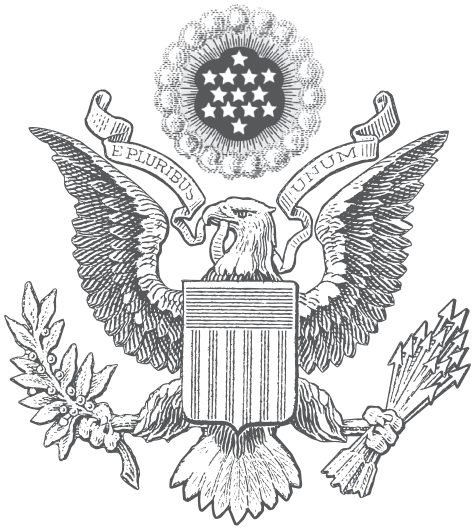


COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK

THE DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE

MESSAGE FROM SECRETARY OF COMMERCE GARY LOCKE

The Internet is an extraordinary platform for innovation, economic growth, and social communication. Using the Internet, entrepreneurs reach global markets, political groups organize, and major companies manage their supply chains and deliver services to their customers. Simply stated, the Internet is becoming the central nervous system of our information economy and society.

Over the last 15 years, personal computers, mobile phones, and other devices have transformed how we access and use information. As powerful, exciting, and innovative as these developments are, they also bring with them new concerns. New devices and applications allow the collection and use of personal information in ways that, at times, can be contrary to many consumers' privacy expectations.

Addressing these issues in a way that protects the tremendous economic and social value of the Internet without stifling innovation requires a fresh look at Internet policy. For this reason, in April 2010, I launched an Internet Policy Task Force (IPTF), which brings together the technical, policy, trade, and legal expertise of the entire Department.

The following report – or green paper – recommends consideration of a new framework for addressing online privacy issues in the United States. It recommends that the U.S. government articulate certain core privacy principles—in order to assure baseline consumer protections—and that, collectively, the government and stakeholders come together to address specific privacy issues as they arise. We believe this framework will both improve the state of affairs domestically and advance interoperability among different privacy regimes around the world so that, globally, Internet services can continue to flourish.

The report represents the collective effort of numerous staff pulled from my office and across the Department. It could not have been developed without unparalleled teamwork; in particular, among staff of the National Telecommunications and Information Administration, the International Trade Administration, and the National Institute for Standards and Technology. I am grateful for the extensive investment of executive time and resources by Department leadership.

In particular, General Counsel Cameron Kerry has been a leader of the IPTF and played an instrumental role in the formulation of this green paper. Assistant Secretary Lawrence E. Strickling, the National Telecommunications and Information Administrator, has helped convene the Department's IPTF and provided keen insights and leadership on

commercial data privacy policy. Finally, I want to thank the respondents to our Privacy and Innovation Notice of Inquiry and the many participants in our outreach meetings.

The report completes just the first phase of this inquiry. For the undertaking to succeed, we will need your ongoing participation and contributions.

Sincerely,

Gary Locke

FOREWORD

The Internet and information technology have become integral to economic and social life in America and throughout the world. They are spurring economic growth, enabling new forms of civic participation, and transforming social and cultural bonds. The growth of digital commerce, and the less quantifiable contributions of the Internet, reflect success not only of innovation and enterprise, but also public policy.

United States Internet policy has avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust in this arena. The United States has developed a model that facilitates transparency, promotes cooperation, and strengthens multi-stakeholder governance that has allowed innovation to flourish while building trust and protecting a broad array of other rights and interests. Addressing commercial data privacy issues is an urgent economic and social matter, but we must proceed in a way that fully recognizes the digital economy's complexity and dynamism. The current framework of fundamental privacy values (with constitutional foundations), flexible and adaptable common law and consumer protection statutes, Federal Trade Commission enforcement, open government, and multi-stakeholder policy development has encouraged innovation and provided effective privacy protections.

Privacy protections are crucial to maintaining the consumer trust that nurtures the Internet's growth. Our laws and policies, backed by strong enforcement, provide effective commercial data privacy protections. The companies that run the digital economy have also shown a willingness to develop and abide by their own best practices. As we entrust more personal information to third parties, however, we can strengthen both parts of this framework. To this end, the green paper recommends reinvigorating the commitment to providing consumers with effective transparency into data practices, and outlines a process for translating transparency into consumer choices through a voluntary, multi-stakeholder process.

Commercial data privacy issues also illustrate the importance of the United States' international engagement on Internet policy issues. Despite having similar substance in practice, U.S. commercial data privacy policy is different in form from many frameworks around the world. The United States is in a strong position to demonstrate that our framework provides strong privacy protections, and that the recommendations in the green paper will further strengthen these protections. Thus, the recommendations in this paper will support U.S. leadership in global commercial data privacy conversations.

The commercial data privacy issues discussed in the Department's green paper, *Commercial Data Privacy and Innovation in the Internet Economy:*

A Dynamic Policy Framework, provide a clear lens through which to assess current policy. Throughout the history of the Internet as a commercial medium, the Department of Commerce has been a key avenue of government engagement. Today, the Department continues this role, primarily through the Internet Policy Task Force, established by Secretary Locke. This Task Force is examining policy approaches that reduce barriers to digital commerce while strengthening protections for commercial data privacy, cybersecurity, intellectual property, and the global free flow of information.

The Department of Commerce is uniquely positioned to provide continued leadership and to work with others inside and outside government to consider a new framework. NTIA, in its role as principal adviser to the President on telecommunications and information policies, has worked closely with other parts of government on privacy and innovation issues. The International Trade Administration (ITA) plays an important role promoting policy frameworks to facilitate the free flow of data across borders, as well as the growth of digital commerce and international trade. For example, ITA administers the U.S.-European Union (EU) Safe Harbor Framework (and a similar framework with Switzerland), which allows U.S. companies to meet the requirements of the 1995 EU *Directive on Data Protection* for transferring data outside of the European Union. In addition, the National Institute of Standards and Technology (NIST), NTIA, ITA, and the Executive Office of the President work closely with U.S. industry in developing international standards covering cybersecurity and data privacy.

This green paper illustrates the power of applying cooperative, multi-stakeholder principles. But in certain circumstances, we recognize more than self-regulation is needed. We hope the recommendations outlined here will play a key role in policy discussions within the Obama Administration.

Indeed, an Administration-wide effort is underway to articulate principles of transparency, promoting cooperation, empowering individuals to make informed and intelligent choices, strengthening multi-stakeholder governance models, and building trust in online environments. The National Science and Technology Council's Subcommittee on Privacy Internet Policy, which I co-chair with Assistant Attorney General for Legal Policy Christopher Schroeder, is leading this effort, in coordination with the Executive Office of the President.

The many comments that we have received from stakeholders are invaluable to our efforts, and I look forward to your continued engagement. Ensuring that all the elements of this framework continue to implement our core principles requires the ongoing engagement by all stakeholders. I also thank Secretary Locke for leading the way toward

Internet policy approaches that balance privacy with the free flow of information, as well as the members of the Internet Policy Task Force from NTIA, ITA, NIST, and others.

The green paper, however, is just a beginning. Developing this initial set of recommendations and discussion points raised new questions, and we invite further public comment to guide our thinking on commercial data privacy.

Cameron Kerry

General Counsel

INTRODUCTION

Strong commercial data privacy protections are critical to ensuring that the Internet fulfills its social and economic potential. Our increasing use of the Internet generates voluminous and detailed flows of personal information from an expanding array of devices. Some uses of personal information are essential to delivering services and applications over the Internet. Others support the digital economy, as is the case with personalized advertising. Some commercial data practices, however, may fail to meet consumers' expectations of privacy; and there is evidence that consumers may lack adequate information about these practices to make informed choices. This misalignment can undermine consumer trust and inhibit the adoption of new services. It can also create legal and practical uncertainty for companies. Strengthening the commercial data privacy framework is thus a widely shared interest.

However, it is important that we examine whether the existing policy framework has resulted in rules that are clear and sufficient to protect personal data in the commercial context.

The government can coordinate this process, not necessarily by acting as a regulator, but rather as a convener of the many stakeholders—industry, civil society, academia—that share our interest in strengthening commercial data privacy protections. The Department of Commerce has successfully convened multi-stakeholder groups to develop and implement other aspects of Internet policy. Domain Name System (DNS) governance provides a prominent example of the Department's ability to implement policy using this model.

Indeed, the Department, along with the White House and the Federal Trade Commission (FTC) took a similar approach to commercial data privacy issues as the commercial Internet was emerging in the early 1990s. What emerged within a few years was a hybrid, public-private system to regulate privacy practices. Major web sites agreed to post privacy policies, the then-nascent online advertising industry developed a code of conduct, and the FTC enforced adherence to those voluntary practices.

This approach has achieved considerable progress, but it requires a renewed commitment on the part of the government. This green paper provides an initial set of recommendations to help further the discussion and consider new ways to create a stronger commercial data privacy framework.

Our recommendations emerge from a year-long review that included extensive consultations with commercial, civil society, governmental and academic stakeholders; written submissions in response to our Notice of Inquiry on privacy and innovation; and discussions at a public symposium that we held on these issues. These recommendations

embody the Department of Commerce's considered but necessarily evolving views on commercial data privacy. To further develop these views, and to contribute to the Obama Administration's development of commercial data privacy policies, we pose a number of questions for further public comment. Public responses to these questions will help us to sharpen and refine the policy ideas that we set out in this report.

