policy in plain language, and make our policy easily accessible to you; we will notify you of revisions to our privacy policy, in advance; you have choices about how AT&T uses your information for marketing purposes. *See AT&T Privacy Policy, available at* <http://www.att.com/gen/privacy-policy?pid=2506> (last visited June 13, 2010).

the hidden or unknown collection of a user's data through data collection mechanisms, such as cookies. In addition, consumer-centric identity management systems like those recommended by the Federal Communications Commission¹⁵ ("FCC") could include the ability to allow users to build virtual profiles that support their information sharing choices online across various websites, applications, and platforms. Using these systems, consumers could actively manage how they will exchange personal information in pre-determined ways. Improved and ubiquitous identity management solutions could help individuals and organizations form trusted communities based on varying degrees of identity exposure. Through a virtual profile, a user could have the option of identifying the level of information he or she wishes to share with different communities, including trusted businesses, friends, or even no one. Such systems could also allow users to establish notifications that alert them before certain information is shared and to track generally when and with whom their personal data is shared.

B. The Federal Government, and the Department of Commerce Specifically, Have an Important Role in Promoting the Successful Development of Privacy-Enhancing Technologies.

By working with stakeholders, including a broad range of industry participants, the U.S. government, and DOC specifically, can play an important role in encouraging the development of privacy-enhancing technologies. Existing government research efforts, such as the White House's National Strategy for Secure Online Transactions have begun to support efforts to develop innovative new technologies. Building from existing efforts, the Federal government should develop policies that will create incentives for Internet innovators to build out the "identity layer" of the Internet ecosystem in a way that secures transactions and protects consumer privacy, while still supporting business growth and economic development.

¹⁵ See NOI, 75 Fed. Reg. at 21,231.

Towards this end, the Federal government should:

First, play a role in the development of best practices for privacy and security protections. Through collaboration across a wide range of stakeholders, the government could identify best practices that allow for secure transactions and protect consumer privacy. For example, areas that need further collaboration are the development of best practices for anonymizing data, minimizing data collection, and limiting data retention periods. As the *Notice* recognizes, recent research has shown that data re-identification may be possible even after such data has been anonymized.¹⁶ The government could specifically work to encourage best practices where they are inadequate to reduce the risks of data re-identification, including practices related to both data minimization and retention periods.

Some self-regulatory frameworks for meaningful privacy protection are already in place, helping to earn consumers' trust in the wireless Internet and cloud computing. AT&T voluntarily adopted strong protections for subscriber location information,¹⁷ and in working with our enterprise customers, we use "privacy by design" in providing cloud computing services. In the wireless industry, CTIA has developed Best Practices and Guidelines for Location-Based Services in order to set benchmarks for the mobile Internet ecosystem in a technology-neutral way.¹⁸ These best practices and guidelines are responsive to individuals' and policymakers' heightened privacy interests in location data while eschewing any particular format requirement, default setting or other rigidity that could hamper innovation. In another example, the Mobile Marketing Association likewise adopted a Global Code of Conduct calling for advertisers to

¹⁶ See NOI, 75 Fed. Reg. at 21,230.

¹⁷ See AT&T Privacy Policy, available at www.att.com/gen/privacy-policy?pid=13692#location (Questions about Location Information).

¹⁸ See CTIA, *Best Practices and Guidelines for Location Based Services* (2010) available at http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

obtain explicit opt-in from individuals for mobile marketing programs.¹⁹

Second, the U.S. government could also support the development of identity management systems and industry privacy control tools through establishing broad goals for these technologies. Although some tools and controls are available today, adoption by both consumers and Internet entities has been low due to the complexity of the ecosystem, lack of knowledge and difficulty of use. In addition, identity management has historically focused on traditional identity theft issues. Therefore, to aid the successful implementation of innovative privacy tools, the government should work with the private sector to promote the expansion of the field to address additional privacy concerns and the development of user-friendly tools and interfaces and to increase education of both consumers and the Internet industry. In this process, DOC's National Institute of Standards and Technology could also bring its technical expertise to bear in promoting development of industry standards should that prove to be necessary to encourage the successful deployment of privacy-enhancing technologies.

