Before the

DEPARTMENT OF COMMERCE
Internet Policy Task Force

In the Matter of	)
	)
Commercial Data Privacy and Innovation in the	)
Internet Economy: A Dynamic Policy Framework	)
	)
	)

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

January 28, 2011

* Admitted only in California

Table of Contents

Introduction

AT&T Inc. ("AT&T"), on behalf of itself and its affiliates, is pleased to provide these comments on the green paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (the "Green Paper") issued by the Department of Commerce (the "Department" or "Commerce"). AT&T also anticipates providing comments to the preliminary staff report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (the "Report") issued by the Federal Trade Commission (the "FTC" or the "Commission"). Given the similar subject matter of these frameworks, AT&T's comments to the Department's Green Paper also address some overlapping issues in the FTC Report.[1]

We submit these comments to the Green Paper with consideration of the FTC's Report in order to emphasize a fundamental goal – no doubt broadly shared in the government, in the private sector, and in civil society – that all federal agencies adopt consistent and effectively coordinated approaches to privacy based on flexible principles that can be adapted as appropriate to each of the various sectors of the economy. 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.

We commend both the Department and Commission for their 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*

[1] AT&T will provide the Department of Commerce with a copy of its response to the FTC's Report when it is filed with that agency.

Journal (Jan. 18, 2011), it is crucial that the public be protected while freedom of commerce is preserved:

> 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.

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."[2]

Both the Commission and the Department have been 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. While the papers issued by the Department and the Commission do not propose regulations, we believe both agencies should continue to put into practice this philosophy of public participation, dialogue, predictability and respect for innovation. As the President's recent Executive Order expresses:

> 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

[2] 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.

> understand. It must measure, and seek to improve, the actual results of regulatory requirements.[3]

AT&T is fully committed to participating in this open and inclusive process that will ensure the Internet continues to create new ways for people to connect and share information in all aspects of their lives. We are particularly pleased to recognize that the Department and Commission share this commitment, as reflected in several of their statements expressed in the Green Paper and Report, such as:

> - Commercial data privacy policy must be able to evolve rapidly to meet a continuing stream of innovation. A helpful step would be to enlist the expertise and knowledge of the private sector, and to consult existing best practices, in order to create voluntary codes of conduct that promote informed consent and safeguard personal information. Multi-stakeholder bodies, in which commercial and non-commercial actors participate voluntarily, have shown that they have the potential to address the technical and public policy challenges of commercial data privacy. . . .
>
> - Consistent with the general goal of decreasing regulatory barriers to trade and commerce, the U.S. Government should work with our allies and trading partners to promote low-friction, cross-border data flows through increased global interoperability of privacy frameworks. . . .
>
> - A reinvigorated approach to commercial data privacy must be guided by open government inspired consultation; it can work only with the active engagement of the commercial sector, civil society, consumers, academia and the technical community. . . .

[3] 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. *See, e.g.,* 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).

- In hosting the roundtables, the Commission sought to evaluate how best to protect consumer privacy, while also preserving the ability of companies to innovate, compete, and offer consumer benefits. . . .

- By clarifying those practices for which enhanced consumer consent is unnecessary, companies will be able to streamline their communications with consumers, reducing the burden and confusion on consumers and businesses alike.[4]

We agree with the efforts of the two agencies in their intention to refine data protection in the United States. We believe that the current federal-state system for setting and enforcing standards for privacy and consumer protection is generally effective. The FTC, federal banking, healthcare and communications regulators, state attorneys general, and private litigants – combined with meaningful self-regulation by industry associations and individual companies – have produced a dynamic and rigorous data protection regime for the United States, that we should consider second to none internationally. Although U.S. standards will continue to be refined and new challenges will appear, we urge the agencies not to lose sight of what has been working well. Continuing this approach through the flexible and balanced frameworks being developed and coordinated by Commerce and the FTC, especially in light of the dynamic pace of technological innovation, has served the public well.

This coordination should also help the United States to better articulate its principles in a consistent and forceful manner to the international community. A coordinated framework may advance the European Union's understanding of the Unites States' approach and ultimately allow the EU to determine that the U.S. data protection regime is "adequate." This will foster global interoperability of communications networks and databases, which, as recognized by the Department, is of vital concern for multinational companies as well as the customers, employees and stakeholders they serve. We look forward to the continued development of the open and thoughtful exchange of ideas represented by the Department's Green Paper and the Commission's Report.

[4] 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"].

Executive Summary

The Department's Green Paper, as well as the Commission's Report, are particularly significant at this important time in the development of policymaking regarding the Internet. AT&T is pleased that both of these analyses expressly recognize and appreciate 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 have 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 is grounded in four pillars – transparency, consumer control, privacy protection and consumer value. We understand our standards to be entirely consistent with both of the proposed frameworks. We are thus generally supportive of both the Department's and Commission's preliminary frameworks, particularly to the extent that they are predicated on flexible performance standards that will evolve over time with technologies and business models that encourage innovation.