To strengthen the foundation of commercial data privacy in the United States, we recommend the consideration of the broad adoption of comprehensive Fair Information Practice Principles (FIPPs). This step may help close gaps in current policy, provide greater transparency, and increase certainty for businesses. The principles that constitute comprehensive statements of FIPPs provide ample flexibility to encourage innovation.

Clarifying how comprehensive FIPPs apply in a particular commercial context may call for multi-stakeholder efforts to produce voluntary, enforceable codes of conduct. The Department of Commerce will help to convene these efforts, in coordination with peer agencies. The resulting voluntary codes of conduct can provide details that are helpful to companies. An open development process that includes industry and consumers can help align these codes and consumer expectations.

With this foundation for commercial data privacy strengthened through comprehensive FIPPs, a scalable approach to providing context-specific guidance, and through continuing examination of all policy approaches, the United States would be in a strong position to reinforce its leadership in global commercial data privacy discussions. This engagement will provide the opportunity to reduce friction in the flow of personal information across national borders, reducing costs for companies and encouraging U.S. exports.

Finally, we should consider whether we can reduce the costs of doing business domestically by ensuring effective, nationally consistent security breach notification rules.

These proposals would maintain the United States' dual emphasis in commercial data privacy policy: promoting innovation while providing flexible privacy protections that adapt to changes in technology and market conditions.

This green paper reflects the hard work of the Department's Internet Policy Task Force, and the Department is deeply grateful to its members, especially the co-chairs of the Task Force, Daniel Weitzner, Associate Administrator at NTIA, and Marc Berejka, Senior Policy Advisor to Secretary Locke. We also acknowledge Manu Bhardwaj, Aaron Burstein, Robin Layton, Caitlin Fennessy, Krysten Jenci, Anita Ramasastry, Brady Kriss, and Ari Moskowitz for their research contributions.

This green paper and the input on which it is based recognize a continued set of challenges presented by rapidly changing technology and economic conditions. The policy options that we discuss seek to chart a way forward. To get there, we will need continued engagement from all stakeholders.

Lawrence E. Strickling

Assistant Secretary of Commerce for Communications and Information

Francisco J. Sánchez

Under Secretary of Commerce for International Trade

Patrick Gallagher

Director, National Institute of Standards and Technology

Table of Contents

Executive Summary

Beginning with the emergence of the mass-market Internet, privacy law around the world has been in transition. During the past 15 years, networked information technologies—personal computers, mobile phones, and other devices—have been transforming the U.S. economy and social life. Uses of personal information have also multiplied, and many believe that privacy laws have struggled to keep up. The lag between developments in intensive uses of personal information and the responses of current systems of privacy regulation around the world leaves consumers with a sense of insecurity about whether using new services will expose them to harm.

Commercial data privacy policy must address a continuum of risks to personal privacy, ranging from minor nuisances and unfair surprises, to disclosure of sensitive information in violation of individual rights, injury or discrimination based on sensitive personal attributes that are improperly disclosed, actions and decisions in response to misleading or inaccurate information, and costly and potentially life-disrupting identity theft. In the aggregate, even the harms at the less severe end of this spectrum have significant adverse effects, because they undermine consumer trust in the Internet environment. Diminished trust, in turn, may cause consumers to hesitate before adopting new services and impede innovative and productive uses of new technologies, such as cloud computing systems.

Though existing U.S. commercial data privacy policy has enabled the digital economy to flourish, current challenges are likely to become more acute as the U.S. economy and society depend more heavily on broadened use of personal information that can be more easily gathered, stored, and analyzed. At the same time, innovators in information technology face uncertainty about whether their innovations will be consistent with consumer privacy expectations.

This green paper reviews the technological, legal, and policy contexts of current commercial data privacy challenges; describes the importance of developing a more dynamic approach to commercial privacy both in the United States and around the world; and discusses policy options (and poses additional questions) to meet today's privacy challenges in ways that enable continued innovation. The Commerce Department's Internet Policy Task Force began work over a year ago by consulting with stakeholders in industry, civil society, academia, and government; followed by publication of the Privacy and Innovation Notice of Inquiry (NOI) on April 23, 2010; consideration of written responses to the Notice;

and participation in the Privacy and Innovation Symposium, held on May 7, 2010.[1]

The Task Force is issuing this green paper to stimulate further public discussion with the domestic and global privacy policy community. While the green paper does not express a commitment to specific policy proposals, it does address areas of policy and possible approaches that were identified and discussed as part of the outreach efforts. More specific proposals may be considered, as appropriate, in a future white paper.

As the Task Force continues to discuss these policy areas, it will coordinate its efforts closely with the Office of Management and Budget (OMB), the Federal Trade Commission (FTC), and other key government actors that play a leadership role in these areas. To the extent that the recommendations in this green paper could have a substantive effect on the privacy framework beyond a purely commercial context, OMB and other agencies have central roles.

NOI respondents were virtually unanimous in calling for strengthening the U.S. commercial data privacy framework.[2] Though the details of the comments varied, a majority of respondents suggested that there is a compelling need to ensure transparency and informed consent, to provide additional guidance to businesses, to establish a baseline commercial data privacy framework to afford protection for consumers,

---

[1] U.S. Dep't of Commerce, Notice of Inquiry, Information Privacy and Innovation in the Internet Economy (Privacy and Innovation NOI), 75 Fed. Reg. 21226, Apr. 23, 2010, *available at* http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf. All comments are available on the NTIA website at http://www.ntia.doc.gov/comments/100402174-0175-01/.

[2] Some commenters, however, explicitly argued that the current commercial data privacy framework is sufficient. *See, e.g.*, Direct Marketing Association (DMA) Comment at 9-11 (stating that the "notice and choice model, including the development of specialized notice mechanisms when appropriate, remains the best way to balance innovation and privacy") (emphasis and capitalization removed from original); Go Daddy Comment at 2 (arguing that "the existing privacy notice and choice framework is sufficient to protect consumer privacy rights, so long as it is consistently applied and vigorous enforced"); TechAmerica Comment at 4-6 (expressing support for notice-and-choice, coupled with data security and "robust enforcement"). Others called attention to particular features of the commercial data privacy framework that, in their views, support flexible protections and innovation and thus ought to be preserved. *See, e.g.*, Comment of Edward McNicholas at 1-5 (explaining the "organic fullness" of U.S. commercial data privacy policy, including constitutional, common law, statutory, regulatory, and industry-based sources of privacy protections); Financial Services Forum Comment at 1-10 (arguing that "[a]n overly prescriptive regulatory regime would likely stifle innovation without truly protecting consumer privacy interests" and embracing the sectoral privacy protections);

and to clarify the U.S. approach to commercial data privacy—all without compromising the current framework's ability to accommodate customer service, innovation, and appropriate uses of new technologies.[3] Commenters also drew our attention to the strengths of the current U.S. privacy regime: fundamental privacy values (with constitutional foundations); flexible, adaptable common law and State-based consumer protection statutes; the Federal Trade Commission's strong enforcement role; open government (promoting accountability and citizens' access to dispersed information); and policy development with the active involvement of many stakeholders and the public as a whole.

To address new challenges and to draw from the best features of current privacy law and policy, the Task Force offers for consideration a **Dynamic Privacy Framework**.[4] The Framework is designed to protect privacy, transparency, and informed choice while also recognizing the importance of improving customer service, recognizing the dynamic nature of both technologies and markets, and encouraging continued innovation over time. This Framework includes policy recommendations under four broad categories:

1. **Enhance Consumer Trust Online Through Recognition of Revitalized Fair Information Practice Principles (FIPPs).** Americans care deeply about their privacy and, in surveys, express disapproval of a variety of common commercial data practices on privacy grounds.[5] At the same time, more and more citizens in the

[3] *See, e.g.*, Comment of the Centre for Information Policy Leadership (CIPL Comment) at 2-3; Comment of the Center for Democracy and Technology (CDT Comment) at 3-4; Google Comment at 4; GS1 US Comment at 2-7; Hewlett-Packard (HP) Comment at 1-2; Intel Comment at 1; Microsoft Comment at 1-2; Network Advertising Initiative (NAI) Comment at 8-9; Comment of Ira Rubinstein; Comment of Robert Sprague at 6-7.

[4] Consistent with our focus in the NOI and throughout this report, the phrase Dynamic Privacy Framework should be understood to refer only to *commercial* data privacy.

[5] For example, nearly two-thirds of American adult social networking users have changed the privacy setting on their profile to limit what they share with others online. Pew Internet and American Life Project Poll (Aug. 2009). The report notes that 71% of social networking users ages 18-29 have changed their settings, while 55% of users ages 50-64 have done so. *See* Mary Madden and Aaron Smith, Pew Internet and American Life Project Poll, Reputation Management and Social Media, at 29 (May 26, 2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf; Chris Hoofnagle, Jennifer King, Su Li and Joseph Turow, How Different are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies? (Apr. 14, 2010), http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf (reporting that "large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions"). *See also* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and*

United States and around the world chose to participate in the Internet marketplace every day. Unfortunately, there is evidence that misunderstandings of commercial data privacy protections are widespread among adult Internet users in the United States.[6] To provide consistent, comprehensible data privacy protection in new and established commercial contexts, we recommend that the United States Government recognize a full set of Fair Information Practice Principles (FIPPs) as a foundation for commercial data privacy.