Third, the U.S. government should also continue its support for positive international developments in this area. For example, as discussed further below, the Asia-Pacific Economic Cooperation Privacy Framework ("APEC Framework")²⁰ promotes a consistent global approach to privacy protection to avoid the creation of unnecessary barriers to information flows and to remove impediments to trade. In addressing international issues, an important objective is giving providers technical and operational flexibility so that services can be designed to meet the needs of customers, rather than overly restrictive legal and regulatory requirements.

¹⁹ See Mobile Marketing Association, *Global Code of Conduct* (2008) available at <http://www.mmaglobal.com/codeofconduct.pdf>.

²⁰ See Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005) available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

III. DISPARATE LEGAL REGIMES REQUIRE HARMONIZATION AND CONSUMER-CENTRIC APPROACHES TO PRIVACY

A strong framework for nourishing privacy and innovation will not exist in a vacuum. It will have to take hold in the midst of many legal and business complexities. In AT&T's view, holding consumer privacy interests paramount and adopting privacy by design will help to simplify this landscape. In addition, harmonization would be helpful to foster clear, predictable rules that are consistent among state and federal regimes and across industry sectors and technologies.

A Clear Legal Foundation for Internet Innovations: Innovation interests are compelling with respect to many dynamic new technologies that hold great prospects for growth, such as location-driven applications for wireless devices and cloud computing. Privacy interests are also at their most keen with respect to these offerings, due to the ubiquity of mobile devices, the growing prominence of cloud computing, and the fact that these technologies are driven by location data and remote data processing, respectively. Although privacy and innovation are well-served through self-regulatory mechanisms, private actors sometimes face difficult legal uncertainty with respect to many dynamic new technologies. Location data, now available through several different technologies, and data associated with cloud computing are no exception.²¹ Harmonization and clarification of divergent legal rules would help service

²¹ See e.g., Elec. Commc'ns Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, *codified at* 18 U.S.C. § 2510 *et seq.*; Commc'ns Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. §§ 1001-1010; 47 U.S.C. § 222; *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F.Supp.2d 747 (S.D. Tex. 2005); *In re Application Of The United States Of America For An Order Directing A Provider Of Elec. Commc'n Serv. To Disclose Records To The Government*, 534 F.Supp.2d 585, 589 (W.D. Pa. 2008); *In the Matter of the Application of the United States of America for an Order Directing the Provider of Elec. Commc'ns Serv. to Disclose Records to the Government*, 534 F.Supp.2d 585 (W.D. Pa. 2008), *aff'd by and objection denied by* 2008 U.S. Dist. LEXIS 98761 (W.D. Pa. Sept. 10, 2008) (currently on appeal to the Third Circuit, Case 08-4227); see also 18 U.S.C. §§ 2701-2712; *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003); *Theofel v. Farey Jones*, 359 F.3d 1066 (9th Cir. 2004).

providers understand their rights and responsibilities, and would give individuals confidence about the protections due to their data.

Government Action to Protect Privacy. The U.S. government can lead by example and ensure that individuals have meaningful control over their personal information. Many government agencies offer online services to the public, such as the ability to submit tax payments and apply for and renew a variety of government-issued licenses. As a provider of online services, the federal government should adopt “privacy by design” and security safeguards as appropriate.

AT&T is participating in multiple efforts to encourage policymakers to clarify and update the rules concerning government access to online information, such as location information and data stored “in the cloud.” For example, we are a member of the Digital Due Process coalition working to encourage the inclusive stakeholder dialogue necessary to establish uniform protections for communications data while preserving the legal tools needed by law enforcement.²²

Balance of Interests in Security, Breach Notification and Data Encryption. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have adopted laws requiring notice in case of a breach in the security of their personal information.²³ AT&T strongly supports the principal of notice in such cases, which is a part of the company’s privacy policy.²⁴ Yet, companies acting in good faith can be bogged down by broad-brush encryption

²² See Digital Due Process, *available at* www.digitaldueprocess.org (last visited June 13, 2010).

²³ See, e.g., Cal. Civ. Code § 1798.82; 815 Ill. Comp. Stat. Ann. 530/5 *et seq.*; N.Y. Gen. Bus. Law § 899-aa.