The expression of generalized privacy principles can play a useful role in framing industry-specific standards, but we should not ossify any specific unduly prescriptive iteration of Fair Information Practices Principles ("FIPPs") reflecting only current concerns with current technologies—surely to become obsolete within a matter of years—or as a one-size-fits-all, inflexible approach to privacy. Rather, FIPPs are usefully expressed as generalized policy guides that should shape the multi-stakeholder collaborative processes to develop flexible and contextualized codes of practice for particular industries. FIPPs can thus play an important role in setting the agenda for voluntary and enforceable codes of conduct, as long as they do not attempt to micromanage technology.

Throughout these processes, we have noted and wish to emphasize the need for a continuing commitment of both the Department and the Commission to remain neutral toward particular current technologies. This 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 supports an "adequacy" determination by the EU
- 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
- Will lead to appropriate national data breach notification standards that give consumers meaningful notice of actual risks of harm
- Work to update ECPA to reflect new technologies, including location-based services and cloud computing.

While these frameworks have provided enhanced clarity on these issues, we are pleased that the Department and the Commission have taken 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."[5]

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

General Comments for Both the Department and the Commission

A. A Call for Enhanced Federal Coordination

Although both the Green Paper and the Report offer significant new perspectives, it is important to ensure consistency in basic understanding about privacy so as to provide meaningful consumer protection without giving rise to duplicative standards that could burden compliance but not increase protection. Consumers approach the Internet with a consistent set of expectations, and they should be able to traverse the Internet having those expectations respected and enforced. Inconsistent frameworks also harm business by introducing uncertainty into business planning, entail undue costs, and discourage innovation.

Significantly, the new frameworks arise within a complex regulatory system that already provides some standards for data protection throughout the economy. Overarching federal and state legal obligations under the FTC Act, 15 U.S.C. §§ 41-58, and state UDAP statutes, such as Cal. Civ. Code § 1750 et seq., N.Y. Gen. Bus. Law §§ 349, 350, and Fla. Stat. Ann. §§ 501.201 - 501.213, proscribe unfair and deceptive business practices. Sectoral laws impose specific requirements on banks and financial institutions, healthcare providers, and certain communications services. General common law norms continue to evolve. And enforcement can come from several different federal agencies, state agencies, or through class action suits – not to mention international regulators. The interrelation between these laws can breed a needless complexity and an uneven playing field. Maintaining consistency, ensuring technological neutrality, and eliminating gaps within this framework are important both for providing substantive privacy protection and incentivizing innovation.[6]

Given the benefits of coordinated, neutral policy and flexible general principles, we are pleased that the Department has suggested that it can and should play a significant leadership role in working with industry and all stakeholders, coordinating the various regulators and engaging with international counterparts. We believe that the substantive goal of ensuring genuine, cost-effective data protection for the public is broadly shared among all regulators,

[6] Responsive to Requests for Comment (1), (35), (36), and (37). Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 80,042, 80,044 (Dec. 21, 2010) [*hereinafter* "RFC"].

responsible businesses and leading advocates in the privacy community. A difficulty, however, has been to reconcile the numerous different approaches in a manner that emphasizes actual privacy protection and accountability over unnecessary regulatory friction, rigidity and bureaucracy.[7]

An Office of Commercial Privacy Policy could be a helpful convening and reconciling authority, especially in light of the limits of the jurisdiction of various regulators. Multi-stakeholder, industry-specific processes could result in flexible, customized codes that account for variations in evolving technologies, the speed of innovation, the variations in applicable regulatory regimes, and the specific harms faced by different industries. Given the considerable efforts by the FTC in convening stakeholders to focus on these issues to date, the Commission should play a significant role in these continuing discussions, in addition to its existing enforcement role in ensuring that industry considers and protects the public interest.[8]

Coordination on the federal level would be undermined, however, if states impose conflicting requirements that unreasonably interfere with interstate business. State attorneys general will benefit from increased coordination with federal regulatory agencies, and will continue to have a robust role policing the promises that companies have made regarding the use of consumer information. The primary regulation, however, should stem from industry codes of practice, developed through coordination as suggested by the Department, and compliance with these codes should afford companies a safe harbor against both federal and state claims of unfair and deceptive trade practices.[9]

[7] Responsive to RFC (1) and (2).
[8] Responsive to RFC (1), (2), (3), (5) (17), and (19).
[9] Responsive to RFC (1), (2), (3), (5), (6), (15), (17), (19), (27), (36), (37), and (38).

B. Ensuring Proportional Policy and Standards

The free flow of information on the Internet, along with sophisticated advertising and data analysis, provides significant value for consumers and the economy.[10] Government approach 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 Department to make a concerted effort to understand and, if possible, to quantify these benefits, and to strive to preserve or enhance such benefits in recommending privacy standards.[11]

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 obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations." Executive Order §1(b).[13]

Implementation of new privacy frameworks should occur in a manner that ensures flexibility and avoids micromanaging how individual companies conduct their businesses and contract with their customers.[14] Accordingly, the best regulations "specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt." Executive Order §1(b).