Revitalized FIPPs should emphasize substantive privacy protection rather than simply creating procedural hurdles. To promote informed consent without imposing undue burdens on commerce and on commercial actors, FIPPs should promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability. Possible approaches include providing strong support for the development of voluntary, enforceable codes of conduct that allow for continued flexibility as technologies and business models evolve; creating safe harbors against FTC enforcement; disfavoring prescriptive rules; and lowering barriers for the global free flow of goods and services online.

Consistent with our focus on commercial data privacy, we make no recommendation with respect to data privacy laws and policies that cover information maintained by the Federal Government, or those

---

Three Activities That Enable It, at 3-4 (Sept. 2009), http://ssrn.com/abstract=1478214 (submitted as an attachment to the Comment of the Samuelson Law, Technology, and Public Policy Clinic) (summarizing survey results indicating that, for example, "[e]ven when they [U.S. adults] are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% 'definitely' would not allow it, and 19% would 'probably' not allow it"). *But see* Datran Comment at 13 n.16 (critiquing Turow et al.'s survey for "failing to consider the trade-off between receiving tailored advertising and receiving free content versus not receiving tailored advertising and having to pay for content")

[6] According to a recent survey, "the savvy that many attribute to younger individuals about the online environment doesn't appear to translate to privacy knowledge," and "the entire population of adult Americans exhibits a high level of online-privacy illiteracy." Hoofnagle et al., *supra* note 5, at 17. This finding is consistent with older data. For instance, a majority of American adults who participated in a 2005 survey wrongly believe that if a website has a privacy policy, then the site is prohibited from selling personal information it collects from customers. *See* Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathan Good and Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade,* 3 I/S: A JOURNAL OF LAW AND POLICY 723, 730-738 (2008) (submitted as part of the Samuelson Law Technology and Public Policy's response to the Privacy and Innovation NOI).

that cover specific industry sectors, such as healthcare, financial services, and education.

2. **Encourage the development of voluntary, enforceable privacy codes of conduct in specific industries through the collaborative efforts of multi-stakeholder groups, the Federal Trade Commission, and a Privacy Policy Office within the Department of Commerce.** The adoption of baseline FIPPs for commercial data privacy, on its own, is not likely to provide sufficient protection for privacy in the dynamic, global Internet economy. Commercial data privacy policy must be able to evolve rapidly to meet a continuing stream of innovations. 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. The United States and other countries can increase their reliance on these institutions, provided that there are adequate back-stops (in the form of regulatory authority or otherwise) to fill in if the multi-stakeholder process fails to develop meaningful, enforceable commercial data privacy practices in a timely way.

   The government also has an important role to play in such a multi-stakeholder approach to developing voluntary codes of conduct as a convener (in additiona to or instead of as a traditional regulator). In this capacity, the government can provide the coordination and encouragement to bring the necessary stakeholders together to examine innovative new uses of personal information and better understand changing consumer expectations—and identify privacy risks—early in the lifecycle of new products or services.[7]

   To this end, we recommend establishing a Privacy Policy Office (PPO) in the Department of Commerce. The PPO would continue

[7] This idea draws on the more general observation that in some cases government agencies can "create structures or incentives for private sector problem-solving" without acting as a full-fledged regulator. *See* Richard B. Stewart, *Administrative Law in the Twenty-First Century*, 78 N.Y.U. LAW REVIEW 437, 450 (2003) (citing "[a]gency-supervised industry self-regulation in fields such as securities, broadcasting, and film" as examples of this approach). *See also* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE LAW JOURNAL 377 (2006) (discussing ways that agencies can use the detailed knowledge of private firms, while remaining publicly accountable, to achieve policy goals in complex policy areas).

the work of the Department's Internet Policy Task Force by acting as both a convener of diverse stakeholders and a center of Administration commercial data privacy policy expertise. The PPO would work with the FTC in leading efforts to develop voluntary but enforceable codes of conduct. Companies would voluntarily adopt the appropriate code developed through this process. This commitment, however, would be enforceable by the Federal Trade Commission. Compliance with such a code would serve as a safe harbor for companies facing certain complaints about their privacy practices. The dynamic process of voluntary code development would provide a greater measure of certainty than many companies are currently able to obtain, but it would also be flexible enough to keep pace with commercial innovations.

Focusing exclusively on commercial data privacy, the PPO would be distinct from the existing roles and authorities of OMB and the senior privacy officers of Federal agencies. Similarly, the work of the PPO would not overlap with the Privacy and Civil Liberties Oversight Board's mission to protect privacy and civil liberties in government collection and use of information in the exercise of its law enforcement, counter-terrorism, and foreign intelligence authorities. The PPO would work closely with OMB and other agencies and would coordinate with the FTC, which will continue to serve independent enforcement, rulemaking, agency policymaking, and education roles.

3. **Encourage Global Interoperability.** At the same time that decreasing regulatory barriers to trade is a high priority, disparate privacy laws have a growing impact on global competition. There is an urgent need to renew our commitment to leadership in the global privacy policy debate. All around the world, including in the European Union, policymakers are rethinking their privacy frameworks. As a leader in the global Internet economy, it is incumbent on the United States to develop an online privacy framework that enhances trust and encourages innovation.

   Congressional leadership, continued FTC enforcement efforts and Administration engagement will all be important to establish that the United States has a strong privacy framework and is committed to strengthening it further. Differences in form and substance between U.S. and other national privacy laws make it increasingly complicated for companies to provide goods and services in global markets. Nations in the European Union and other major U.S. trading partners have adopted omnibus privacy laws, a situation that requires individual companies to demonstrate that their own practices provide privacy protections that foreign governments

consider adequate. This process can be costly, complicated, and uncertain, especially as other countries and regions consider changes to their own privacy laws.

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 flow through increased global interoperability of privacy frameworks. While the privacy laws across the globe have substantive differences, these laws are frequently based on the same fundamental values. We should work with our allies to find practical means of bridging differences, especially those that are often more a matter of form than substance.

Global privacy interoperability should build on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). Agreements with other privacy authorities around the world (coordinated by key actors in the Federal Government) will reduce the significant business global compliance costs.

4. **Ensure Nationally Consistent Security Breach Notification Rules.** Finally, we recommend the consideration of a Federal commercial data security breach notification (SBN) law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities. State-level SBN laws have been successful in directing private-sector resources to protecting personal data and reducing identity theft,[8] but the differences among them present undue costs to American businesses. The FTC and individual States should have authority to enforce this law. A comprehensive national approach to commercial data breach would provide clarity to individuals regarding the protection of their information throughout the United States, streamline industry compliance, and allow businesses to develop a strong, nationwide data management strategy. This recommendation, however, is not meant to suggest preempting of other federal security breach notification laws, including those for specific sectors, such as healthcare.

[8] *See* Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, JOURNAL OF POLICY ANALYSIS AND MANAGEMENT (forthcoming 2011), draft at 26, available at http://ssrn.com/abstract=1268926 (estimating based on FTC panel data that the adoption of security breach notification laws reduces identity theft due to data breaches by 6.1 percent, on average).

A reinvigorated approach to commercial data privacy must be guided by open government-inspired consultation;[9] it can work only with the active engagement of the commercial sector, civil society, academia, and the technical community. The Task Force will work closely with other Federal Government actors to further this engagement and to address new challenges.

Section I of this report reviews the technological changes that have occurred since many current domestic and foreign privacy laws were passed and how these changes have created both an economic and a social imperative for a new approach to commercial data protection. Section II describes the Dynamic Privacy Framework in more detail. To continue the process of engaging all stakeholders, this report presents additional questions for comment throughout the document, which are summarized, along with our recommendations, in Appendix A.

[9] *See* Peter R. Orszag, Memorandum for the Heads of Executive Departments and Agencies on the Open Government Directive, Dec. 8, 2009, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.

I. Facing the Commercial Data Privacy Challenges of the Global Information Age

The value of privacy is deeply embedded in U.S. law and society, reflecting long-standing legal, religious, and cultural traditions.[10] Respondents to the Internet Policy Task Force's Notice of Inquiry on Privacy and Innovation uniformly recognized the value of privacy. Online businesses and advertisers volunteered that they will lose customers if they do not respect customer privacy. Information and communications technology companies stated that privacy protections are necessary to encourage individuals to adopt new devices and services. Commenters from academia and civil society groups noted that protecting privacy is critical to preserving the Internet's value as a tool for free expression, democratic participation, and forming and maintaining social bonds.

Many of these same commenters, however, suggested that changes in technology and business models have rendered parts of our privacy policy framework out of date. To revitalize our privacy framework for the new challenges of the global information age, we must first take note of current privacy policies and arrangements, both in the United States and around the world.

A. Commercial Data Privacy Today

Technology has played a key role in expanding U.S. privacy policy from its roots as a constraint on government conduct to a much broader set of legal norms. The foundation for privacy in the United States is the Fourth Amendment to the U.S. Constitution, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." American judges and legal scholars have linked this protection of physical objects and spaces from government searches to a broader sense of respect for security and dignity that are indispensible both to well-being and to participation in a democratic society.[11]

---

[10] *See generally* Alan Westin, *Privacy and Freedom* (1967). *See also* White House, *Framework for Global for Global Electronic Commerce*, at § 5, http://clinton4.nara.gov/WH/New/Commerce/ (1997) (stating that "Americans treasure privacy, linking it to our concept of personal freedom and well-being").