²⁴ See AT&T Privacy Policy, *available at* <http://www.att.com/gen/privacy-policy?pid=13692#protection> (Question 4 about Data Security and Protection) (last visited June 13, 2010).

requirements, disparate notice specifications and inconsistencies in the data whose breach can trigger a notice.²⁵ The robust privacy framework sought by AT&T could go far in resolving these tensions. In addition, the Internet Policy Task Force should lend its support to the creation of a information security “Safe Harbor.” No company can completely eliminate the risk of breach, but, a set of security safeguards should be developed that, if met and maintained in good faith, should meet the policy goals.

AT&T supports the need for ongoing U.S. government support for the so-called “Good Samaritan provisions” of the Communications Act, Section 230.²⁶ The statute strikes the right balance, allowing service providers to police their websites without fear that immunity will be lost, thereby creating incentives for stronger privacy protections.

IV. CONTINUING ACTIVE ENGAGEMENT ON INTERNATIONAL PRIVACY ISSUES

U.S. leadership is essential to advancing the development of a strong privacy framework on an international basis that will facilitate transborder data flows and the growth of the global Internet. Dramatic decreases in transport costs and increased connectivity arising from the Internet create an enormous opportunity for cloud computing and other service platforms that can overcome geography and distance limitations. These advances mean that privacy concerns are global and, in the international policy arena, of paramount importance. The U.S. government is a critical partner in helping to shape international dialogues, support U.S. competitiveness and advocate on behalf of the free flow of information.

A consumer-centric approach to privacy will help to promote innovation in the United

²⁵ See, e.g., 201 Mass. Code Regs. §17.03(1); Nev. Rev. Stat. §§ 205.4742; Iowa Statutes, Section 715C.1 et seq.; Utah Code Ann. §§ 13-44-101, *et seq.*

²⁶ 47 U.S.C. § 230(c).

States, and further, will advance these same interests on a global basis. It should appeal to foreign authorities, as it delivers substantive privacy protection and provides a basis for accountability and enforcement. In the case of cloud computing, for example, reasonable and clear protections in the United States for stored information will help reassure foreign governments wary of data collection and storage outside their borders. Simultaneously, the approach provides value to industry, avoiding prescriptive, one-size-fits-all rules in favor of flexible privacy principles that can be adapted to a particular industry. The framework insists on technological neutrality and advances the goal of harmonization. AT&T encourages a shared understanding of privacy values, in part, to establish a solid foundation for the U.S. government and U.S. industry to advocate successfully abroad for a balance of privacy and innovation interests.

Data protection policy is increasingly under discussion in foreign and international bodies. To shape these dialogues, coordinated action by the Commerce Department, the State Department, the U.S. Trade Representative, the Federal Communications Commission, the Federal Trade Commission and other relevant agencies will be critical. The following is but a short list of multinational venues where continued U.S. leadership is needed:

- As discussed above, AT&T believes that the APEC Framework²⁷ holds great promise as a set of broadly-applicable privacy standards that can be adapted to particular jurisdictions and industries, while enjoying mutual recognition by participating economies. We appreciate the efforts of the Office of Technology and Electronic Commerce within the Commerce Department and the Federal Trade Commission in developing the Framework. The U.S. government should continue to actively support

²⁷ See APEC, *supra* note 20.

the Framework's development and implementation, which could yield greater information flows and trade.

- The Organisation for Economic Co-operation and Development (“OECD”) is celebrating the 30th Anniversary of its influential Privacy Guidelines by examining their impact and studying how they should be updated to better facilitate trans-border data flows.²⁸ The U.S. government should engage in this process in order to ensure that revised Guidelines reflect the Administration's view that privacy should promote free flows of information.
- The European Commission is considering whether the 15-year-old EU Data Protection Directive should be updated.²⁹ The lack of an efficient format for mutual recognition between EU Member States continues to be a major hurdle for international business, and the U.S. government should support the European Commission in its push for harmonization. Moreover, because the EU Directive continues to exert a strong influence on global privacy standards, coordinated U.S. action is necessary to promote models conducive to cross border data flows and responsive to real-world privacy risks and business practices.

