Before the

FEDERAL TRADE COMMISSION

In the Matter of	)
	)
Protecting Consumer Privacy in an Era	)
of Rapid Change: A Proposed Framework	)
for Businesses and Policymakers	)
	)
	)
	)

COMMENTS OF AT&T INC.

Alan Charles Raul
Edward R. McNicholas
Colleen Theresa Brown
Jonathan P. Adams*
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Counsel for AT&T Inc.

Paul K. Mancini
Keith M. Krom
Theodore R. Kingsley
AT&T INC.
1133 21st Street, N.W.
Washington, D.C. 20036
(202) 463-4148

Kelly Murray
AT&T SERVICES INC.
208 S. Akard Street
Dallas, TX 75202
(214) 757-8042

February 18, 2011

* Admitted only in California

Table of Contents

INTRODUCTION

AT&T Inc. ("AT&T"), on behalf of itself and its affiliates, is fully committed to participating in the open and inclusive process the Federal Trade Commission (the "FTC" or the "Commission") has established in order to ensure the Internet continues to create new ways for people to connect and share information in all aspects of their lives . To this end, we are pleased to provide these comments on the preliminary staff report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" ("the Report")[1] issued by the Commission. AT&T also recently provided comments to the green paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (the "Green Paper")[2] issued by the Department of Commerce (the "Department" or "Commerce"); such comments are attached for the Commission's consideration given that they address some issues that overlap with the Commission's Report. AT&T suggests the Commission also consider the Department's Green Paper as well as the comments submitted in response to it in order to promote consistent and effective coordination among all federal agency approaches to privacy. Just as harmonization of international privacy frameworks is beneficial to U.S. consumers and businesses, increased harmonization within the United States that is based on flexible principles adapted for the various sectors of the economy can also produce more effective and efficient privacy protection. Coordination between the agencies should encourage the smartest, most cost-effective, and least burdensome ways of securing consumer privacy.

We encourage the Commission and the Department to work together in conjunction with industry and civil society to ensure that a consistent set of baseline privacy protections is a reality for consumers throughout the Internet ecosystem, while recognizing that the expression and implementation of these principles should be flexible and adaptable in light of the nature and uses of the information involved. Inconsistent frameworks entail undue costs, discourage innovation, and can harm the economy by introducing uncertainty into business planning. The

[1] Fed. Trade Comm'n, Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 2010) [*hereinafter* "FTC Staff Report"].

[2] U.S. Dep't of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 2010) [*hereinafter* "IPTF Privacy Green Paper"].

Commission and Department should instead aim to develop and implement a framework "designed to reduce burdens, redundancy, and conflict."[3]

Significantly, the Commission should acknowledge that any new dimensions for privacy protection arise within a complex system of constitutional, statutory, regulatory, and common law norms that already provide significant standards for data protection throughout the economy. Sectoral laws impose specific requirements on certain financial institutions, healthcare providers, and communications carriers. General common law norms continue to evolve. And enforcement of these provisions is carried out by a variety of federal agencies, state agencies, or private litigation, as well as data protection authorities outside of the United States. Conflicts among existing laws and standards – let alone new ones – can breed needless complexity and generate an uneven playing field. At the very least, the Commission and the Department should work together to maintain consistency, ensure technological neutrality, and eliminate counter-productive overlaps within this framework. Doing so would promote both substantive privacy protection and incentivize innovation.

Moreover, AT&T believes that the current federal-state system for setting and enforcing standards for privacy and consumer protection is generally effective. Meaningful self-regulation by industry associations and individual companies combined with oversight by the FTC, federal banking, healthcare and communications regulators, and state attorneys general have produced a dynamic and rigorous data protection regime for the United States that is second to none. As industry self-regulation advances and U.S. standards are refined, we urge the Commission not to lose sight of what has been working well.

We commend the Commission for its thoughtful consideration of new ways to protect consumer privacy across various information platforms, while promoting the significant consumer benefits that derive from fostering innovation and flexibility in technology, products and services. As President Obama wrote recently in the *Wall Street Journal*, it is crucial that the public be protected while freedom of commerce is preserved:

---

[3] Memorandum from Cass R. Sunstein, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, to Heads of Executive Departments and Agencies, and of Independent Regulatory Agencies, M-11-10 at 3 (Feb. 2, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-10.pdf. "Efforts at harmonization might occur within agencies, as efforts are made to coordinate various rules. Such efforts may also occur across agencies, as agencies work together to produce greater simplicity and predictability." *Id.*

> For two centuries, America's free market has not only been the source of dazzling ideas and path-breaking products, it has also been the greatest force for prosperity the world has ever known. That vibrant entrepreneurialism is the key to our continued global leadership and the success of our people.
>
> But throughout our history, one of the reasons the free market has worked is that we have sought the proper balance. We have preserved freedom of commerce while applying those rules and regulations necessary to protect the public against threats to our health and safety and to safeguard people and businesses from abuse.[4]

We also strongly agree with the recent statement of the White House that "[i]n this digital age, a thriving and dynamic economy requires Internet policies that promote innovation domestically and globally while ensuring strong and sensible protections of individuals' private information and the ability of governments to meet their obligations to protect public safety."[5]

The FTC Report itself acknowledges the highly significant benefits of online collection of data and personalized services and advertising. The Report states that:

> . . . technological advancements and increased computing power have allowed companies to collect, store, manipulate, and share ever increasing amounts of consumer data at very little cost. This has led to an explosion of new business models that depend upon capturing consumer data at a specific and individual level and over time, including online behavioral advertising, social media services, and location-based mobile services. . . . These developments can provide enormous benefits to consumers, including instant, around-the-clock access to products and services, more choices, lower prices, personalized content, and the ability to communicate and interact with family, friends, and colleagues located around the globe.[6]

The Commission should continue to be mindful of the need for balanced, thoughtful engagement with all stakeholders in order to ensure that both consumer privacy and Internet innovation are preserved and enhanced by these innovative frameworks. As the President's recent Executive Order expresses:

---

[4] President Barack Obama, *Toward a 21st-Century Regulatory System*, Wall St. J., Jan. 18, 2011, at A17.

[5] White House Office of Sci. & Tech. Policy, *White House Council Launches Interagency Subcommittee on Privacy & Internet Policy* (Oct. 24, 2010), http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy.

[6] FTC Staff Report, *supra* note 1, at 21.

> Our regulatory system … must allow for public participation and an open exchange of ideas. It must promote predictability and reduce uncertainty. It must identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends. It must take into account benefits and costs, both quantitative and qualitative. It must ensure that regulations are accessible, consistent, written in plain language, and easy to understand. It must measure, and seek to improve, the actual results of regulatory requirements.[7]

Moreover, in Section 230 of the Communications Decency Act, 47 U.S.C. § 230(b), Congress expressed the policy of the United States "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." While statements of policy are not law, they can help delineate the proper contours of statutory authority and agency activity. In light of Congress's statutory pronouncement that Internet regulation is disfavored, and the Presidents' admonition about the need to preserve the dynamic benefits to society created by technological innovation, the FTC should take care to approach privacy standards deftly. The FTC may thus wish to consider how to apply the President's Executive Order in the context of articulating privacy standards and guidelines and also respect the policy of Congress to foster a vibrant Internet free of unwarranted governmental constraints.