[11] *See, e.g.*, City of Ontario v. Quon, 130 S.Ct. 2619, 2627 (2010) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government.") (citations omitted); Kyllo v. United States, 533 U.S. 27, 31 ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.") (internal quotation and citation omitted); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("They [the Framers] sought to

Privacy policy in the absence of government intervention also seeks to protect these basic norms of individual well-being and democratic participation, but the institutional foundations are quite different.[12] Indeed, courts have also recognized that individuals have substantive privacy interests against private parties.[13] The common law—particularly tort law—has also played a versatile role in the development of the U.S. commercial data privacy framework. The fountainhead for this development is Samuel Warren and Louis Brandeis's article *The Right to Privacy*, published in 1890.[14] Warren and Brandeis specifically emphasized the right to keep personal information outside of the public domain.[15] Their work laid the foundation for the common law development of privacy, understood by some as a broader "right to be let alone,"[16] including a right to control personal information,[17] during much of the 20th Century.[18]

---

protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men.").

[12] As one privacy scholar has written, "[p]rivacy is the relief from a range of kinds of social friction. It enables people to engage in worthwhile activities in ways that they would otherwise find difficult or impossible." Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 477, 484 (2006). Solove is quick to caution that "privacy is not freedom from all forms of social friction; rather, it is protection from a cluster of related activities that impinge upon people in related ways." *Id.*

[13] *See Mainstream Marketing Services., Inc. v. FTC*, 358 F.3d 1228, 1232-33 (10th Cir. 2004) (holding that advancing consumer privacy is an important government interest and that restricting commercial telemarketing calls protects this interest and does not violate the First Amendment).

[14] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193. *See* Solove, *supra* note 12, at 482 (discussing importance of Warren and Brandeis's article).

[15] *E.g.*, Warren and Brandeis wrote: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." *Id.* at 198.

[16] *Id.* at 193.

[17] We note, however, that the Fair Information Practice Principles framework that we discuss below does not involve a full right to control. Instead, this framework articulates rights and obligations in personal information, such as a right to access and correct information about oneself and an obligation to use personal information only for specified purposes.

[18] Not all courts and scholars have viewed privacy as a broad "right to be let alone." Dean William Prosser examined common law privacy cases and argued that the common law right of privacy is confined to four tort causes of action: intrusion upon seclusion, public disclosure of private facts, putting an individual in a false light, and appropriation of an individual's name or likeness. *See* William L. Prosser, Privacy, 48 CALIFORNIA LAW REVIEW 383, 389 (1960).

As information technologies became more prevalent in the latter part of the 20th Century, however, government action through legislation and regulation became the dominant mode of setting privacy policy in the United States. In particular, the rise of computerized data processing prompted action by the Executive Branch and, ultimately, Congress. In 1973, the Department of Health, Education, and Welfare (HEW) released its report, *Records, Computers, and the Rights of Citizens*, which outlined a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government.[19] This Code of Fair Information Practices, now commonly referred to as fair information practice principles (FIPPs), established the framework on which much privacy policy would be built.

Following the HEW report, Congress enacted the Privacy Act of 1974, which "set forth a series of requirements governing Federal agency personal record-keeping practices."[20] The purpose of the statute and OMB's implementing guidance is "to assure that personal information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon personal privacy."[21]

Congress did not extend such data privacy requirements to the private sector; and today, the United States does not have generally applicable commercial data privacy rules. Instead, the U.S. protects personal data through a sectoral framework that has facilitated innovation and spurred some of the world's most technologically advanced services, while also providing meaningful privacy protections. The United States Government has adopted a flexible approach to privacy protection that uses voluntary enforceable codes of conduct enforced by the Federal Trade Commission together with strong sectoral privacy laws covering certain information categories such as health,[22] finance,[23] education,[24] and information about

---

[19] U.S. Dep't of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (July 1973).

[20] Office of Management and Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948 (Nov. 21, 1975).

[21] *Id.*

[22] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (codified in scattered sections of title 42 U.S.C.) 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

[23] *See* Gramm-Leach-Bliley Act (GLBA), Title V of the Financial Services Modernization Act of 1999 (codified at 15 U.S.C. §§ 6801, 6809, 6821, and 6827); 16 C.F.R. part 313 (implementing privacy rules pursuant to GLB Act).

[24] *See* Family Educational Rights and Privacy Act of 1974 (FERPA) (codified at 20 U.S.C. § 1232g *et seq.*); 34 C.F.R. part 99 (implementing FERPA). *See also* Individuals with Disabilities Education Act of 1970 (IDEA), as revised generally by the Individuals with

children.[25] This sectoral approach allows tailoring of legislative rules to fit specific industries, but it does not apply broadly to all types of data across all sectors. Some have referred to areas that are not covered by these sectoral laws as "gaps" in the framework of privacy policy.[26]

Much of the personal data traversing the Internet falls into these gaps. The United States adopted and maintained this sectoral model as many Americans began connecting to the Internet in the mid-1990s and the model remains in place today. As a result, many of the key actors (e.g., online advertisers—and their various data sources—cloud computing services, location-based services, and social networks) in Internet commerce operate without specific statutory obligations to protect personal data.

Other countries have adopted different models. With the advent of Internet commerce, several multinational bodies developed comprehensive privacy models, drawing nearly all privacy contexts under a single legal framework. In 1995, for example, the European Union (EU) passed its Data Protection Directive, which provides an EU-wide, omnibus framework.[27] The EU's 27 member countries have implemented this framework in their own national laws.[28] In addition, over the past few decades, many countries—including Argentina, Australia, Canada, India, Japan, Mexico, and South Korea—have enacted or updated data privacy laws. These laws are mostly generally applicable to personal data irrespective of the industry in which the data processor participates.

Disabilities Education Improvement Act of 2004, Title I of Pub. L. 108-446 (codified at 20 U.S.C. § 1400 *et seq.*), particularly 20 U.S.C. § 1412(a)(8).

[25] *See* Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277 (codified at 15 U.S.C. § 6501 *et seq.*); *see also* 16 C.F.R. part 312.

[26] *See, e.g.*, CDT Comment at 12 (referring to "gaps" in federal commercial data privacy protections); Google Comment at 4 ("Inconsistency and gaps in the rules [of federal commercial data privacy] create unnecessary costs and burdens to innovation and undermine user trust."); Microsoft Comment at 7 (asserting that sector-specific data privacy regulations "potentially result[] in certain gaps in the law for emerging sectors or business models").

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://ec.europa.eu/justice/policies/privacy/law/index_en.htm.

[28] *See* European Commission, Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data, http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm (last updated Aug. 6, 2010) (listing national laws).

B. The Imperatives for a Dynamic Privacy Framework for Commercial Data

Many have argued that addressing commercial data privacy is both an economic and a social imperative. The information and communications technology marketplaces are vital components of our domestic economy and global competitiveness. Commercial data privacy policy, however, puts more at stake than strictly economic concerns. Privacy protections are crucial to maintaining consumer trust, which is necessary to secure full use of the Internet as a political, educational, cultural, and social medium.

Trust—the belief that someone or something will behave as expected, and not another way[29]—is of central importance to the Internet. For example, the entities that run the large interconnected networks that constitute the Internet trust that the routing information they receive from other, comparable networks is accurate.[30] At the individual level, Internet users trust that entering a URL into their Web browsers will take them to the site they wish to visit. But where hundreds of millions of consumers interacting with millions of Web sites are concerned, it is much more difficult to establish the cues and relationships that underlie trust. Public policy can help establish trust not only by defining obligations but also making available information that helps individuals decide whether to entrust another person or entity with personal information. This green paper explores options for policies that can help promote consumer trust in this environment.

1. The Economic Imperative

Commerce today depends on rapid online communications and transmission of significant amounts of data.[31] A considerable amount of global commerce takes place on the Internet. Global online transactions currently total an estimated $10 trillion annually.[32] In the United States

---

[29] *See* National Academy of Sciences, *Trust in Cyberspace* (ed. Fred B. Schneider) (1999) (discussing trust in the context of IT systems); P. Brann and M. Foddy, *Trust and the Consumption of a Deteriorating Resource*, 31 JOURNAL OF CONFLICT RESOLUTION 615 (1987).

[30] See Ashwin Jacob Mathew and Coye Cheshire, *The New Cartographers: Trust and Social Order Within the Internet Infrastructure*, draft at 7 (describing the importance of trust in the design of Internet routing protocols).

[31] *See, e.g.*, Comment of The Business Forum for Consumer Privacy, Appendix B, 2 (noting how "realities of a data-fueled economy require a re-examination" of how privacy principles can be implemented to effectively serve the consumer).

[32] These data are from the Information Technology and Innovation Foundation (ITIF), The Internet Economy 25 Years After .com (Mar. 15, 2010), http://www.itif.org/publications/internet-economy-25-years-after-com.

alone, according to the U.S. Census, domestic online transactions are currently estimated to total $3.7 trillion annually.[33] In 2009 alone, online retail sales accounted for over $140 billion in retail sales for U.S. companies.[34] In addition, businesses are increasingly taking advantage of the flexibility and cost savings of using distributed, remotely managed "cloud" computing systems.[35]

The Internet is also increasingly important to the personal and working lives of individual Americans. Ninety-six percent of working Americans use the Internet as part of their daily life,[36] while sixty-two percent of working Americans use the Internet as an integral part of their jobs.[37] Finally, the Internet is creating new kinds of jobs. Between 1998 and 2008, the number of domestic IT jobs grew by 26 percent, four times faster than U.S. employment as a whole. According to one estimate, as of 2009, advertising-supported Internet services directly or indirectly employed three million Americans, 1.2 million of whom hold jobs that did not exist two decades ago.[38] By 2018, IT employment is expected to grow by another 22 percent.