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

---

[10] *See* Fed. Trade Comm'n, Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 33-34 (Dec. 2010) [*hereinafter* "FTC Staff Report"] ("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.").

[11] Responsive to RFC (1), (3), (5), and (8).

[12] Executive Order No. 13,563, *supra* note 3, at 3821.

[13] Responsive to RFC (1) and (3).

[14] Responsive to RFC (1) and (3).

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 Department to draw upon the resources of industry and civil society colleagues to assess the factual record regarding the benefits to preserving consumer privacy through flexible principles that encourage innovation. These processes should fully appreciate the dignitary and qualitative elements of information autonomy, as well as seek input from industry on the variable costs of different methods of achieving those ends and the marginal costs of incremental regulation so that the most cost-effective means can be selected.[16]

Given this highly dynamic environment, government should continue to promote private sector incentives that create new privacy protections and increase consumer security. The free flow of information, the ability to exercise freedom of expression, and the freedom to associate without governmental scrutiny are cherished principles of our Republic. The control of personal and other information should remain primarily an area into which the government intervenes only when needed.[17]

When regulation is appropriate, such regulation should appreciate the significant benefits that flow to individuals from long-term sharing of information in a trusting business relationship, such as when an investment advisor can suggest better options because he 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. And indeed, maintaining strong customer trust and loyalty is a very tangible incentive for companies. This incentive has driven successful business models for decades.[18]

These benefits should be weighed against a robust identification and assessment of tangible privacy harms such as those identified by the Commission. Ranking such harms and targeting measures to combat the most significant issues are key elements for effective and

[15] Matt Ridley, *There's Nothing So Old as the Recently New*, Wall St. J., Jan. 8, 2011, at C4. Comments in this paragraph are responsive to RFC (1), (2), (3), (5), (7), (8), (9), (17), and (19).
[16] Responsive to RFC (3), (7), (8), and (15).
[17] Responsive to RFC (1), (2), (3), and (5).
[18] Responsive to RFC (3).

efficient enforcement, such as with the Commission's Red Flags initiative which targets vulnerabilities to identity theft. Agencies should make a concerted effort to request quantitative data that makes clear what data practices pose the greatest threat to information security and are of greatest sensitivity and true concern to consumers.[19]

Throughout this process, the Department and the Commission should allow – indeed 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. Indeed, we agree with the agencies' view that competition among companies on the parameters of privacy protection is both possible and desirable. These powerful incentives are important tools for policy makers.[20]

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 Department could also convene industry to encourage and promote the development of innovative interoperable privacy tools. 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 Do Not Track proposals of the Commission.[21] As consumers demand more privacy, the market will provide powerful incentives to companies to provide that privacy, and to do so in a cost effective, innovative manner.[22]

---

[19] Responsive to RFC (1), (3), (7), and (8).
[20] Responsive to RFC (25).
[21] 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.
[22] Responsive to RFC (20), (21), (23), and (25).

C. Global Interoperability

We were particularly pleased to see the significant attention that the Department affords to the substantial need to develop principles that work internationally, and both agencies should proceed together in a manner that is consistent with international norms. Principles should be designed in a flexible way to satisfy basic standards of protection across different jurisdictions.[23]

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.[24]

In particular, a priority should be given to achieving a détente with the E.U. through the Department's effort to achieve a mutual recognition of substantively compatible approaches to privacy protection. The APEC Pathfinder process is encouraging, but it is important to appreciate that the less prescriptive APEC system will not be particularly useful for global companies, if it must be added on top of the more prescriptive E.U. processes. The time has surely come for the U.S. to press the E.U. for mutual recognition, and a finding that the two privacy regimes, albeit procedurally different, provide adequate protection. In this regard, it could be highly useful for the U.S. agencies to develop and provide the E.U. with a comprehensive summary of the overall data protection regime in the United States. This was done in 2000, in connection with the negotiation of the US-EU Safe Harbor,[25] and would only be much more impressive today. There is simply no reasonable argument that the U.S. system of federal laws does not robustly protect privacy; that system comprises, of course, of the Privacy Act, 5 U.S.C. § 552a, the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827, the

[23] Responsive to RFC (1), (3), (8), and (11).
[24] Responsive to RFC (1), (11), and (16).
[25] *See* U.S. Dep't of Commerce, Export.gov, Safe Harbor Enforcement Overview, http://www.export.gov/safeharbor/eg_main_018264.asp; U.S. Dep't of Commerce, Export.gov, Safe Harbor Damages and Authorizations, http://www.export.gov/safeharbor/eg_main_018265.asp; Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n, to John Mogg, Dir. Gen. Internal Mkt. and Fin. Servs, European Comm'n (July 14, 2000), *available at* http://www.export.gov/static/FTCLETTERFINAL_Latest_eg_main_018266.pdf (explaining Federal Trade Commission privacy and data security authority in connection with the development of the Safe Harbor).

Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 201 et seq., the Health Information Technology for Economic and Clinical Health Act ("HITECH"), 42 U.S.C. §17921 & 17931 et seq., the Communications Act, 47 U.S.C. § 151 et seq., the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. 2510 et seq., the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030 et seq., the Fair and Accurate Credit Transactions Act ("FACTA"), 15 U.S.C. 1681 et seq., the Right to Financial Privacy Act ("RFPA"), 12 U.S.C. 3401 et seq., the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6508, the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, Section 5 of the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, state data security laws, state data breach notification laws, state unfair and deceptive acts and practices statutes, common law tort protections for invasions of privacy, and the Fourth Amendment and various state constitutional provisions, among other applicable privacy and data security laws and legal requirements.[26] Certainly the US, along with all international privacy regimes, faces challenges in crafting policy for new and emerging technologies,[27] but more can be done by working together for mutual recognition of substantively comparable standards and for agreement on procedures to avoid barriers to international trade and international flows of data, goods, and services, and eventually to move towards greater harmonization.

A governmental restatement of the law of privacy and data protection that looks beyond Prosser's classic privacy torts could be an important work in this regard. If Commerce and the FTC once again collaborated on the preparation of a summary of the U.S. privacy and data protection system – as the two agencies did in 2000 – we believe that the resulting work product would be enlightening for not only international regulators, but also helpful for U.S. citizens. Such a compilation would also help identify and reconcile any areas of unnecessary or counter-productive conflict, duplication or over-lap.

---

[27] *See, e.g.,* Viviane Reding, *The Digital Forecast Is Cloudy: European Consumers Need Protection Against Misuse of Their Information in the Online "Cloud,"* Wall St. J. Euro. Ed., Jan. 25, 2011, at 13. Writing "[a]s the EU commissioner in charge of data protection," Justice Commissioner Reding stated: "The underlying approach should be a 'cloud-friendly' environment. Having cloud-friendly rules can only help technology companies—many of which in Europe are small businesses—to know exactly what is allowed and what is not. This may mean simpler, harmonized measures, such as the registration forms for notification purposes. We also want to encourage self-regulatory initiatives. Codes of conduct or codes of practice like the 'binding corporate rules' for international data transfers are good solutions. Regulatory certainty is essential: companies must know what the rules are about the flow of data within the EU and at a global level."

D. Enhancing Consumer Privacy Choices

Consumer understanding about 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 and 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 will then encourage and reinforce further market competition fueled by these enhanced and diverse privacy choices.[28]

For privacy choices to be meaningful, 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, Commerce 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. This flexibility should also allow companies to describe the use of data within broad categories, such as "for marketing purposes," without the need 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 ways that were not expected or understood when they were collected.[29]

The brief history of the Internet amply demonstrates that the novel technologies of today will frequently become commonplace and then obsolete in well less than a decade. Policy should thus anticipate and allow for change and recognize that the goal here is a moving target. A frozen form notice could well curtail innovation by linking the future uses of data to current technology. Allowing companies to continue to innovate customized and more consumer

[28] Responsive to RFC (2), (5), (6), (15), (16), (17), and (19).
[29] Responsive to RFC (13), (15) and (17).

friendly notices, in contrast, will preserve their freedoms to offer innovative products that make new uses of data while respecting the privacy promises made in their notices.[30]

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. 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 may be helpful for there to be a common understanding of these practices. Further, to prevent these examples from quickly becoming obsolete in the wake of innovation, the description of "commonly accepted" and "not commonly accepted" practices may need to be periodically reviewed and updated. The Commerce Office of Privacy Protection will be a helpful venue for exploring what is "commonly accepted practices" as it could touch the full diversity of the online economy.[31]

As part of this innovation for consumer privacy choices, and consistent with AT&T's ongoing privacy commitments, AT&T supports more robust notice and consent for novel data practices. The evolution in privacy policies should be particularly focused on sensitivity to and responding to the expectations of the consumer.[32] The progress of the Internet is continually evolving towards a more interactive, personalized online experience. 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 wish to have 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 online services can and should be promoted

[30] Responsive to RFC (3), (7), and (8).
[31] Responsive to RFC (3) and (28).
[32] Responsive to RFC (5) and (13).

to aid online diversification of privacy options.[33]

The need for flexibility in developing these options will become only more pronounced with the evolution of next generation user interface options, such as heads-up displays for car phones and three dimensional displays. Moreover, the intense specialization of many of these technologies frequently results in user interfaces that, although appearing seamless to the user, in fact result from multiple data streams involving multiple business partners. The commercial arrangements between these various entities will need to be adjusted based on the potential secondary value of the information obtained in the course of providing those services, and governmental policy would be ill advised in favoring certain technologies in those commercial negotiations or declaring who owns the data-stream associated with those devices.[34]

E. Transparency and Clarity Are Essential for Privacy Protection

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 is 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.[35]

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 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

[33] Responsive to RFC (3) and (5).
[34] Responsive to RFC (11) and (12).
[35] Responsive to RFC (10, (13), (14), and (15).

with a company. Consumer choices should be simplified, and options should be responsive to consumers expectations. AT&T's Privacy Policy is one model of a substantive, easily accessible, consumer friendly informative notice.[36] The CTIA (The International Association for the Wireless Telecommunications Industry) Location Based Services guidelines[37] are also a good example of how to manage these issues.[38]