[7] Exec. Order No. 13,563, 76 Fed. Reg. 3821, 3821 (Jan. 21, 2011) ("Improving Regulation and Regulatory Review"), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf (requiring that each regulatory agency must "tailor its regulations to impose the least burden on society . . . [and] select . . . those approaches that maximize net benefits"). Although the Executive Order does not directly apply (since no actual regulations are at issue), it provides important principles for sound policy-making. In addition, the President and White House have encouraged independent agencies to apply the principles of this Executive Order. *See, e.g.,* Memorandum from Cass R. Sunstein, *supra* note 3, at 6 ("Executive Order 13563 does not apply to independent agencies, but such agencies are encouraged to give consideration to all of its provisions, consistent with their legal authority."); Hearing on the Views of the Administration on Regulatory Reform Before the Subcomm. on Oversight and Investigations of the H. Energy & Commerce Comm. (Jan. 26, 2010) (prepared statement of Cass R. Sunstein, Administrator, Office of Information & Regulatory Affairs), *available at* http://energycommerce.house.gov/media/file/hearings/oversight/012611_OIRA /012611sunstein.pdf (noting that the President hoped that the independent agencies would comply with the Executive Order).

EXECUTIVE SUMMARY

The Commission's Report is particularly significant at this critical time in the development of Internet policy. AT&T is pleased that the analysis expressly recognizes and appreciates the tremendous financial and social benefits that derive from the free flow of information. Our society benefits from continuing and accelerated growth and change on the Internet; it is the backbone of the phenomenally productive information age and digital economy. To be sure, future innovation will far surpass current technologies, and companies will find it in their direct economic interest to continue to foster consumer comprehension of and comfort with these innovations so that consumers will trust and use them.

AT&T's approach to protecting our customers' privacy rests upon four pillars – transparency, consumer control, privacy protection and consumer value. We are thus generally supportive of the Commission's preliminary framework, particularly to the extent that it is predicated on flexible performance standards that will evolve over time with technologies and business models. The Commission's framework must continue to encourage innovation and remain neutral toward particular current technologies.

This commitment to technology neutrality is essential to the creation of any enduring framework, and AT&T lauds the desire not to stymie dynamic growth or use the law to select technological winners. Robust competition will drive the innovation of technologies that will no doubt be far more advanced than anything available today. Each actor in the Internet ecosystem should be free to develop such innovative products to provide consumers with the maximum range of choices that enhance their ability to communicate – and each actor should be held to the same high standards that ensure consumer control of personal information. In particular, AT&T supports solutions that:

- Continue to focus on engagement with consumers regarding privacy;
- Ensure that consumers have meaningful controls of their personal information;
- Maintain neutrality among various technologies;
- Are coordinated among various federal regulatory stakeholders;
- Are proportional to the needs of consumers, and flexible enough to enhance the continued innovation and the diversity of the Internet economy;

- Are consistent with global interoperability by reflecting shared international as well as US privacy requirements;
- Articulate that the overall US data protection regime is entitled to mutual recognition by the EU, and support an "adequacy" determination by the EU;[8]
- Increase meaningful consumer outreach regarding consumer privacy choices, including just-in-time notice, and greater transparency into privacy practices;
- Encourage innovation in easily accessible, consumer friendly, multi-media, plain-language privacy policies, settings, icons, and other interactive consumer notice mediums;
- Reasonably expand protections to data linked to particular computers and other devices;
- Provide consumers with reasonable access in the context of that company's specific business operations;
- Reserve express notice and consent requirements for data practices that are not "commonly accepted;"
- Eschew a rigid one-size-fits-all mindset for FIPPs, privacy notices, or ways to assess privacy impacts;
- Enhance the diversity in data practices among industries, data systems or technologies to provide real consumer choice; and
- Will lead to appropriate national data breach notification standards that give consumers meaningful notice of actual risks of harm.

[8] As the European Article 29 Data Protection Working Party recently stated: "the Working Party has invested a lot in the . . . principle of Mutual Recognition. . . [and] suggests that the [EU] Commission investigates to what extent and under what conditions the principle of Mutual Recognition can be formalised and made more binding in the new legal framework"; the Working Party also focused on developing "appropriate transfer instruments that are effective in ensuring adequacy," which may require "improving and streamlining the rules applying to international data transfers." *See* Letter from Article 29 Data Protection Working Party to Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship, European Commission (Jan. 14, 2011), *available at*http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_ communication_approach_dp_en.pdf.

While the Commission's proposed framework, along with the Department's Green Paper, have provided enhanced clarity on these and other issues, we are hopeful that the Commission will take to heart President Obama's direction to protect the public by acting against real threats and abuse on the Internet and in the digital economy, while preserving the freedom of commerce that has "been the source of dazzling ideas and path-breaking products, [and] the greatest force for prosperity the world has ever known."[9]

COMMENTS ON THE COMMISSION'S PROPOSED FRAMEWORK

A. Ensuring Proportional Privacy Standards[10]

The free flow of information on the Internet, along with sophisticated advertising and data analysis, provides enormous value for consumers and the economy.[11] Governmental approaches to privacy should take full account of these benefits and ensure that regulations provide for the protection of privacy in a manner that is proportional to the harms it addresses and mindful of the benefits of freedom. We urge the Commission to make a concerted effort to understand and, if possible, to quantify (or at least rigorously characterize) these harms and benefits, and seek to achieve a favorable cost-benefit balance for society in recommending any new privacy standards.

As President Obama recently re-emphasized in his Executive Order No. 13,563 of January 18, 2011,[12] ("Executive Order"), a policy standard will work best when it is based on "a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify)" and when they "impose the least burden on society, consistent with

[9] Barack Obama, *Toward a 21st-Century Regulatory System*, *supra* note 4.

[10] Responsive to Questions for Comment ("QFCs") contained in Appendix A of the FTC Staff Report, *supra* note 1, listed under subheadings "Scope," "Incorporate substantive privacy protections," "Maintain comprehensive data management procedures," and "Practices that require meaningful choice: Special choice for online behavioral advertising: Do Not Track."

[11] *See* FTC Staff Report, *supra* note 1, at 33-34 ("Another recurring theme from the roundtables was that the increasing flow of information provides important benefits to consumers and businesses. . . . Online advertising helps to support much of the content available to consumers online and allows personalized advertising that many consumers value.").

[12] Executive Order No. 13,563, *supra* note 6, at 3821.

obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations."[13]

Implementation of new privacy frameworks and privacy enhancing proposals should occur in a manner that ensures flexibility and avoids micromanaging how individual companies conduct their businesses and contract with their customers. Accordingly, the best regulations "specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt."[14]

Standards for consumer protection that require a particular compliance mechanism for communicating with customers will likely fail to keep pace with changing technology and business models. As Matt Ridley noted in the *Wall Street Journal*, "Government policy rarely ages as fast as when it contains pronouncements about new technology."[15] Although it can be counterproductive to mandate particular compliance formats that would quickly become obsolete and unduly burdensome, industry should be responsible for satisfying baseline performance objectives for protecting privacy.

We urge the Commission to continue to draw upon the resources of industry and civil society to assess the actual costs and benefits that drive consumer behavior, relate to bona fide social concerns, and influence whether innovation will be permitted to occur as quickly as desirable. Such costs and benefits must, of course, take account of (by rigorously characterizing and weighing) the intangible and qualitative impacts that improper or uncomfortable invasions of privacy can have on human dignity and the values of informational autonomy (*i.e.*, one's interest in controlling information about oneself). At the same time, the FTC should consider the benefits that consumers derive from the relatively free flow of information in the economy, the benefits consumers enjoy from technological innovation leading to new products and services (many of which we do not even realize we need or want yet), the benefits of customization and personalization that are made possible by sharing of information, and the benefits in terms of personal convenience resulting from all of the above.