Yet the lack of cross-border interoperability in privacy principles and regulations creates barriers to cross-border data flow and significant compliance costs for companies.[39] Improving the global interoperability of data privacy approaches could enable increased exports of U.S. services and strengthen the American economy, in line with the President's National Export Initiative, which sets a number of goals to

---

[33] U.S. Census Bureau, *E-Stats*, May 27, 2010, http://www.census.gov/estats/2008/2008reportfinal.pdf.

[34] U.S. Census Bureau, *E–Stats,* May 28, 2009, http://www.census.gov/econ/estats/2007/2007reportfinal.pdf, at 2.

[35] NIST has identified five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Peter Mell and Tim Gance, The NIST Definition of Cloud Computing, version 15, Oct. 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[36] Pew Internet and American Life Project, Most Working Americans Now Use The Internet or Email at Their Jobs, Sept. 24, 2008, http://www.pewinternet.org/Press-Releases/2008/Most-working-Americans-now-use-the-internet-or-email-at-their-jobs.aspx (reporting results of a survey that found that 62% of employed American adults use the Internet or email at work, and that 96% of this group use the Internet, email, or a cell phone "for some purpose in their lives").

[37] *Id. See also* Federal Communications Commission (FCC), National Broadband Plan at chapter 13, *available at* http://www.broadband.gov/plan/13-economic-opportunity/.

[38] IAB, Economic Value of the Advertising-Supported Internet Ecosystem (June 10, 2009), http://www.iab.net/media/file/Economic-Value-Report.pdf.

[39] *See, e.g.*, TechAmerica Comment at 5-6.

support the overall objective of creating jobs by promoting exports.[40] Thus, commercial data privacy considerations are vital not only to our domestic commerce, but also to international trade.

Strengthening consumer trust is also essential to advancing these economic goals, as many respondents to the Privacy and Innovation NOI recognized.[41] This sense of consumer trust—the expectation that personal information that is collected will be used consistently with clearly stated purposes and protected from misuse is fundamental to commercial activities on the Internet.[42] Conversely, commenters widely recognized that an erosion of trust will inhibit the adoption of new technologies.[43] The Department of Commerce shares the belief that maintaining consumer trust is vital to the success of the digital economy.

---

[40] *See* National Export Initiative, Exec. Order 13534, (Mar. 11, 2010), 75 Fed. Reg. 12433 (Mar. 16, 2010), http://www.whitehouse.gov/the-press-office/executive-order-national-export-initiative.

[41] *See id.*; *see also* TRUSTe Comment at 1 ("Consumers look for signs of trustworthiness of companies they may deal with online, including by looking for trustmarks and third party certification programs."); *infra* note 43.

[42] This recognition has long been a core value of U.S. Internet policy. *See* White House, *Framework for Global Electronic Commerce, supra* note 10; NTIA, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (Oct. 1995), http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

[43] Privacy and Innovation NOI, 75 Fed. Reg. at 21227 ("Since Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained. At the same time, companies need clear policies that enable the continued development of new business models . . ."). For views of respondents on this point, see AT&T Comment at 5-10; CDT Comment at 3 (endorsing the proposition that Internet commerce depends on consumer trust); *id.* at 34 ("Continued growth in these areas [cloud computing and location-based services] . . . depends upon consumer trust."); DMA Comment at 4 ("No company can succeed in today's highly competitive marketplace unless it wins and retains the trust of its customers."); eBay Comment at 2 ("innovation in the Internet economy depends on consumer trust and that maintaining consumer privacy is essential to the continued growth of the Internet"); Go Daddy Comment at 2 ("We understand that the success of our business relies almost entirely on the trust of our users."); Google Comment at 8 (noting the importance of developing U.S. privacy policy that builds consumer trust); GS1 US Comment at 3 ("[W]e realize that commerce cannot thrive in an environment where there is no effective fabric of trust and where consumers do not participate because they lack confidence that they will be fairly treated and that their personal information will be appropriately protected."); HP Comment at 1 ("We firmly believe that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust."); Intel Comment at 1 ("Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth."); Online Trust Alliance (OTA) Comment at 1 ("Ensuring public trust and confidence is the foundation for participation and the growth of the internet."); Telecommunications Industry Association (TIA) Comment at 2 ("Consumers will only adopt new information and communications technologies if they trust that their

Commercial data privacy concerns go far beyond the questions of profiling and targeting for advertising, which largely framed the first stage of Internet privacy policy. Individuals and businesses are rapidly increasing their use of cloud computing systems to store and share documents, photos, videos, and other records, as well as to use software that runs remotely. Increased capacity to store and process large amounts of information enables many new ways of analyzing these data and putting them to economic use. Commenters noted, however, that one of the main advantages of cloud computing—taking advantage of professionally managed, globally accessible storage and processing power—also has the effect of moving information from systems under consumers' direct control to systems controlled by a third party.[44] Several commenters asserted that data receive lower levels of privacy protection as the data move from consumers' personal computers to cloud-based systems.[45] Consumers' and industry's ability to safely use services such as cloud-based email and file storage to their full potential depends on privacy protections that are consistent with other computing models.

2. Commercial Data Privacy: the Social and Cultural Imperative

In addition to playing a central role in advancing Internet commerce, consumer trust is essential to ensuring that the Internet remains the vital platform for democracy and free speech that Americans rightly celebrate. Protecting privacy is critical to maintaining these ideals.[46] Online privacy

---

personal privacy preferences will be respected and that their personal information will remain secure."); Zix Comment at 2.

[44] *See* ACLU of Northern California, Cloud Computing: Storm Warning for Privacy? at 3-7 (submitted as an attachment to ACLU's main comment). Cloud computing does not necessarily involve hosting data with a third party. A company might, for example, move toward distributed, networked storage and application architectures in which all infrastructure remains under the company's possession and control. The involvement of third parties in cloud computing, however, is an emphasis in this report.

[45] ACLU Comment at 4; CDT Comment at 33; CCIA Comment at 6; Digital Due Process Comment at 6; Google Comment at 4 ("The advent of 'cloud computing' – where users store their data with online providers and access them via the Internet – is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers. ECPA, however, affords lesser protections to e-mail communications based on where messages are stored, whether messages have been opened, and how long messages have existed. Such distinctions belie consumer expectations concerning the privacy of e-mail communications."); ITIF Comment at 6 ("As ITIF and others have argued previously, Congress should act to reform laws such as the Electronic Communications Privacy Act (ECPA) to ensure that citizens have a right to privacy for their electronic data whether it is stored at home on a PC or remotely in the cloud."); Mulligan Comment at 3.

[46] *See* CDT Comment at 6 ("Privacy is an essential building block of trust in the digital age."); Mulligan Comment at 5 (noting "entrepreneurial efforts . . . to embed privacy—as

is important to many Americans, as 65 percent of online social network users say they have changed their privacy settings to limit what they share online.[47] Popular discussions of privacy often suggest that younger Internet users have little concern for their own privacy. Recent studies have found that a significant number of young adult users of online social networks change their privacy settings, and one study suggested that young adult users' perceptions of online privacy may be in harmony with older users' perceptions.[48] A study has also suggested that young adult users often misunderstand the protections that they are afforded

---

trust and consumer expectations—into the corporate psyche as well as business operations"); Comment of NetChoice Coalition (NetChoice) at 5 ("[T]he challenge for policymakers is a similar calling for online companies—'align flexibility for innovators along with privacy protection'—in order to earn consumer trust."); W3C Comment at § III.a ("Sustainable online commerce requires sustained trust by users in their online experiences. A key piece of trust online is confidence that privacy expectations are met. Even when the provider acts in good faith, a consumer who does not understand the provider's effort, will not gain more trust, and might very well walk away. User trust requires user understanding. Privacy-related interactions need to be simple and understandable to everyday users. Unfortunately, today's interfaces tend to display large complex statements or technical jargon that nobody understands, if they say anything about privacy at all. Such incomprehensible messages neither improve privacy, nor increase the trust and confidence required for online transactions.").

[47]Mary Madden and Aaron Smith, Pew Internet & American Life Project, *Reputation Management and Social Media: How People Monitor Their Identity and Search for Others Online*, at 3, May 26, 2010, http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf. According to the same survey, "adult internet users have actually become less likely to express concern about the size of their digital footprints," *id.* at 4, though the most of this decrease is attributable to those who have never used a search engine to check up on their digital footprints," *id.* at 4. Moreover, the report notes that "it is important to note that the results from this question are not a measure of internet [sic] users' overall views on 'privacy' or the extent to which they wish to have control over their personal information online." *Id.* at 21.