In developing these safe harbors, Commerce and the FTC should eschew developing a one-size-fits-all model form. Model forms work only for companies in a particular industry which has similar, routine data practices, not across the vast breadth of commerce within the rapidly evolving Internet ecosystem. And even within a particular industry, many model forms result in less information about privacy practices being made public and fail to account for technological differences between market participants. 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. Market actors should retain the flexibility to tailor their privacy policies to their actual practices, products and consumer agreements, rather than be forced into a rigid and potentially deficient model form notice. 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. Rather, the emphasis should be on flexibility, transparency and clarity – and not on rigid simplicity.[39]

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 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

[36] *See* AT&T Inc., Privacy Policy, *available at* http://www.att.com/Common/about_us/privacy_policy/print_policy.html.
[37] *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.
[38] Responsive to RFC (3), (5), (6), (10), (13), (16), and (17).
[39] Responsive to RFC (3), (6), (16), (17), and (29).

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.[40] 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.

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 flexibility requisite for them.[41]

Civil society and industry have already began developing a sample of this type of consumer shorthand indicator. The Targeted Advertising Cookie Opt-Out ("TACO") technology provides one potential model.[42] The FTC's suggestion of a persistent 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

[40] Responsive to RFC (3), (6), (16), (17), and (29).
[41] Responsive to RFC (5) and (10).
[42] *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 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.").

adopted an icon that will be used throughout the industry to increase transparency.[43] AT&T is helping to build on this momentum by working with Evidon to trial the icon in certain ads.[44]

The need for such transparency is particularly significant for cloud computing, that is, business models involving the provision of data storage, processing, and related functions by or on a third-party network operator. Cloud services present special issues because responsibility for the operational control of the data and related processing is in the hands of an organization other than the user or the user's organization. Moreover, cloud resources, including processing or storage, can transcend national boundaries in a manner that may not be transparent to consumers.[45] 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.

Given the rapid adoption and proliferation of cloud computing, as well as the potential lack of consumer knowledge on the dynamics of cloud computing technology, Commerce and the FTC should encourage cloud providers to strive for transparency in their data practices both with consumers and with their commercial partners. In addition to transparency regarding data collection, storage and use, cloud providers should also clarify whether the cloud provider retains data after the customer no longer purchases the service, or whether the cloud provider uses the data for advertising purposes. Customers should have control over the data stored in the cloud, with the option to access, remove and control use of their data. Further, cloud providers face compelling security responsibilities as they are stewards for data of numerous parties that are subject to a variety of different laws and privacy policies and security standards. Given the

---

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

[44] *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/; TRUSTe Internet Privacy and Security for Businesses, TRUSTe Launches TRUSTe Ads Privacy Platform, Oct. 4, 2010, http://www.truste.com/about_TRUSTe/press-room/news_truste_trustedads.html.

[45] *E.g.,* Kevin J. O'Brien, *Cloud Computing Hits Snag in Europe*, N.Y. Times, Sept. 20, 2010, at B4, *available at* http://www.nytimes.com/2010/09/20/technology/20cloud.html ("[C]loud-based breakthroughs face a formidable obstacle in Europe, however: strict privacy laws that place rigid limits on the movement of information beyond the borders of the 27-country European Union."). *But cf.* Viviane Reding, *The Digital Forecast Is Cloudy, supra* note 29.

intermingling and fluidity of the cloud, cloud providers must engage in even more rigorous data integrity and security protocols, tailored to their specific products and services.[46]

F. Consumer Education Is Crucial

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 and with innovation in multimedia presentation of the content to provide more inquisitive consumers with information, and to force thoughtful and detailed corporate transparency.[47] 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 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 Department and Commission 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.[48]

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

[46] Responsive to RFC (1), (5), (13), (40).
[47] Responsive to RFC (5) and (10).
[48] Responsive to RFC (5).

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. [49]

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.[50]
- 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 effectives messages in virtual world experiences for children ages 8–11.
- 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.

[49] For more information, visit http://www.att.net/smartcontrols.
[50] For more information, visit www.ikeepsafe.org/asca.

- 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.[51]

AT&T's efforts are an example of the many industry initiatives around privacy and consumer outreach, and the Department and Commission can help support these initiatives by encouraging and supplementing these efforts. AT&T appreciates the extent to which the FTC has provided valuable consumer information on its website. And while the FTC's efforts satisfy broad general information needs, other sector specific government agencies and trade associations should be encouraged to focus particular efforts on new industry segments—some of which may not even have a trade association. A Commerce Office of Privacy Protection could also provide valuable educational resources for new industry players, such as app developers, who perhaps do not have the same level of privacy sophistication as more established companies.

G. Consumers Should Have Reasonable Access to Data About Them

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 company's system and infrastructure would be enormously burdensome.[52] Companies in many industries rarely have one singular data system that could 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.