A cost benefit analysis must also appreciate that undue governmental prohibition or prescription in this context can chill the free flow of information, the freedom of expression, and

---

[13] *Id.* §1(b).

[14] *Id*.

[15] Matt Ridley, *There's Nothing So Old as the Recently New*, Wall St. J., Jan. 8, 2011, at C4.

the freedom to associate (in commerce, or otherwise). These freedoms are foundational principles of our Republic, and federal courts have recognized certain constitutional limitations on governmental efforts to control the dissemination of non-deceptive commercial speech.[16] In light of these concerns, the control of personal and other information should remain primarily an area into which the government intervenes only when needed, and the intervention of government into the marketplace of ideas carries with it structural risks against which the Founders protected us with the First Amendment.

When regulation is appropriate, the regulation should appreciate the significant benefits that flow to individuals from sharing information with trusted business partners, such as when an investment advisor can suggest better options because she appreciates your investment style, risk tolerance, and financial goals, or when your cell-phone company can better estimate the most economical plan given historical usage information and patterns. It is a positive thing for consumers to choose to form such long-term bonds with companies. Indeed, maintaining strong customer trust and loyalty is a very tangible incentive that has driven successful business models for decades.

Throughout this process, the Commission should encourage the market to provide as many solutions as it can, particularly given the substantial economic rewards that exist for companies that can produce technologies with which consumers feel comfortable, and the substantial market pressure companies can experience when they overstep. Competition among companies on the parameters of privacy protection is both possible and desirable. These powerful incentives are important tools for policy makers.

These incentives can be the wellspring of the next generation of privacy enhancing technologies. Allowing flexible, market-driven solutions should be sufficient to develop technologies for the verification of personal information usage practices and monitoring of data usage to support internal accountability mechanisms. The Commission could convene various industries to encourage and promote the development of innovative interoperable privacy tools.

---

[16] *Compare Sorrell v. IMS Health Inc.*, No. 09-1913, 2010 U.S. App. LEXIS 24053 (2d Cir. 2010), *cert. granted* 131 S. Ct. 857, 178 L. Ed. 2d 623, (U.S. Jan. 7, 2011) (No. 10-779) (striking down restrictions on the use of prescriber data), *and U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (striking down the FCC's rule initial restrictions of the use of CPNI for marketing purposes as violative of the First Amendment), *with IMS Health Inc. v. Mills,* 616 F.3d 7 (1st Cir. 2010) (upholding certain restrictions on the use of prescriber data), *and National Cable & Telecommunications Ass'n* v. *FCC*, 555 F.3d 996 (D.C. Cir. 2009) (upholding revised restrictions on the use of CPNI).

But government-mandated solutions in this area will systematically fail to anticipate the next generation of information usage because such solutions can never be nimble enough to contemplate technologies that are still in development or future products and services that will break new paths to dazzle consumers and boost the economy. For example, a number of companies that develop and distribute browser software recently announced Do Not Track features for their browsers which were no doubt in development months (if not years) before the Commission's Do Not Track proposals.[17] Alex Fowler, Mozilla's global privacy and public-policy leader, said his company wanted to give users flexibility in choosing the companies they will and will not allow to track them: "[w]e've done this intentionally because there is a spectrum of values across our users … [some] 'don't want to see ads or be tracked' at all, while others 'see value in free services by receiving free advertising.'"[18] As consumer demand establishes the appropriate range of tracking activity, the market will provide powerful incentives to companies to provide that ability, and to do so in a cost effective and innovative manner.

B. Global Interoperability[19]

Particularly in a globally competitive marketplace, privacy frameworks must remain flexible enough to satisfy basic standards of protection across different jurisdictions. As the Commission staff noted, "[i]nternational enforcement and policy cooperation . . . has become more important with the proliferation of complex cross-border data flows and cloud computing,"[20] and the FTC's development of an internationally harmonized framework should assist in accomplishing those goals while furthering consistent global privacy standards.

U.S. and foreign companies are already obligated to expend extensive resources to understand and address jurisdictional differences, and these resources could be re-focused on providing effective privacy protection when regulations are consistent. Indeed, lowering the costs of substantive compliance for companies by working through flexible, consistent international protections will no doubt increase broad-based compliance. It is imperative that, to

[17] Austin Carr, *Google Chrome, Firefox add 'Do Not Track' Features*, CNN.com, Jan. 25, 2011, http://articles.cnn.com/2011-01-25/tech/do.not.track.features.fc_1_mozilla-google-chrome-behavioral-advertising.

[18] Julia Angwin et al., *Lawmaker Introduces New Privacy Bill*, Digits WSJ Blog, Feb. 11, 2011, http://blogs.wsj.com/digits/2011/02/11/lawmaker-introduces-new-privacy-bill/?mod=rss_WSJBlog&mod= (quoting Mr. Fowler).

[19] Responsive to QFCs listed under subheadings "Scope" and "Incorporate substantive privacy protections."

[20] FTC Staff Report, *supra* note 1, at 17.

the extent they do not unreasonably curtail the market developing privacy standards, "[m]any elements of the framework also parallel . . . international guidelines and laws governing privacy."[21]

C. Consumer Data That "Can be Reasonably Linked to a Specific Consumer, Computer or Other Device," and the Incentive for Anonymization[22]

AT&T supports the reasonable and proportionate application of privacy frameworks to consumer data that can be reasonably linked to specific consumers, computers, or devices. The distinction between PII and non-PII is increasingly complex and diminishing in its significance. AT&T already defines "Personal Information" in its Privacy Policy to include "information that directly identifies or reasonably can be used to identify an individual Customer or User."[23]

Reasonable limits, however, must apply to this definition. Security and privacy requirements should indeed be proportional to the likelihood of data being linked with an individual and the risk of harm if such data were to be linked. "Data that can be reasonably linked" should thus be interpreted to mean *non-public* data that can be *linked with reasonable effort*.

Inclusion of *public* information within the scope of the definition could result in a burdensome regime that regulates information reasonable people would have little interest in regulating.[24] In certain contexts, personal data is not always protected as "Personal Information." For example, Subscriber List Information (defined as "any information…(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses or primary advertising classifications…or any combination of such…..(b) that the carrier….has published….in any directory format') is specifically excluded from the statutory definition of – and the regulatory restrictions applicable to – Customer Proprietary Network Information (CPNI).[25]

---

[21] *Id.* at 39.

[22] Responsive to QFCs listed under subheading "Scope" and "Practices that require meaningful choice: Special choice for online behavioral advertising: Do Not Track."

[23] *See* AT&T Inc., Privacy Policy, *available at* http://www.att.com/Common/about_us/privacy_policy/print_policy.html.

[24] *See id.* ("Personal Information does not include Published Listing Information as discussed in more detail below.").

[25] *See* 47 U.S.C. § 222(h).

It will also be significant to exclude data which will not be linked with an individual because of contractual or internal controls. In certain instances, data may be intentionally anonymized for an additional layer of privacy protection, and then administrative and technical safeguards put in place to prohibit the re-association of this data. Certainly it will be important to acknowledge that data cannot be *reasonably* linked with a consumer, computer, or device when the controller of the data has affirmatively broken such links.