[48] Mary Madden and Aaron Smith, Pew Internet and American Life Project Poll, Reputation Management and Social Media, at 29 (May 26, 2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf (reporting that 71% of "social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online"). *See also* danah doyd and Eszter Hargittai, *Facebook Privacy Settings: Who cares?*, FIRST MONDAY, vol. 15, No. 8 (2010), (finding that "the majority of young [18- and 19-year-old] adult users of Facebook are engaged with managing their privacy settings on the site at least to some extent"), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589; Chris Hoofnagle, Jennifer King, Su Li and Joseph Turow, *How Different are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* (Apr. 14, 2010), http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf (reporting that "large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions").

under existing privacy laws when engaged in online commercial transactions .[49]

There is also evidence that consumers generally—and incorrectly—believe that a company's posting of a privacy policy sets categorical limits on the company's sharing of personal information. It is reasonable to conclude that this misunderstanding of the law leads consumers to *expect* that commercial and non-commercial organizations will use their personal information with care and protect it from misuse.[50] Consumers' expectations, however, are continually evolving and often vary with context.[51] For example, consumers might expect that their web-based emails will be kept private, but they join online social networks to share at least some information publicly.[52] While some commenters noted that consumers understand that websites are free because of the ads

---

[49] Hoofnagle et al. found that "The entire population of adult Americans exhibits a high level of online-privacy illiteracy; 75 percent answered only two or fewer questions [out of five] correctly, with 30 percent getting none right. But the youngest adults perform the worst on these measures: 88 percent answered only two or fewer correctly, and 42 percent could answer none correctly." Although Hoofnagle does not make this claim directly, the responses to the questions in his study suggest that young adults may overestimate the level of privacy protection that the law provides for online commercial transactions. Hoofnagle et al., *How Different are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?*, *supra* note 48, at 17-18.

[50] Joseph Turow, Chris Hoofnagle, Deirdre Mulligan, Nathaniel Good and Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: A JOURNAL OF LAW AND POLICY 723. 724 (2008) ("When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information.") (submitted under cover of Samuelson Law, Technology and Public Policy Comment).

[51] A wide variety of authorities recognize that information privacy depends on context and that expectations of privacy in the commercial context evolve. On the contextual point, see, e.g., U.S. Dept. of Homeland Security, *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security* § 1.2.1, Oct. 31, 2008 (stating that "[c]ontext matters" when it comes to determining whether an element of personally identifiable information is sensitive); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 242 (2010). For discussions of evolving consumer expectations, see, e.g., Council of Better Business Bureaus (CBBB) Comment at 2 (discussing "the evolving privacy expectations of internet users regarding the passive collection and use of their personal data in certain contexts"); Edward Robert McNicholas Comment at 4 (stating that "evolving notions of privacy" are "an aspect of broader conceptions of human autonomy, such as the rights of free association," among others); Google Comment at 2-3 (arguing that commercial data privacy policy should take into account evolving consumer expectations of privacy).

[52] *See* Facebook Comment at 20-21 (noting that "by definition, social-networking sites require users to share some information with others, and indeed exist to enable such sharing" and that "[e]ngaging a social-networking site is, by definition, a public endeavor").

provided,[53] others noted that consumers do not always understand how and with whom their information might be shared, or the potential negative implications of sharing such information.[54]

C. Challenges in Developing Innovative, Effective Privacy Protection for the Global Information Society

When major public policy priorities, including commercial data privacy, come into contact with the Internet, they face a common series of challenges. Unlike traditional mass media, the Internet is global. Additionally, in contrast to the relatively high barriers to entry in traditional media marketplaces, the Internet offers commercial opportunities to an unusually large number of innovators, and the rate of new service offerings and novel business models is quite high. Taken together, these characteristics give the Internet its strength as a global open platform for innovation and expression. We are committed to preserving the open nature of the Internet but also recognize that it poses a unique set of public policy challenges. The commercial data privacy policy recommendations that we offer in this report constitute an effort to respond to the unique challenges of the Internet environment.

In the years following the commercialization of the Internet (in the early 1990s), the government imperative was to seek unrestrained growth of the Internet as an exciting new medium for free expression and commerce. During this time, early online privacy policy engagements between the Commerce Department, the FTC, and commercial and non-commercial private sector stakeholders began to set out a model for addressing emerging privacy challenges such as those posed by the new and rapidly growing online advertising industry.[55] These efforts led to

---

[53] *See* Advertising Agencies Comment at 1 ("The revenue generated by online advertising supports the creation and entry of new businesses, communication channels (*e.g.*, micro-blogging sites and social networks), and free or low-cost services and products (*e.g.*, email, photo sharing sites, weather, news, and entertainment media.").

[54] CDT Comment at 6-7 ("Study after study has shown that consumers do not understand how their data is collected or used under these new models – and when they find out, it is cause for great concern. Privacy worries continue to inhibit some consumers from engaging in even more established business models such as online shopping.") (internal citations removed).

[55] The FTC helped to prompt the development of this self-regulatory activity following the model originally laid out in the White House paper on Global Electronic Commerce. In addition, the FTC recently issued a preliminary staff report that recommends strengthening commercial data privacy protections through a combination of applying the privacy by design concept, simplifying consumer choice, and increasing the transparency of commercial data practices. *See generally* FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

progress toward voluntary, enforceable codes of conduct to govern commercial privacy. The premise behind this approach was that industry codes would develop faster and provide more flexibility than legislation or regulations. Using the bully pulpit of government (and with the background possibility of regulation), the U.S. Government successfully encouraged industry, in consultation with privacy advocates and regulators, to develop a set of privacy practices that set the model for the early days of the Internet economy.

The Internet grew rapidly through the 2000s and, during that time, supported tremendous economic growth and social innovation. Personal data available on the Internet also grew rapidly in volume and granularity, which in turn expanded the market for personal information. Meanwhile, the "notice-and-choice" model of commercial data privacy policy—posting privacy policies on websites to inform consumers' choices about whether to use the site—remained in place. The FTC, of course, continued to enforce companies' obligations under this framework, but the Administration pulled back from its earlier efforts to promote industry codes that addressed new privacy challenges. Meanwhile, some consumers grew uneasy about the privacy of their online personal data, and businesses faced increasing uncertainty about what U.S. and international privacy policies required of them. This emphasis on notice and choice and FTC enforcement in the midst of a broader retrenchment of government attention to commercial data privacy policy characterized the second phase of commercial data privacy on the Internet.

As we begin this decade with the recognition of the Internet's vital role in daily life, we also recognize that a new approach may well be necessary. Foundational principles, such as enabling individuals to give (or withhold) informed consent before information about them is collected, used, or disclosed in a commercial context, must guide efforts to strengthen commercial data privacy. At the same time, commercial data privacy must be protected in a way that does not stifle innovation or disregard the potential value, to consumers and companies alike, of appropriate data-sharing. Finally, the global dimension of commercial data privacy policy requires close attention, not only to enable the flow of commerce, but also to prevent conflicting policy regimes from serving as trade barriers.

The remainder of this green paper proposes a way to combine these elements—law, multi-stakeholder institutions, technology, and market forces—in a framework that is suitable for protecting commercial data privacy and promoting innovation in a dynamic, global, and increasingly mature Internet economy. While we do not endorse specific legislative

proposals at this time, we intend to provide a guide to help the Administration and all stakeholders move the discussion of commercial data privacy forward.

II. Policy Options for a Dynamic Privacy Framework for Commercial Data

The Task Force is examining how commercial data privacy policy advances two higher-level goals: protecting consumer trust in the Internet economy, and promoting innovation. Based on what we have learned through this inquiry, achieving these goals may necessitate a reevaluation of current policy. From the consumer perspective, the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use, which may leave consumers with doubts (or even misunderstandings) about how companies handle personal data and inhibit their exercise of informed choices. Businesses generally recognize that their sustainability depends on maintaining consumer trust but find that the rules of the road are hard to discern, and sometimes become clear only after FTC enforcement actions.[56] Internationally, differing legal frameworks and new technologies present privacy challenges and complicate commercial data flows across national borders. Because of these basic conditions, we should consider updating the commercial data privacy framework, in order to protect the Internet's important role in our economy and society.

This section sets forth a series of recommendations for a comprehensive national framework for commercial data privacy. Drawing on the Task Force's analysis of the current framework and informed by the insights of NOI commenters, our framework relies on five main recommendations. First, we recommend adoption of a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts not covered by an existing sectoral law. Second, we propose to use commitment to a comprehensive FIPPs baseline as the basis for recognizing expanding interoperability between U.S. and international commercial data privacy frameworks. Third, to maintain the flexibility of the current U.S. commercial data privacy policy framework, an integral part of our Framework is to allow adherence to voluntary industry codes of conduct. Fourth, we propose to create a new Privacy Policy Office within the Department of Commerce to help provide the Administration with greater expertise and a renewed focus on commercial data privacy. Finally, we recommend setting a national standard for notifications following security breaches involving personal information in the commercial context.

[56] Some commenters complained that companies confront a maze of state laws, which makes compliance difficult for companies and does not protect consumers evenly. *See, e.g.*, Procter & Gamble (P&G) Comment at 3; *see also* HP Comment at 2

Recommendations are accompanied by questions for further comment. These questions focus on the specific policy options proposed below. We invite comment on these questions and on any other issues raised by this report. The Department will publish these questions separately as part of a Federal Register Notice, which will provide instructions on how to submit comments.[57]

A. Bolstering Consumer Trust Online Through 21st Century Fair Information Practice Principles

> **Recommendation #1:** The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

Widespread adoption of comprehensive FIPPs is important to achieving the goals we have set for the Dynamic Privacy Framework. If widely adopted, FIPPs would provide flexible protection for privacy interests in commercial data that currently receive little or no statutory privacy protection. That is, baseline FIPPs would respond to consumer concerns about the uses of personal data—and help increase consumer trust—by filling gaps in current data privacy protections. There is reason for concern that, under the current commercial data privacy framework, "heightened consumer concerns about existing privacy threats" will remain unaddressed, even though business expends considerable effort on compliance.[58] In the broad areas of commercial activity that are not regulated by a specific privacy law—areas that rely heavily on notice-and-choice measures—one commenter noted that "the current notice and consent policy framework has not only been ineffective at promoting innovation in this area, but it has not adequately protected consumer data from unexpected or inappropriate collection and use."[59]

Many respondents recommended creating a statutory baseline for U.S. commercial data privacy, while also emphasizing that such a baseline should be part of a larger framework that includes voluntary codes of conduct and government enforcement.[60] The options that commenters

---

[57] U.S. Dept. of Commerce, Notice and Request for Public Comments on Information Privacy and Innovation in the Internet Economy, (to be published in the Federal Register) (requesting comments within 30 days of publication of the Notice).