---

[51] *See* Ponemon Institute, Ponemon Survey Names Twenty Most Trusted Companies for Privacy, Feb. 26, 2010, *available at* http://www.ponemon.org/news-2/26. Responsive to RFC (5) and (10).

[52] 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/. Responsive to RFC (5).

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. 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.[53]

H. Privacy Impact Assessments Are Not a Panacea

Government mandated Privacy Impact Assessments ("PIAs") for commercial entities would be a prime example of 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. An undue reliance on PIAs as a one-size-fits-all remedy will indeed undercut innovation in a number of contexts, and will quickly become form over substance. Adherence to an externally mandated process will result in the development of a privacy bureaucracy disconnected from the product development teams – as opposed to connecting privacy expertise more closely with the development teams.[54]

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

[53] Responsive to RFC (41).
[54] Responsive to RFC (6), (7), (8), and (9).

development.[55]

Companies should be responsible for securing the privacy of their customers. It is incumbent on businesses to manage data responsibly and ensure that data is only retained as long as necessary for legitimate business purposes. Companies should be reasonably prepared to establish how they implemented their compliance program in response to a proper investigation or enforcement proceeding, but the government should not dictate processes for such internal oversight.[56]

Agencies should provide guidance, as they do in this report, as to what they consider appropriate principles and suggest useful frameworks, but it would be unduly burdensome to impose a specific requirement for exercising oversight in a particular manner through mandated PIAs. As the President's recent Executive Order emphasized, the government functions best when it demands results – not forms (i.e., "to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt").[57]

Indeed, agencies 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. [58]

[55] Responsive to RFC (7), (8), and (9).
[56] Responsive to RFC (6), (7), (8), (9), and (22).
[57] Responsive to RFC (6), (7), (8), and (9).
[58] Responsive to RFC (2), (5), (6), (7), (8), (9), (31), and (33).

Specific Comments on the Department of Commerce's "Green Paper"

AT&T wishes to offer the following specific comments on items which appeared primarily or exclusively in the Department's exceptionally thoughtful "Green Paper." Overall we applaud Commerce for its practical leadership in offering to convene industry, civil society, and regulators in efforts to develop nuance codes of privacy practices that are adapted to particular industries. AT&T welcomes, and will gladly participate, in these collaborative efforts.

A. Commerce Office of Commercial Privacy Policy

The potential for the Commerce Department to establish a commercial privacy policy office offers an exceptional potential avenue for industry and government to maintain the dialogue established as part of the Commerce initiative regarding this rapidly evolving area. This office could help industries to define and explain the implementation of best-in-class privacy practices, while also providing a forum for coordinated efforts to address new challenges, particularly online.[59]

This office could ameliorate many of the difficulties caused by the fractured and dispersed sources of authority for privacy and security requirements by fostering consistent codes of practices. This current state of play has led to inefficiencies in the distribution of compliance resources for private actors. Commerce could serve an important information centralizing function by creating an online clearinghouse of privacy and security requirements imposed at federal, state and international levels.[60]

This resource would also provide an invaluable educational resource for both industry and consumers, to enhance compliance, promote best practices, and facilitate mutual recognition internationally. Moreover, this centralized function would also serve to rationalize privacy and security obligations and to support work to eliminate regulation that imposes burdens not commensurate with the benefits achieved, and as President Obama has recently directed.[61]

[59] Responsive to RFC (2) and (5).
[60] Responsive to RFC (1).
[61] *See* Exec. Order No. 13,563 (requiring that each regulatory agency must "tailor its regulations to impose the least burden on society . . . [and] select . . . those approaches that maximize net benefits").

Government, industry and civil society should recognize that privacy protections will necessarily evolve in response to a rapidly transforming information ecosystem. These processes should not be constricted by particular deadlines for reaching specific codes of conduct because codes of conduct will need continual innovation and renewal as new technologies are developed. If self regulation proves inadequate over time, the Department could develop an analysis of the particular market failure at play and work with the administration and Congress to develop appropriate solutions to cure that market failure, but they should not presume that the market will fail to provide a solution before this process has been implemented. The Department and the Commission could play a useful role in recognizing specific technologies as providing a safe harbor either through a seal or other approval process.[62]

B. US Data Protection "Adequacy"

A Commerce commercial privacy office would have the added benefit of providing consolidated evidence for the proposition that the United States enjoys a more than "adequate" data protection framework, which is at least equally if not more protective than the European Union's approach as a result of the numerous layers of legal obligation and enforcement.

International companies daily face conflicting rules for international data transfers even within the same international entity, as well as conflicts in other areas central to corporate operations, such as employee privacy. Standards will no doubt vary by conflict. This conflict inhibits the global free flow of the digital economy where information, communications, databases, and transactions are untethered to any particular geography or jurisdiction.