Moreover, privacy standards should both promote existing and future privacy-enhancing technologies that minimize the association of data with individuals and expand existing methods for anonymizing data.[26] An approach to information security, using advanced data security, anonymization, and organizational safeguards such as contractual provisions and internal controls, provides more than ample assurance that customer data will not be reasonably linked to individuals. Mathematicians will no doubt continue to demonstrate that certain otherwise seemingly non-identified data can be linked with unique individuals in particular circumstances. Business systems, however, cannot shift with every new academic paper, and must have some level of certainty in the scope of data subject to a particular classification within an organization Companies like AT&T that aggregate or anonymize data as required for business purposes should not be subject to uncertain definition "creep." Contractual provisions and internal controls combined with restricted access should be recognized as sufficiently reasonable controls that the data would be not linked.

In this regard, the FTC should recognize that robust anonymization standards, including restricted access provisions, can provide sufficient protection to justify treating the resulting data sets as non-personal information. Such standards can allow for enhanced commercial certainty and protect innovation while providing a significant incentive for companies to anonymize and aggregate information in responsible ways. The definition of "Personal Information" should thus recognize a flexible continuum that appreciates the reasonable possibility of linking any data to individuals, as well as the commitments that entities make not to engage in such linkage.

[26] The FTC proposal to extend the privacy framework to include IP addresses and other device identification information alongside PII, *see* FTC Staff Report, *supra* note 1, at 35-37, 42, is a particular source of concern. It does not appear to reflect developments in privacy enhancing data protection technologies and may well prove unworkable and inconsistent with pre-existing privacy laws. Unless significantly refined, such proposals may limit innovation while also reducing incentives for companies to maintain data in non-identifiable formats.

Companies would indeed be incentivized to consider obligating their business partners by contract to desist from any attempts at personal linkage in order to extend privacy protection.

D. Holistic Privacy by Design[27]

AT&T agrees that companies should be encouraged to promote consumer privacy throughout their organizations and at every stage of product or service development. The privacy and security implications of new products and services and related consumer protections should be considered early in the design and implementation processes, and throughout the product and service lifecycle.

AT&T also appreciates the FTC's recognition of the flexibility inherent in privacy by design. The size and scope of any privacy program must vary with the business, the type of data it collects and uses, and its use of the data. In elaborating on their vision for privacy by design, the Commission should avoid micromanaging internal business processes or being overly prescriptive by requiring the inclusion of specific privacy elements in developing products or services.

For example, because data retention periods are dependent on multiple factors, including tax, employment, and discovery considerations, the specific needs of a business, and the sensitivity of the data, it will be very difficult to prescribe a specific data retention period. Technical limitations, such as those common with legacy systems, further illustrate the importance of developing flexible, principles-based standards that can be implemented rationally and prospectively by commercial entities.

Technologies used to enhance privacy and protect data continue to evolve. The FTC rightly acknowledges the beneficial impact of recent technologies such as "identity management, data tagging tools, and the use of [TLS/SSL] or other encryption technologies" to "establish and maintain strong privacy policies."[28] These technologies have gradually come into more widespread use, and it can be expected that further developments in technology will provide even more robust privacy and data protection. Accordingly, the FTC should not tie privacy by design or privacy notices to particular technologies in existence at this point in time. Rather, the

[27] Responsive to QFCs listed under subheadings "Scope," "Incorporate substantive privacy protections," and "Maintain comprehensive data management procedures."

[28] FTC Staff Report, *supra* note 1, at 52.

Commission should develop a flexible, principles-based standard that will encourage businesses to incorporate emerging privacy technologies into their privacy protection programs.

Government-mandated Privacy Impact Assessments ("PIAs") for commercial entities could exemplify inflexible, inappropriate governmental micromanaging of technology. PIAs may well be a useful tool in achieving transparent collection and handling of personal information, but the precise process for determining how privacy impacts are accessed and managed by a business should not be mandated by government. It is entirely reasonable and appropriate for the Commission to expect that companies will consider the privacy implications of their products and services as they develop and deploy those product and services. But, it is also reasonable for the FTC to leave the format and parameters of such planning and consideration up to individual companies. A one-size-fits-all remedy will indeed undercut innovation in a number of contexts, and elevate form over substance (without increasing actual consumer protection). Indeed, restricting online businesses to a narrow format for communication with their customers about privacy will constrain rather than promote competition among companies to be relatively more privacy-protective or consumer-friendly.[29]

Industries vary considerably in the manner in which they develop new projects. In some, confidentiality and speed are paramount to maintaining competitive advantage and intellectual property rights. And different organizations, of course, have different cultures for product development. The Commission should, at least initially, rely upon non-governmental auditing and assessment functions to help companies learn about their internal data usage and measure the effectiveness of their programs. Violations of industry code by a company that has publicly subscribed to that code could be addressed as a deceptive trade practice under existing FTC authorities, but there is no need to dictate a particular internal method of oversight.

AT&T encourages the FTC to engage with industry groups and businesses to develop sectoral best practices that take into account the varied needs of different stakeholders. These principles, or other principles developed by the FTC in conjunction with Commerce and the business community, can be enforced primarily through self-regulatory regimes operated by non-governmental organizations with sufficient government oversight of the organizations to further ensure compliance.

---

[29] The FTC Report encourages companies to compete on the basis of their privacy offerings. *See* FTC Staff Report, *supra* n. 1, at *vii*. AT&T supports this proposed competition.

E. Enhancing Consumer Privacy Choices[30]

Consumer comprehension of data collection and use should be enhanced through more effective consumer outreach and greater clarity of policies. As the FTC recognizes, a primary mechanism to protect privacy is to highlight privacy choices for consumers and to encourage robust articulation of the particular uses of data that require special notice and consent. As more market players invigorate their privacy policies and enable more privacy preferences, this will in turn strengthen consumer understanding. Increased demand for privacy disclosures and commitments will then encourage and reinforce further market competition.

For privacy choices to be meaningful, however, notice and disclosures of data practices must be clearly articulated and streamlined so as not to overwhelm the consumer with unnecessary and distracting verbiage. Further development of privacy-enhancing technologies and business practices should be encouraged to provide consumers information about how and what data is collected and used, and to facilitate awareness of when personal information is being shared. With improved tools, consumers will be better-positioned to make informed choices about protecting their own privacy. In addition to more privacy choices, the Commission should encourage innovation for cross-platform permissions and authentication in the pursuit of greater security and convenience for consumers so that consumers are not forced to go through a screen of privacy options for each new website or app unless they choose to do so.

This flexible approach should also allow companies to describe the use of data within broad categories, such as "for marketing purposes," without the need to specify the particular purpose for the collection of each piece of data. Indeed, the power of Web 2.0 inter-related media is precisely that content can be used in novel ways.

It is also apparent that certain online services have thrived by providing value in exchange for commercial access and fluidity of consumer data. Consumers gain benefits from intensely personalized applications, and some may desire the convenience of highly customized features. Any policy directing a more stringent notice and consent paradigm should tread with caution to ensure that regulations do not overburden the consumer experience that has already proven commercially successful. As the FTC has recognized, innovation and competition in

[30] Responsive to QFCs listed under subheadings "Scope," "Incorporate substantive privacy protections," "Commonly accepted practices," "Practices that require meaningful choice," "Improved privacy notices," and "Reasonable access to consumer data."

online services can and should be promoted to aid diversification of privacy options.