[58] HP Comment at 2.

[59] eBay Comment at 3.

[60] CDT Comment at 3; Google Comment at 1; HP Comment at 1-2; Microsoft Comment at 2 (calling for "basic privacy guidelines to be laid down" in legislation and supplemented with "industry self-regulation and best practices, technology solutions, and consumer education"); Intel Comment at 1-2; GS1 US Comment at 4 (noting the difficulty of

recommended included a baseline commercial data privacy framework at the national level, support for emerging self-regulatory initiatives, greater FTC enforcement of the existing framework, enhanced FTC rulemaking authority on privacy issues,[61] or a combination of these approaches.

In one respondent's view, comprehensive baseline commercial data privacy rules would help bridge domestic and international frameworks that "are incomplete and sometimes in tension with one another to the detriment of both Internet users and online providers."[62] One commenter stated that a principles-based Federal privacy policy would "give both industry and consumers a framework they can understand and manage."[63] Another noted that "the vast majority of consumer data is not covered by any privacy law" but that "[s]imple flexible baseline privacy legislation" would protect consumers "while enabling legitimate business."[64] Another commenter noted the need for businesses to "collaborate and share information across country boundaries" and stated that "comprehensive and preemptive U.S. Federal commercial data privacy legislation is a key mechanism" for bringing U.S. privacy law into line with this need.[65] As another commenter put its succinct case for a comprehensive commercial data privacy baseline: "consumers want it, we believe companies need it, and the economy will be better for it."[66]

However it is implemented, a FIPPs-based framework for commercial data privacy would increase clarity and promote informed consent for consumers and certainty for consumers, industry, and U.S. trading partners, while fostering compatibility in privacy protection across

---

effective, flexible self-regulation in a fragmented legal environment); P&G Comment at 3 (recommending a "mix of principle-based laws & regulations, together with self-regulation"); Qwest Comment at 2-3; Walmart Comment at 2-3; Miriam Wugmeister, Karin Retzer, and Cynthia Rich, *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEORGETOWN JOURNAL OF INTERNATIONAL LAW 449 (2007) (discussing advantages of Corporate Privacy Rules developed against a backdrop of comprehensive privacy legislation based on Fair Information Practice Principles) (submitted as a response to the Privacy and Innovation NOI);

[61] Note that in its rulemakings in other areas, the FTC consults informally with interested Federal agencies. A similar set of consultations would be appropriate for any rulemakings in the area of commercial data privacy.

[62] Google Comment at 1.

[63] Qwest Comment at 3.

[64] CDT Comment at 4-5.

[65] Intel Comment at 1. *See also* BFCP, A Use and Obligations Approach to Protecting Privacy: A Discussion Document, at 2 (Dec. 9, 2009) (submitted as an attachment to BCFP's comment) (stating that "[p]rinciples of fair information practices serve as the starting point for privacy protection around the world.").

[66] HP Comment at 2.

industry sectors. Comprehensive baseline FIPPs would maintain the flexibility for each industry sector to develop tailored implementation plans that correspond to the privacy risks posed by their services. Also, given the flexibility inherent in the individual principles, a FIPPs baseline would help ensure consumer privacy protection as new technologies emerge. Finally, the FIPPs-based framework that we envision would allow companies to direct resources to the principles that matter most for protecting privacy in a particular technological, business, or social context. Establishment of a FIPPs-based framework could occur through action by industry, civil society, the Executive Branch, or Congress, and enforcement agencies can also help this framework take hold.

Some commenters cautioned that enacting general, FIPPs-based privacy legislation could recreate some of the challenges associated with the current U.S. commercial data privacy framework. As one commenter put it, the current framework tends to leave "privacy to the lawyers and their process-based 'click if you "consent" to the privacy policy' approach," while better privacy practices are likely to develop when businesses "integrate substantive considerations of consumers' privacy expectations into their workflows."[67] Placing form over substance,[68] resulting in a costly, compliance-oriented outlook that distracts organizations from the goal of protecting consumer privacy, is not a desirable outcome.[69]

Experiences with FIPPs in other data privacy contexts suggest that FIPPs are both flexible and comprehensive, making them applicable to a wide range of technologies and data usage contexts. FIPPs are well-established, having been developed in the United States over nearly 40 years and have been incorporated into numerous international frameworks.[70] For example, FIPPs were influential in the development of the OECD's privacy guidelines, the EU Data Protection Directive, and the APEC Privacy Framework.[71] In the United States, the Department of

---

[67] Mulligan Comment at 3-4.

[68] *See* Google Comment at 2. Google makes the distinction, however, that "an enforcement framework that places substance over form" is responsible for "Internet innovation" and "real and effective protections" for privacy. *Id.*

[69] The discussion in this section is limited to the commercial context. The virtues of process and form in the criminal context are quite different.

[70] CDT Comment at 8.

[71] CDT Comment at 8. Some commenters also noted that the Department of Homeland Security adopted a comprehensive set of FIPPs to guide its privacy practices. *See, e.g.,* CDT Comment at 8; Joint Comments of the Center for Democracy and Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid, at 15 (Mar. 9, 2010), submitted as an attachment to the comment of the Samuelson Law, Technology & Public Policy Clinic.

Homeland Security (DHS) adopted a set of FIPPs to govern its use of personally identifiable information.[72] The DHS FIPPs include:

- **Transparency:** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected. *Note that, while the discussion of use limitations that follows below draws on the DHS statement of this principle, it goes significantly beyond DHS's statement.*
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use

[72] *See* DHS guidance at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. The individual principles contained in the other principles-based frameworks cited above overlap significantly with the DHS FIPPs. In each case, the statements contain broad principles that leave companies significant discretion about how to implement them. *See* Intel Comment at 1-2.

> of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[73]

In addition, in its recently released report on commercial data privacy, the FTC calls for adopting many of the same principles, though the report does not structure its recommendations around FIPPs.[74]

To be sure, criticism of notice-and-choice was not uniform. Some commenters voiced explicit support for this framework, stating that it meets the current market and technological environments[75] and that it had "fostered a . . . robust environment for free information flows and rapid innovation."[76] Others stopped short of explicitly embracing the current notice-and-choice framework but urged caution with respect to changing it.[77] These commenters stated that the current framework permits innovation through its flexibility while protecting consumers and punishing bad actors through FTC enforcement. A reasonable conclusion is that notice-and-choice can be helpful, or is most helpful, when the relevant notice is sufficiently clear and simple to consumers.

Still others pointed to voluntary industry efforts as evidence that current commercial data privacy policy provides adequate incentives for industry to adopt voluntary codes of conduct. The prime example is the

---

[73] *See* IAPP Comment at 6 (discussing expertise of corporate privacy officers in conducting audits). To be consistent with DHS's statement of FIPPs, we have copied its language verbatim. We recognize that some adjustment to or additional elaboration of this statement may be warranted. For example, to avoid the impression that adhering to FIPPs would require a company to obtain an independent audit of its information practices, the final principle (accountability and auditing) could be adjusted to establish a flexible evaluation requirement, thus permitting a variety of approaches, including independent review.

[74] *See generally* FTC, Privacy in an Era of Rapid Change (staff report), Dec. 1, 2010.

[75] Comment of National Business Coalition at 3 ("The view of the Coalition is that notice and choice have NOT outlived their value, that both are, and continue to be, essential to giving the consumer an understanding about how data collected from him/her will be used and whether that consumer wishes such collection to continue.") (emphasis in original); Comment of Retail Industry Leaders Association (RILA) at 3 (stating that "Notice and Choice are Not Outdated Models").

[76] Comment of the United States Council for International Business (USCIB) at 3 ("We continue to believe that existing legal and other requirements—including robust enforcement—have been effectively protecting customer privacy interests in the U.S. The U.S. regime has undoubtedly fostered a more robust environment for free information flows and rapid deployment of services than many if not most of its counterparts.").

[77] NAI Comment at 8-10 ("Any adjustments to the existing privacy framework must be carefully calibrated to preserve the growth of the Internet economy as well as the significant advances in privacy protection already provided by self-regulation.").