The APEC Pathfinder process is an important example of the useful coordination of varying international norms in a manner that is respectful of individual sovereign interests and historical experiences, while facilitating greater consumer privacy cooperation across member country borders. But more can and should be done. Commerce should conduct further internal and academic or consultant studies on these subjects regarding the best methods for achieving international consensus. This process would also serve as a valuable resource to legislators to

[62] This Seal approval process could be similar to the process the Commission proposes with respect to "green" advertising. See Fed. Trade Comm'n, Proposed Revisions to the Green Guides 50-66, Oct. 6, 2010 (permitting substantiated, understandable third-party seals to show environmentally beneficial aspects of particular products).

the extent that they review or consider changes or modernization of existing laws.

The possibility that the Pathfinder or similar process could lead to mutual adequacy designations is encouraging. Companies with international operations are frequently stuck in the middle of competing E.U. and U.S. requirements. Not only should Commerce take into account the foreign privacy and data security requirements many international companies must adhere to, but Commerce should continue to advocate for the U.S. model that honors both personal privacy as well as the freedom of expression and market innovation. There has already been measured success in the development and implementation of the U.S. Safe Harbor Program, and in the recent APEC agreements. These working relationships should be built upon, and Commerce in particular should continue to build upon the success of the U.S. Safe Harbor Program, the multitudes of sector specific legislative and regulatory privacy protections, and the government supported and incentivized privacy innovations of industry self-regulation to achieve an improved privacy adequacy designation.

C. National Strategies for Trusted Identities in Cyberspace (NSTIC)

AT&T also applauds the White House and Commerce's cybersecurity initiative to promote the creation of secure digital identification for consumer use in online financial transactions. More trusted digital IDs can support online security and privacy, in cooperation with private sector development. In particular, trusted IDs which expose only relevant data elements (such as age), while concealing unnecessary elements (such as gender or name), can help to enhance convenience as well as privacy.[63]

AT&T is eager to see the development of more details on this initiative, and supports a voluntary and competitive digital identity, created by the private sector, rather than controlled by a single government offering. The U.S. government could also support the development of identity management systems and industry privacy control tools through establishing broad goals, rather than narrowly prescribed specifications, for these technologies. In this process, DOC's National Institute of Standards and Technology has the relevant technical expertise to

[63] *See generally* Nat'l Inst. of Standards and Tech., Nat'l Strategy for Trusted Identities in Cyberspace, NSTIC Frequently Asked Questions (FAQs), http://www.nist.gov/nstic/faqs.html (last visited Jan. 27, 2011).

facilitate development of industry standards regarding deployment of privacy-enhancing technologies. Going forward, ID management will be a crucial component of consumer security, privacy, and convenience, and AT&T is hopeful that this Commerce initiative could advance consumer data protection and convenience, leading to even greater functionality and use of Internet-based services.[64]

D. A Comprehensive National Data Breach Notification Framework

As the Green Paper appreciates, current state-driven breach notification laws require disparate obligations and frequently drain the resources that could alternatively be used for privacy enhancing innovation.[65] AT&T supports consideration of a national data breach notification standard to harmonize and rationalize consumer-facing security incident responses.[66]

More data breach notices have now been sent than there are people in the United States.[67] A blizzard of paper does not advance privacy objectives, but it certainly may undercut trust in e-commerce and electronic records. A major contributing factor to this blizzard is the multiple variations in state data breach notification laws, in effect incentivizing massive breach notification for nearly all security incidents.[68] To prevent unduly alarming consumers and diluting the effectiveness of a breach notification where a significant risk of harm does exist, a national data breach notification framework could focus on ensuring consumer notice only when a significant risk of harm is present.[69]

---

[64] Responsive to RFC (20).

[65] IPTF Privacy Green Paper, *supra* note 4, at 57-58 (noting that many commentators agreed that a national data security breach law would "provide clarity for businesses. It would better assist good companies that want to fulfill privacy requirements with a clear path to do so in a consistent manner across State jurisdictions and affording consumers the same treatment").

[66] Responsive to RFC (34).

[67] *See, e.g.,* Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/data-breach (last visited Jan. 23, 2010) (tabulating, as of January 23, 2010, 512,317,699 records breached from 2,306 data breaches made public since 2005 for a country of 300 million people).

[68] For example, many states require breach notification only where electronic data is involved, whereas a minority of states extend notification requirements to paper data as well. *Compare* Cal. Civ. Code 1798.82 ("Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system.") *with* Haw. Rev. Stat. §§ 487N-1 – 487-N-2 ("'Records' means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.").

[69] Responsive to RFC (34).

A breach may present a significant risk of harm to one individual, who should be alerted so he may take precautions to protect himself from the effects of potential identity fraud. Similarly, an insignificant breach of security protocol, that presented no actual loss of company control over data nor loss of data integrity, could nevertheless involve a data file with thousands of individuals' personal information. Thus, numerical thresholds should not be a relevant consideration for a consumer data breach notification trigger, nor in determining the parameters of what may constitute a significant risk of harm. However, given the tremendous reporting potential, and to economize the regulator and industry resources in responding to breaches, notice to regulators should be required only where a data security breach presents a significant risk of harm to a large number of data subjects.[70]

E. Privacy and Security Disclosures in the Cloud

As noted above, cloud computing is rapidly being adopted across the economy and for a vast array of data. But this technology is still in its adolescence, and consumer understanding of the infrastructure processes involved is still in its infancy. Unsettled expectations lead to perennial renegotiation of basic storage terms, and stall consumer understanding. Cloud computing would be enhanced by standardized expectations to secure privacy choices now and to ensure basic security protocols.[71]

[70] Responsive to RFC (34).
[71] Responsive to RFC (5) and (40).