While all privacy practices should be generally and adequately disclosed in consumer facing privacy policies, we strongly agree with the FTC that consumer understanding can be enhanced by not requiring express notice and/or choice for commonly accepted practices. The five categories identified as routine "commonly accepted practices" by the FTC are among those that would be appropriate as broadly applicable guidelines. In some areas, however, it may be helpful for industry, policymakers, and other stakeholders to come together through the Commerce Office of Privacy Protection to formulate industry-specific, customary use examples to provide further guidance. Such identified "commonly accepted practices," however, should serve as illustrative examples as a guide for industry compliance, rather than as an exhaustive list hemming in new and innovative practices and requiring extensive and burdensome justification if one varies from it.

AT&T agrees with the Commission that the following practices should be considered commonly accepted: (1) product and service fulfillment, (2) internal operations, (3) fraud prevention, (4) legal compliance and public purpose, and (5) first-party marketing.[31] This list, however, may be more useful in certain industries, while other industries may have their own customary practices, commonly accepted within their field. The FTC's initial efforts to identify commonly accepted practices should thus serve as a starting point for collaboration with industry to formulate further, industry-specific commonly accepted practices. Indeed, it will be important to provide examples of the types of activities contemplated by these categories:

- *Product and Service Fulfillment.* Product and service fulfillment should include providing data to third parties for service fulfillment or internal operations, like sending a phone number to another carrier for portability purposes. Moreover, practices that support the basic functionality of a website, including serving advertisements (providing non-targeted advertisements according to a particular user's preference) and loading other features of the website are common. To work properly, website functions frequently require the collection and use of the user's IP address, as well as clickstream data or browser settings associated with the user's preferences. These actions are now basic

[31] FTC Staff Report, *supra* note 1, at 53-54.

functions of consumers' interaction on the Internet. Providing choice mechanisms before a webpage loads is impractical and will negatively impact the user experience.

- *Internal Operations.* Commonly accepted practices relating to internal operations should include practices used for the improvement of a provider's services. For communication services providers like AT&T, this may include practices that use location data to determine where calls are dropped or where issues arise in network traffic, or that use information pertaining to types of internet usage over periods of time for network operation and planning purposes. Basic Internet operations necessary for the functionality of the Internet should also be considered internal operations that need not be disclosed. For example, it is necessary to collect certain online data such as clickstream data, browser headers, and some cookie data for the basic functionality of the Internet, to load web pages and serve non-targeted advertising. It could be helpful, however, to develop a common technical understanding of these practices to avoid inadvertently favoring one technology over another.

- *Network and Cyber-Security.* The protection of customers and critical national infrastructure for hacking and cyber attack should certainly be accounted for as a common practice. Ensuring the security of the network in order to protect the privacy of consumers, the rights and property of the carrier, and the data on the network is likewise an essential element of normal internal operations, as ECPA and the state wiretap laws have recognized for years.[32] In this regard, use of information to identify and disrupt viruses, malicious code, and spam should be deemed normal internal operations. Likewise, efforts to monitor and optimize network performance, route traffic, and maintain optimal resource usage levels should be recognized as a common practice.

- *Fraud Prevention.* Commonly accepted practices relating to fraud prevention must take into account the fact that modern fraud prevention involves the accumulation and scanning of vast data sets for irregular or suspicious activity in order to detect patterns suggesting conduct worthy of further investigation.

[32] *See, e.g.*, 18 U.S.C. § 2511(2)(a).

- *Legal Compliance and Public Purpose*. This category should include duties to comply with legal process, the conduct of internal investigations, the assertion and development of legal positions, and other activities in good faith furtherance with legal proceedings.

- *Corporate Transactions.* It will also be important to recognize that the orderly functioning of capital markets should result in routine corporate transactions being allowed without express notice and choice. Indeed, most privacy policies now include disclosures for corporate sales, reorganizations, and bankruptcies, but it is unclear that these disclosures provide any ascertainable benefit to individual consumers who obviously cannot be informed of potential corporate transactions before due diligence and negotiations have concluded and the deal has become public.

- *First Party Marketing.* AT&T agrees with the FTC's inclusion of first party marketing in its list of commonly accepted practices. This category should include contextual marketing, where the first party has selected advertisements for its customers based on their activity on its website, such as their use of related search terms. Co-branding and joint ventures should also be considered first parties for the purposes of marketing: whenever it is *apparent to users* that certain sites are related, the first party rules should apply. This approach avoids corporate gamesmanship, and leaves the FTC free to enforce against unfair or deceptive business practices in this regard. First-party marketing should extend across particular platforms and include both online and offline contexts. Subject to medium-specific laws, such as CAN-SPAM, businesses should be able to engage with customers through email, text messages, mobile alerts, or in-store promotions, and should not be limited to communicating through the means by which the customer relationship began. Existing opt-out laws already provide consumers with significant control over such marketing communications, and businesses often may provide consumers with even more personalized control over the means through which they may be contacted.

AT&T likewise generally agrees with the FTC that certain practices should fall outside of the commonly accepted practices.[33] The industry is currently working to improve choice mechanisms for these practices: for example, the implementation of the Digital Advertising Alliance ("DAA") industry guidelines will soon place targeted advertising icons on targeted advertisements, providing consumers a place where they can exercise their preferences with respect to receiving such advertisements. Likewise, increased implementation and use of online "profile managers" may provide consumers with simple, interoperable mechanisms to manage data sharing choices and options across websites and internet and mobile platforms.

This work by industry groups is particularly important when the distinction between first parties and third parties blurs as a result of the varying interactions between different companies in the delivery of online advertising. The FTC's approach may be strengthened, and provide more advantages to consumers, by a focus on the relatedness of the marketing and the product or service at issue, rather than on the distinctions between parties. Certainly, one major challenge facing the FTC and industry is to ensure that any policy framework developed includes all entities in the data collection and use chain. All entities involved in Internet advertising, including advertising networks, search engines, and ISPS, should adhere to a consistent set of privacy principles.

With respect to deep packet inspection ("DPI"), it is worth noting that DPI is generally not deployed extensively for advertising purposes, and AT&T has long held that it will engage in the use of DPI for behavioral advertising only with the express consent of its customers.[34] But other technologies, such as automated scanning of the text of email messages to serve targeted advertising, and use of certain tool bars or browsers that can also track all of a user's online activity, web browsing and search activity. The DAA guidelines recognize this fact, and require

[33] FTC Staff Report, *supra* note 1, at 55-56.

[34] *See* AT&T Inc., Privacy Policy, *supra* note 21 ("AT&T does not currently use technologies available to Internet Service Providers, such as deep packet inspection, to track your web browsing activities across the Internet for the purpose of tailoring advertising that could be relevant to you. If AT&T ever decides to use technologies such as deep packet inspection to provide personalized advertising, you have our commitment that we will protect your privacy and provide you with value in exchange. Specifically, we will give you notice and provide easily understood tools to allow you to exercise meaningful consent before we use such information for advertising purposes.").

that any technology which tracks all or substantially all a users web browsing and search activity obtain consent after a clear, meaningful, prominent notice presented to the consumer.[35]

F. "Just in Time" Choice[36]

AT&T supports the FTC's efforts to require choice at the correct time and in the context where it can be most meaningful for consumers. Customers are best served when there is transparency and choice regarding the collection and use of their information at the time it is collected and used. Treating these choice mechanisms as part of the features of a product, rather than as a legal disclosure, holds the most promise for providing consumers meaningful choice.