²⁸ See, e.g., OECD, “30 Years After: The Impact of the OECD Privacy Guidelines,” available at http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html (last visited June 13, 2010).

²⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC (E.U. 1995) available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (last visited June 13, 2010); see, e.g., European Commission, Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data, available at http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm (asking for public comment on whether the current legal framework meets new challenges for personal data protection) (last visited June 13, 2010).

- The recently agreed Framework for Cooperation on Trade and Investment establishes an ongoing dialogue between the United States and India to strengthen bilateral economic cooperation.³⁰ The U.S. Trade Representative and other U.S. government actors should seize the opportunity in upcoming meetings to promote a clear, harmonized privacy framework that preserves business flexibility while conferring consumer-oriented privacy protections on outsourced data.

In working closely with industry, the U.S. government has a track record of substantial success in facilitating trans-border trade. As an example, the U.S.-EU Safe Harbor program, negotiated by the Department of Commerce in the late 1990s, preserved the free flow of personal data from the EU for eligible companies, provided means for participating U.S. companies to meet EU data protection adequacy requirements, and enshrined the principle of self-regulation, backed-up by government enforcement where necessary.³¹ AT&T is committed to working in partnership with the U.S. government to foster this type of international environment.³²

Freedom of Information. AT&T commends the U.S. government for speaking out in support of free data flows.³³ We believe that Internet innovation rests on information exchanges and that strong privacy protections and user controls ultimately promote these exchanges. We

³⁰ Press Release, Office of the United States Trade Representative, United States and India Sign Framework for Cooperation on Trade and Investment (Mar. 17, 2010) *available at* <http://www.ustr.gov/about-us/press-office/press-releases/2010/march/united-states-and-india-sign-framework-cooperation-t>.

³¹ See Dept. of Commerce, Issuance of Safe Harbor Principles and Transmission to European Commission, Notice, 65 Fed. Reg. 45,666 (July 24, 2000).

³² To be clear, the common carrier components of AT&T are ineligible to participate in the U.S.-EU Safe Harbor because they are exempt from the enforcement jurisdiction of the Federal Trade Commission. See 15 U.S.C. § 45(a)(2). Nonetheless, AT&T believes that the Safe Harbor exemplifies how U.S. government involvement can help harmonize disparate data protection regulatory regimes.

³³ See, e.g., Secretary Clinton Remarks on Internet Freedom, *supra*, note 8.

support efforts of the U.S. government to focus on fostering respect among the international community for privacy, freedom of information and freedom of expression.³⁴

Free Trade and Innovation. Although AT&T primarily offers enterprise solutions rather than consumer offerings abroad, all U.S. companies are potentially susceptible to privacy enforcement actions motivated by protectionism. Local data storage requirements can also be barriers to trade. We have seen some foreign governments attempt to create national technical standards for the Internet; these efforts generally should be discouraged in favor of international standards that promote competitiveness and universality. In general, the Commerce Department, the U.S. Trade Representative, the State Department and the Federal Communications Commission should, in various international circles, push open doors for U.S. business and for further Internet innovations.

Privacy by Design. We believe the “privacy-by-design” model of integrating personal data controls into new technologies and business processes can be effective internationally. The role of the U.S. government should be to advocate on behalf of clarity and flexibility, to ensure that “privacy-by-design” initiatives neither mandate nor prohibit any particular feature or system configuration, which could hamper innovation.

³⁴ See, e.g., Tunis Agenda For the Information Society, World Summit on the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1-E) ¶ 42 (2005), available at <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html> (“We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.”) (last visited June 13, 2010).

V. CONCLUSION

To maintain the pace of Internet innovation, the Administration must continue to find ways to strengthen consumer trust online. AT&T urges DOC to move forward in advancing a consumer-centric privacy framework, as articulated herein.

Respectfully submitted,

/s/ Bruce R. Byrd

David A. Gross
Scott D. Delacourt
Amy E. Worlton
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000
Counsel for AT&T Inc.

Paul K. Mancini
Bruce R. Byrd
Theodore R. Kingsley
AT&T INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3862

June 14, 2010