F. Updating ECPA

The Department recommends that the Administration review ECPA and consider the issues related to law enforcement access to modern technologies, such as location-based services and cloud computing. Clarity with respect to ECPA standards is important to domestic and international commerce, as well as the interests of consumers, service providers and law enforcement. In contrast, uncertainty undermines consumer privacy expectations and deters commerce.

The recent holding of the U.S. Court of Appeals for the Sixth Circuit illustrates the ECPA issues that are arising from technological change. *See U.S.* v. *Warshak*, --- F.3d ----, 2010 WL 5071766 (6th Cir. 2010). In that case, the court held that there is a constitutional expectation of privacy in email stored by third parties, equal to the expectation of privacy in telephone calls and letters and other correspondence, and thus that the government must obtain a court warrant to require ISPs to turn over stored e-mail. Under the Stored Communications Act (SCA) provisions of ECPA, however, e-mail over 6 months old is subject to access via subpoena. The court reasoned that, "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." 2010 WL 5071766 at *14. It also noted that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[72] 2010 WL 5071766 at *10.

The goal of any ECPA review should be to ensure clear and consistent standards that preserve the balance struck by Congress. It is reasonable to conclude that law enforcement and private sector actors, such as ISPs and other service providers in the telecommunications and technology sectors, would benefit from specific guidance on how, to what extent, and by what means law enforcement may properly request and obtain access to the data collected incidental to the services that are provided to consumers. And consumers benefit from greater understanding and appreciation of the standards that apply to their information before it is shared with law enforcement. In contrast, heightened uncertainty may stifle innovation ("the inexorable march of

[72] Responsive to RFC (42). We note that the *Warshak* court properly recognized that consumer privacy expectations are necessarily affected by the user agreements and privacy policies entered into between online customers and ISPs. 2010 WL 5071766 at *11-*14.

technological progress") from the private sector, and also create potential difficulties for law enforcement.[73]

Because consent standards under ECPA have already been developed by the courts to allow flexibility for consent either via opt-in or opt-out depending on the circumstances,[74] and because this flexibility is necessary to cover the broad spectrum of possible technologies, products, and services available online and through other communications mediums, any new policy activity in this area should acknowledge existing jurisprudence that has been carefully crafted to reflect expectations of privacy, and preserve this flexibility. ECPA's essential reliance on a *notice and consent* model of consumer choice should not be undermined to the extent that ECPA is reformed to extend to location-based services and data in the cloud. In particular, ISPs and other technology providers should continue to be permitted to tailor subscriber agreements and terms of service to best reflect the technologies they develop and services they offer, and to compete for market segments through innovation and customer service, as well as privacy enhancing benefits, along with a host of other service and product benefits that consumers value.[75]

Finally, ECPA also firmly recognizes the need of service providers to handle data they process in the ordinary course of providing services, and maintaining and protecting their networks and other technologies. Any updating of ECPA to address location-based services and cloud computing should continue to preserve the service provider exceptions that are essential to the telecommunications industry's operation and innovation.[76]

---

[73]Responsive to RFC (42).

[74]Several courts have implied "consent in fact from surrounding circumstances indicating that the appellants knowingly agreed to the surveillance," in part because "Congress intended the consent requirement to be construed broadly." *United States* v. *Amen*, 831 F.2d 373, 378 (2d Cir. 1987) (holding that consent by inmates was implied). Indeed, the "Senate Report [for Title III] specifically says in relation to section 2511(2)(c): 'Consent may be expressed or implied. Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to.'" *Id.* (*citing* S.Rep. No. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182.) Rulings on consent, however, are highly fact-specific questions, and "[i]mplied consent is not constructive consent, but rather, 'consent in fact' which is inferred 'from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance.'" *Hay* v. *Burns Cascade Co., Inc.*, 2009 WL 414117, at * 8-9 (N.D.N.Y. 2009) ("Knowledge of the capability of monitoring alone cannot be considered implied consent. Consent may not be inferred if an employee is not informed: (1) of the manner in which the monitoring is conducted; and (2) that she/he would be subject to such monitoring. It must be left to trial to determine the scope of plaintiff's consent, if any, to the monitoring of her phone calls and the extent to which defendants may have overstepped the scope of such consent." (internal quotations and citations omitted)).

[75] Responsive to RFC (42).

[76] Responsive to RFC (42).

Conclusion

AT&T applauds the work of Commerce in driving this discussion forward, and looks forward to participating in the continued industry collaboration contemplated by the Green Paper. AT&T remains committed to fostering greater consumer understanding of technology and of consumer privacy choices, and will work together with the Department and the Commission, 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

January 28, 2011

* Admitted only in California