For example, Apple's innovation with respect to location-based services provides a useful model for asking consumers, application-by-application, whether they want to use location features, and then selectively incorporating these features into the user experience.[37] This practice seems particularly helpful for consumers since certain services—such as applications finding friends, hotels, taxis, or restaurants, or applications aiding in navigation—are inherently location-based, while others may only use location information to target offers or information. AT&T's Buzz.com offers another example of how effective disclosures may work. Buzz.com incorporates the selection of a user's sharing preferences into the sign-up process, rather than registering users with default preferences and then requiring them to seek out the settings page to personalize their use of the site.[38]

The FTC should acknowledge and further encourage the industry developments already being made for just in time notice. Industry-developed standards, such as the CTIA Location Based Services ("LBS") best practices and guidelines can provide for user notice, consent, and

---

[35] Specifically, the guidelines require consent "in response to a clear, meaningful, prominent notice regarding the collection and use of data" prior to providing a customer with online behavioral advertising. Digital Advertising Alliance, Self Regulatory Principles for Online Behavioral Advertising: Implementation Guide 13 (2010), *available at* http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf .

[36] Responsive to QFCs listed under subheading "Practices that require meaningful choice."

[37] Apple iOS 4.2 provides users the ability to turn off location use application-by-application and provides just-in-time notice of the use of location tracking by displaying a small arrow within the application. Apple, Inc., iOS 4.2 Software Update for iPad, Nov. 22, 2010, http://support.apple.com/kb/DL1060 .

[38] *See* Buzz.com, How you can control the information you share on Buzz.com, http://buzz.com/sharing; Buzz.com, Sign up to get started on buzz!, http://buzz.com/signup.

safeguards.[39] In addition to the CTIA LBS guidelines, the Center for Democracy and Technology and Future of Privacy Forum are examining further means by which industry may provide meaningful and timely choice to consumers. At this point in time, however, prescribing specific, codified requirements may freeze the development of further disclosure and choice mechanisms and thwart improvement in this area.

G. Do Not Track[40]

Commensurate with AT&T's commitment to consumer choice, AT&T generally supports a reasonable and thoughtfully implemented mechanism for consumers to surf in private. There are, however, potential pitfalls along the way to implementing a Do Not Track ("DNT") system. Any such mechanism must not be allowed to eliminate the benefits of personally tailored, or customized advertising – or unduly inhibit the relatively free flow of information on the Internet. To proceed otherwise could contravene the policies advanced by the President and Congress, as noted at the outset of these comments, and conflict with the powerful positive dimensions of new technology that the FTC report acknowledges, such as the "explosion of new business models that depend upon capturing consumer data at a specific and individual level and over time, including online behavioral advertising, social media services, and location-based mobile services. . . . [which] developments can provide enormous benefits to consumers."[41]

As Chairman Liebowitz noted in the press conference announcing the FTC Staff Report, many consumers—himself included—find great value in personalized advertising on the web and may refrain from using a DNT mechanism.[42] AT&T applauds the FTC for emphasizing in the Staff Report that the DNT system should not substantially interfere with consumer choice or with the primary mechanism for funding many otherwise "free" online services and content. AT&T agrees with the Staff Report that new technologies and business models aimed at

---

[39] *See* CTIA - The Wireless Association, Best Practices and Guidelines for Location Based Services, *available at* http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

[40] Responsive to QFCs listed under subheading "Practices that require meaningful choice: Special choice for online behavioral advertising: Do Not Track."

[41] FTC Staff Report, *supra* n. 1, at 21.

[42] *See* Daniel Lyons, *Don't Track Me, Bro*, Newsweek, Jan. 4, 2011, *available at* http://www.newsweek.com/2011/01/04/making-sure-net-advertisers-do-not-track-you.html.

"capturing consumer data at a specific and individual level and over time . . . can provide enormous benefits to consumers, including instant, around-the-clock access to products and services, more choices, lower prices, personalized content, and the ability to communicate and interact with family, friends, and colleagues located around the globe."[43]

A DNT mechanism accordingly should not disrupt the use of cookies or similar technologies for purposes unrelated to behavioral advertising, such as cookies employed for security, site analytics or user recognition. Indeed, a DNT mechanism should not focus exclusively on cookies, as there are many other existing technologies that can track web browsing and search activity over time, and still others will no doubt be invented. The DNT mechanism likewise should not simply provide an all-or-nothing choice for consumers, but should instead allow consumers to exercise more granular control over which entities may collect and use information about their web browsing and search activity.

Because of this, the DNT mechanism should require that all relevant entities within the information ecosystem participate. The DNT mechanism should not unduly burden businesses which have direct customer relationships particularly where businesses that have no relationship with the customers frequently engage in the most aggressive tracking. Any implementation of the DNT mechanism should provide adequate time for entities to recognize and implement customer preferences.

H. Transparency and Clarity Are Essential for Privacy Protection[44]

We agree that consumer privacy policies in general should present more information and clearer choices than commonly offered today. AT&T pursued this essential transparency when consolidating its former policies into a new easily accessible, consumer friendly and multi-media Privacy Policy in 2009. And AT&T is not alone in its outreach to consumers to provide more information in easy to understand mediums. Innovative approaches to engaging consumers through increased transparency and control tools emerging in the marketplace can serve as models for the next phase in the evolution of privacy practices. The privacy policy approach to notice and choice will continue to improve with practical, consumer-focused innovation.

[43] FTC Staff Report, *supra* note 1, at 21.

[44] Responsive to QFCs listed under subheadings "Maintain comprehensive data management procedures," "Practices that require meaningful choice," "Improved privacy notices," "Reasonable access to consumer data," "Material changes," and "Consumer education."

To encourage further consumer engagement and transparency, safe harbors should be developed and recognized to provide incentives for companies to incorporate strong privacy principles into their practices and to describe their data practices fully in privacy policies and other notices. These safe harbors would ensure that complying entities' privacy practices would be presumptively deemed to be in compliance with applicable standards for conduct that is not "unfair or deceptive," and in compliance with future industry codes. Further, if consumers understand data practices, they can determine for themselves whether or not they are comfortable doing business with a company. Consumer choices should be simplified, and options should be responsive to consumers' expectations.

While AT&T agrees with the need to evolve consumer choice, the Commission should not eliminate those aspects of notice and choice that enhance consumer education, specifically the familiarity of knowing where to locate information on privacy practices, the flexibility to customize privacy policies to a particular entity's products and technologies, and the ability to tailor privacy policies to reflect industry-specific particularities.

The ability to explain privacy and information practices in a privacy notice is particularly important when new technology may be using data in novel ways. As the FTC resolution *In the Matter of Sears Holding Management Corporation*[45] made clear, companies making especially intrusive uses of personal information should provide especially clear notice and choice. Privacy policies are the most direct and expected means for which consumers look for this information. Likewise, based on the accepted practice of publishing privacy policies, the privacy community reviews and analyzes these privacy disclosures, and provides an additional source of information and perspective for consumers. Implementation of the proposed framework should not undercut the ability of businesses to provide tailored notice and choice to consumers – and for consumers to thus benefit from a wide array of service options.

AT&T believes that the general adoption of an overly-simplistic model format for privacy disclosures and notices would be counter-productive, and agrees with the White House on the importance of "considering flexible approaches and alternatives to mandates, prohibitions, and command-and-control regulation."[46] Model privacy notices could prevent businesses from

[45] *In the Matter of Sears Holding Management Corporation*, FTC File No. 082 3099, *available at* http://www.ftc.gov/opa/2009/09/sears.shtm.

[46] Memorandum from Cass R. Sunstein, *supra* note 3, at 3.

developing more helpful, readable, and practical privacy notices, tailored for that particular industry and their customers' needs. It would also be unfortunate if companies were forced to constrain their information practices to conform to one-size-fits-all model notices, for that would surely stifle innovation.[47]

The AT&T Privacy Policy provides its customers with simplified statements, focused on its telecommunications products and services, concerning its data practices and the general nature of how data will be used, along with specific examples. AT&T also provides FAQs and other interactive features to explain its privacy practices. Not all online entities, however, are in the same position as AT&T. Other industries may involve less interconnectivity, more limited data, more sophisticated or institutional data subjects, or may not require the same degree of external protection. For instance, banks, healthcare companies and telecommunications companies exist in different information ecosystems, and it would certainly not be appropriate to force them into using the same form of privacy notices. One size does not fit all for privacy policies, particularly across industries, because privacy is dependent on the nature of the relationship at issue and policies should not be forced into Procrustean standardization.[48] It is also important to recall that global enterprises frequently must comply with requirements in other privacy regimes that require very robust and specific notices. It will be important to preserve the ability of US companies to comply with these requirements, while also providing information as concisely and directly as possible.

Further, it is difficult to see the realistic possibility of standardizing privacy policy disclosures given the fast moving nature of the telecommunications, technology and Internet based industries. With so much opportunity for innovation of privacy features, dedicating significant resources to the specifics of a model general notice would be misguided. Rather, companies should be encouraged to continue to experiment with plain language and format

---

[47] Indeed, Executive Order 13,563, *supra* note 6, "emphasizes the potential value of approaches that maintain freedom of choice and improve the operation of free markets (for example, by promoting informed decisions). It directs agencies to consider the use of tools that can promote regulatory goals through actions that are often less expensive and more effective than mandates and outright prohibitions. When properly used, these tools may also encourage innovation and growth as well as competition among regulated entities." Memorandum from Cass R. Sunstein, *supra* note 3, at 3.

[48] For instance, the model privacy notice form for financial institutions governed by the Gramm-Leach-Bliley Act, developed by the FTC in collaboration with other regulators, illustrates how one industry's standard may not prove effective elsewhere. Federal Trade Commission, Federal Regulators Issue Model Privacy Notice Form, Nov. 17, 2009, http://www.ftc.gov/opa/2009/11/glb.shtm.

varieties to improve their policies and consumer comprehension, as AT&T did in 2009, and continues to do in regular reviews and updates.

Of course, to the extent that model privacy forms or notices were truly optional tools or resource materials that could be adapted by smaller entities, or businesses with less complex practices, that would be reasonable and helpful. It should be made clear, however, that companies that develop and comply with more comprehensive privacy policies do not have to justify their decisions not to use the models, or to modify or supplement any model language, but rather should be held to the standard of whether their policy provided effective and clear notice to a reasonable consumer. Company resources are more efficiently allocated towards further privacy enhancing innovation than toward the development of model forms or the need for producing legalistic justifications for using or not using model forms.

Accordingly, AT&T encourages the FTC and the Department to work with industry representatives to continue to examine methods for developing industry-specific standards for privacy disclosures. This will allow businesses to provide adequate and pertinent information to consumers while ensuring that the myriad specific needs of each particular industry are not neglected in the process.

We should be clear, however, that consumer comprehension can certainly benefit from shorthand icons or indicators to reflect a simplified gradient of privacy practices in the appropriate circumstances. For instance, a consumer "traffic light" on a browser could show green for a site with only commonly accepted uses, yellow to alert consumers of sharing outside the first party organization, and red for sharing with unaffiliated third parties without an opt-out or not having a privacy policy. This would also aid consumer comprehension when transitioning among websites controlled by different entities, who may have vastly different privacy practices. AT&T supports such innovations, and it encourages approaches that maintain the technology neutrality and flexibility required for them.

Civil society and industry have already begun developing a sample of this type of consumer shorthand indicator. The Targeted Advertising Cookie Opt-Out ("TACO") technology provides one potential model.[49] The Commission's suggestion of a persistent

[49] *See* Mozilla.org, Targeted Advertising Cookie Opt-out (TACO) 3.51, *available at* https://addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/ (providing users with persistent opt-out settings and real-time information on online tracking and monitoring). *See also* FTC Staff Report, *supra* note 10, at D-2 (concurring

browser cookie to convey personal privacy settings to visited sites is also a reasonable possibility. Internet ads with granular information apparent under an icon are also helpful. The Internet Advertising Bureau has unified the presentation of the Network Advertising Initiative opt-out tool, and adopted an icon that will be used throughout the industry to increase transparency.[50] AT&T is helping to build on this momentum by working to trial an icon in certain ads.[51] Moreover, AT&T has formed a national Consumer Advisory Panel to enable a collaborative dialogue aimed at addressing concerns and receiving feedback on a wide range of consumer-oriented issues from representatives of core constituencies of AT&T customers and leading consumer groups from across the country. At core, however, it remains most important to appreciate that the process of developing new methods of communicating transparently will necessarily be tied together with particular technologies that continue to evolve rapidly.

I. Consumers Should Have Reasonable Access to Data About Them[52]

AT&T supports efforts to allow consumers reasonable access to data about them, and companies should surely be challenged to determine the extent to which they can reasonably grant consumers access to their data in the context of that company's specific business operations. A universal approach to consumer access, however, would likely be an inadequate solution for the diversity of information ecosystems. Rather, specific industries should be looked to develop norms for access consistent with their information systems, and consumer access to data should be subject to a rule of reason. Many of these rights face technical limitations in legacy networked systems. For example, phone records can be generated for particular numbers or accounts, but access to all references to a consumer name within a telecommunications

---

statement of Commissioner William E. Kovacic) ("The increasingly widespread use of privacy controls such as NoScript and TACO—a development the report cites—might suggest that firms are working to meeting consumer demands for privacy.").

[50] *See* National Advertising Initiative, Opt Out of Behavioral Advertising, *available at* http://www.networkadvertising.org/managing/opt_out.asp.

[51] *See* Diana Dilworth, *AT&T To Test Transparent Internet Banner Ads This Month*, Direct Marketing News, July 2, 2010, http://www.dmnews.com/att-to-test-transparent-internet-banner-ads-this-month/article/173657/.

[52] Responsive to QFCs listed under subheadings "Scope," "Incorporate substantive privacy protections," "Maintain comprehensive data management procedures," "Practices that require meaningful choice," "Improved privacy notices," and "Reasonable access to consumer data."

company's system and infrastructure would be enormously burdensome.[53] Companies in many industries rarely have one singular data system that can be queried for all information about a given individual. Further, not all customer-related data held by a company is useful or interesting for consumers.

The cost to require all companies to retrofit the architecture for an access system for any application would be enormous and likely disproportionate to any resulting consumer benefit. While next generation systems can, in many circumstances, be designed to include these sorts of reporting functions, current technology often does not allow for cost-effective searching across platforms. Indeed, this issue is one of the many ways in which it is clear that privacy by design principles are an important aspect of ensuring future privacy rights. If the engineers know in the design phases that consumer information will need to be subject to access rights, they can build interfaces into the systems frequently at a fraction of the cost of bolting privacy protections onto an already designed project. For instance, profile managers built into systems can get consumers real access to and choices about personal data in a form that is far more meaningful than a data dump from their cookies. Thus, rather than require a one-size-fits-all capacity for full data histories, companies should be allowed to respond to consumer requests by reasonably accommodating requests commensurate with their specific data infrastructure. Further, companies should be allowed to recover costs, including overhead for administering access systems, in responding to requests.

J. Material Changes Should be Disclosed[54]

Transparency likewise demands that consumer receive notice of material changes to privacy policies. Particularly given the rapid evolution of information collection and sharing technologies – as well as the dynamic legal environment – companies appropriately reserve the right to update their privacy policies as they make changes that are necessary to reflect technological changes and to satisfy legal requirements. The "materiality" of such changes is often uncertain, and so companies may feel obligated to treat uncertain minor changes as material – despite the fact that such over-reporting of changes serves only to numb consumers to

[53] The Internet Advertising Bureau provides one excellent example of a trade association's consumer education initiative. *See* Interactive Advertising Bureau, IAB: Privacy Matters, http://www.iab.net/privacymatters/.

[54] Responsive to QFCs listed under subheading "Material Changes."

truly material changes by over-loading them with superfluous information.

Consumers receive adequate notice of material change to privacy policies when prominent notice of changes is posted on the relevant web site, and consumers are given appropriate notice and opt-out choice regarding the proposed future uses of their information, at least 30 days before the effective date of the changes. Affirmative opt-in consent to changes may be appropriate for material changes in the use of particularly sensitive health or similar personal information, but material changes in the use of non-sensitive personal information can be appropriately addressed through the provision of clear notice of the changes and a real choice to exclude data from the new uses of data proposed in the revised privacy policy.

K. Consumer Education Is Crucial[55]

Engineers, product developers, marketing specialists, lawyers, and policy makers must all appreciate that we face a challenge to create mechanisms to communicate information and educate consumers about new technologies and information practices. Privacy choices must become transparent enough that consumers can express their privacy preference even when they may not fully appreciate the technologies they are using. Written notices of privacy practices are an important form of education, but can provide much more utility when presented in an easily accessible, consumer friendly context, such as in innovative multimedia presentations. Particularly in industries that have not been historically subject to regulation, the education of programmers, engineers, and business leaders about their responsibilities for protecting privacy is also a crucial need.

Privacy policies also force thoughtful and detailed corporate transparency by requiring a company to make a formal statement of its practices. Privacy advocates in civil society also play an important role in educating the public about the privacy dimensions and implications of new technologies, practices and business models. Indeed, these groups provide careful scrutiny of the privacy policies and practices of all major online businesses, and help inform and alert the public about changes, new developments and areas of potential concern. The Commission and

[55] Responsive to QFCs listed under subheadings "Scope," "Maintain comprehensive data management procedures," "Improved privacy notices," and "Consumer education."

Department should likewise engage in public education campaigns to ensure that consumers have access to resources that help explain Internet practices from a neutral point of view.

AT&T supports the continued need for consumer education and awareness, which is a hallmark of AT&T's privacy program. In 2009, AT&T overhauled its consumer Privacy Policy to consolidate policies across AT&T services. This new Policy provided an easily accessible, consumer friendly notice to give more detailed information to consumers who want to learn more about the AT&T information ecosystem. AT&T explored the use of multiple media to provide this information in a variety of easily understood deliveries, including short form high level policy points, as well as the long form privacy policy, topic specific short videos, and consumer Frequently Asked Questions. AT&T chose this approach to satisfy the variety of consumers who seek information, with an appreciation of how multi-media content can be particularly effective in reaching different segments of the consumer population. AT&T's Smart Controls website provides comprehensive access to information about AT&T safety and control tools, expert resources and tips designed to help customers manage their technology choices and address safety concerns about their children's use of AT&T products and services.[56]

AT&T also collaborates with third parties to support online safety and privacy education initiatives tailored for children, middle and high school students, seniors and others. For example:

- AT&T supports a privacy education initiative for middle and high school students launched by KeepSafe, working along with the American School Counselor Association to bring important privacy lessons to students, in order to help them build positive online reputations for their future. To date, more than 4,200 counselors and educators have sought out the materials for use in their schools.[57]
- Based on research by the Rochester Institute of Technology, AT&T also has sponsored iKeepSafe and their public health partner, Harvard's Center on Media and Child Health (CMCH), to create educational objectives and curricula that includes privacy and other effective messages in virtual world experiences for children ages 8–11.

[56] For more information, see AT&T Inc., AT&T Smart Controls, http://www.att.net/smartcontrols.

[57] For more information, see iKeepSafe.org, iKeepSafe Educators, http://ikeepsafe.org/iksc_educators/.

- AT&T also recently announced *Mobile Safe Kids™,* a major collaborative effort to promote safe, healthy, and responsible mobile phone use both on and offline, and to reduce mobile phone victimization of children.
- AT&T is a sponsor of the Enough is Enough Internet Safety 101^{SM} program, which the organization created in partnership with the U.S. Department of Justice. Internet Safety 101^{SM} is a resource and teaching series that educates and empowers parents, educators and other adults with the necessary information to protect children online. It includes information and instruction on myriad issues including privacy, parental controls and effective communication.
- AT&T helped support the development of "Online at Woogi World," a virtual educational platform, children will experience and complete interactive *missions* designed to help them identify and choose healthy, ethical, and responsible mobile phone use.
- In addition, under its MAC (Mature Adults Connected) Initiative, AT&T provides a cyber safety educational program for mature Americans, *Safe Surfing,* at various cities throughout the country, presenting tips and support to approximately 2,500 seniors. MAC also helps mature adults stay connected by teaching them how to use their wireless devices more safely and efficiently—more than 3,500 senior consumers have had individual "coaching" sessions on how to operate their wireless devices. OASIS, one of the senior organizations we support, helped develop the model for this program and it is now available throughout the country with groups like SeniorNet and the National Center and Caucus on Black Aged providing sessions to its members. AT&T has also included sessions tailored to Spanish-speaking seniors. Most recently, we have helped seniors learn how to safely explore social networking sites so they can better stay connected to friends, activities and resources. Collectively, we have helped more than 6,000 seniors learn to stay safer and protect their privacy in the digital word.

Based in part on these educational activities and privacy practices, in February 2010, AT&T was named one of the Most Trusted Companies in Privacy by the Ponemon Institute.[58]

AT&T's efforts are an example of the many industry initiatives around privacy and consumer outreach, and the Commission can help support these initiatives by encouraging and supplementing these efforts.

[58] *See* Ponemon Institute, Ponemon Survey Names Twenty Most Trusted Companies for Privacy, Feb. 26, 2010, *available at* http://www.ponemon.org/news-2/26.

CONCLUSION

AT&T applauds the work of the Commission in driving this discussion forward, and looks forward to participating in the continued industry collaboration contemplated by the Report. AT&T remains committed to fostering greater consumer understanding of technology and of consumer privacy choices, and will work together with both the Commission and the Department, as well as other stakeholders in the community, to continue promoting a reasonable and effective privacy framework that encourages innovation and consumer confidence.

Respectfully submitted,

Alan Charles Raul
Edward R. McNicholas
Colleen Theresa Brown
Jonathan P. Adams*
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Counsel for AT&T Inc.

Paul K. Mancini
Keith M. Krom
Theodore R. Kingsley
AT&T INC.
1133 21st Street, N.W.
Washington, D.C. 20036
(202) 463-4148

Kelly Murray
AT&T Services Inc.
208 S. Akard Street
Dallas, TX 75202
(214) 757-8042

February 18, 2011

* Admitted only in California.