"enhanced notice"[78] model that a consortium of online advertising trade groups is developing.[79] The effort includes technical specifications that allow online advertisers—particularly those engaged in behavioral advertising—to provide "information on which organization(s) served the ad, where to find their advertising policies, and how to opt-out of such targeting in the future."[80] An icon in or near an online ad would alert users that this information is available.[81] Some commenters argued, however, that such tools may require more explanation and refinement to appeal to consumers. Some of the choices that consumers have to opt out may be too complex to allow consumers fully to understand the available choices.[82] Consumers also may not understand that certain familiar ways of controlling information collection about one's online activities, such as rejecting or deleting Web browser cookies, are not effective against some means of collecting information.[83]

---

[78] The self-regulatory initiative discussed in the main text above was prompted by a call for meaningful, transparent self-regulation by the FTC in 2008-2009. This latest round of FTC support for voluntary, enforceable codes of conduct builds on the model originally presented in President Clinton's Framework for Global Electronic Commerce and then elaborated and implemented by a collaboration of the Commerce Department and the Federal Trade Commission over the last fifteen years. *See* President William J. Clinton and Vice President Albert Gore, Jr., A Framework For Global Electronic Commerce, http://clinton4.nara.gov/WH/New/Commerce/read.html (1997); FTC, *Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behaveadreport.pdf.

[79] *See* American Association of Advertising Agencies et al., Self-Regulatory Principles for Online Behavioral Advertising (July 2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf, which describes enhanced transparency as follows: "To implement enhanced notice, an entity that collects and uses data for online behavioral advertising purposes will provide at least two mechanisms for consumer notice. First, an entity will provide consumer notice on its own Web site. Second, an entity will provide consumer notice at the time that data is collected and used for online behavioral advertising." *Id.* at 5.

[80] NAI Comment at 13. *See also* Comment of the Council of Better Business Bureaus (CBBB Comment) at 7 (describing this "enhanced notice" program); DMA Comment at 8, 10 (same); Future of Privacy Forum Comment at 11-12 (describing use of an icon to direct consumers to more detailed information and opt-out controls); OTA Comment at 2 ("suggest[ing] the importance of moving to an enhanced notice framework").

[81] Future of Privacy Forum Comment at 11-12.

[82] Future of Privacy Comment at 27-28.

[83] Future of Privacy Forum Comment at 22-23; *see also* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It*, at 8-9 (Sept. 2009), http://ssrn.com/abstract=1478214 (submitted as an attachment to the Comment of the Samuelson Law, Technology, and Public Policy Clinic) (discussing specific practices for restoring cookies after deletion and usability issues in opt-out interfaces).

In contrast to the general agreement of commenters in favor of a baseline commercial data privacy framework, there was disagreement on the role for private rights of action in such a framework. Several commenters noted that private lawsuits—particularly in the form of class actions—provide a potent incentive for organizations to keep personal data secure.[84] One commenter noted that "[i]n an absence of private rights of action, . . . there is likely to be significant underenforcement of privacy interests" because of Federal and State authorities' resource constraints.[85] Others stated, however, that the potential for large damage awards from private lawsuits provides a reason to limit private rights of action. In particular, one commenter identified potential class action liability as one of the "largest hurdles" that companies face when they seek insurance and contract with other entities that handle personal data.[86] The Department seeks further comment on the appropriate role for private enforcement under baseline FIPPs.

We acknowledge the broad support commenters express for legislation, and also recognize the downsides that others point out as to the danger of locking-in outdated rules that would fail to protect consumers and stifle innovation. As we consider our position on legislation, we are particularly interested in exploring the following possibilities:

- Baseline commercial data privacy policies that would fill any gaps in existing U.S. law;
- Support for development of voluntary, enforceable codes of conduct that enable continued flexibility in rules that can evolve with new technologies and business models;
- Safe harbors against FTC enforcement for practices defined by baseline data privacy or voluntary, enforceable codes;
- Limited rulemaking authority over certain baseline FIPPs if it is established that market failures require prescriptive regulatory action; and
- A framework likely to lead to lower barriers to the global free flow of goods and services online.

---

[84] *See, e.g.*, McNicholas Comment at 2 ("Few would doubt that the potential for a consumer class action based on a privacy tort is as significant as the potential for a notice of a regulatory inquiry in shaping corporate behavior. U.S."); Chris Jay Hoofnagle, *Internalizing Identity Theft*, at 19-23, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf (submitted as an attachment to the Comment of the Samuelson Law, Technology and Public Policy Clinic) (arguing in favor of a strict liability standard for credit issuers for identity theft, on the ground that issuers are the least cost avoiders); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE LAW JOURNAL 902, (2009) (submitted as an attachment to the Comment of the Samuelson Law, Technology and Public Policy Clinic).

[85] Schwartz, *Preemption and Privacy*, *supra* note 84, at 944.

[86] State Privacy and Security Coalition Comment at 8, 14.

Questions for Further Comment:

1) Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other means, to address how current privacy law is enforced?

2) How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?

3) As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?

4) Should baseline commercial data privacy legislation include a private right of action?

B. Advancing Consumer Privacy Through a Focus on Transparency, Purpose Specification, Use Limitation, and Auditing

Recommendation #2: To meet the unique challenges of information intensive environments, FIPPs regarding **enhancing transparency**, encouraging greater detail in **purpose specifications** and **use limitations**, and fostering the development of verifiable **evaluation** and **accountability** programs should receive high priority.

A baseline commercial data privacy framework, such as the FIPPs-based framework discussed above, should provide greater substantive privacy protection to consumers, as opposed to merely additional procedural hurdles for data users. Here, we highlight how certain principles—transparency, purpose specifications and use limitations, and evaluation and accountability—can directly advance this objective, if they are implemented carefully. This discussion should not be read to suggest that some principles should be left out of a FIPPs-based commercial data privacy framework. Nor do we mean to suggest that companies or enforcement authorities overlook some FIPPs. FIPPs are, to some extent, interdependent. Rather, our view is that emphasizing the FIPPs discussed

below could be highly effective in increasing consumer understanding of commercial data practices while remaining a flexible, low-cost legal framework.

The remainder of this section explores ways to increase attention to substantive protections, as opposed to process regulations that produce more burden than benefit. By sharpening their focus on transparency, purpose specification, use limitations, and evaluation and accountability, organizations and regulators could significantly improve consumer privacy protection—now and as technologies evolve.

1. Enhancing Transparency to Better Inform Choices

Numerous NOI comments and legal scholars have called attention to the lack of transparency under current commercial data privacy policy. There is reason to believe that lengthy and complex disclosure or notice policies may fail to inform; simplicity and clarity are generally preferable and may well be necessary to ensure transparency.[87] Many commenters posed critical questions about the notice-and-choice model, at least when the relevant notice is not transparent.[88] Under the current notice-and-choice model, consumers' privacy rights depend on their ability to understand and act on each individual company's privacy policy. These documents "are generally written in legalese that is unintelligible to the average consumer."[89] As a result of the number and complexity of such notices, this situation is "typically overwhelming to the average consumer."[90] The result, according to these commenters, is a lack of transparency into actual privacy practices and a diminished ability of consumers to make informed choices.

Merely providing general information about data practices is not effective transparency; this information must be accessible, clear, meaningful, salient, and comprehensible to its intended audience.[91] When information is presented in a way that is highly complex or detailed, it may not be

---

[87] *See* Office of Information and Regulatory Affairs, Memorandum for Heads of Executive Agencies and Departments, Disclosure and Simplification as Regulatory Tools, June 18, 2010, *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/disclosure_principles.pdf

[88] *See* Walmart Comment at 4 ("We understand that a growing topic in the public policy debate is whether a traditional privacy approach, including consumer notice and choice, is still valid as technology, business practices, and consumer expectations evolve.").

[89] CDT Comment at 10.

[90] OTA Comment at 2.

[91] See http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/disclosure_principles.pdf.

transparent. According to the comments we received, it seems the level of effective transparency and awareness of current privacy practices is low. Privacy policies are the current framework's primary mechanism for informing consumers of companies' privacy practices. The shortcomings of many privacy policies, as we discussed in Section II.A.1, are widely recognized: they can be dense, lengthy, written in "legalese," and "overwhelming" to the few consumers who actually venture to read them.

The range of services, business models, and organizational structures to which a FIPPs-based framework would apply counsel against attempting to develop comprehensive, prescriptive rules.[92] We are also mindful that a hallmark of the digital economy is the wide variety of rapidly evolving products, services, and content that are often made available free of charge in part through the use of personal data.[93] Commenters touted this benefit to personal data use and cautioned against policies that would alter the existing economic balance.

The current privacy policy framework provides consumers with a limited basis to understand the basis of this economic bargain. To evaluate the privacy risks of any particular online interaction, consumers must understand all of the information practices of all of the entities that gain access to personal data. As consumers use the Internet from more places and through more platforms, it is becoming increasingly difficult to keep track of all relevant practices. Implementing FIPPs in a way that maintains or exacerbates this situation would serve neither the privacy nor the innovation purpose of this inquiry.[94]

Transparency has a key role to play in moving the U.S. privacy policy framework forward, but the privacy risks that commenters identified call for changes in how companies put this principle into practice.[95]

---

[92] *See* Cass R. Sunstein, *Administrative Substance*, 40 DUKE LAW JOURNAL 607, 627 (1991) ("A large source of regulatory failure in the United States is the use of rigid, highly bureaucratized 'command-and-control' regulation. The resulting programs dictate national control strategies for hundreds, thousands, or even millions of companies and individuals in an exceptionally diverse nation."). *See also* Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stanford Law Review (forthcoming 2011), draft at 50-51, *available at* http://ssrn.com/abstract=1568385 (discussing the implications of Sunstein's work for information privacy regulation).

[93] *See, e.g.*, Datran Comment at 15-16 (stating that "online marketers . . . subsidize free content on the Internet"); Facebook Comment at 12 (noting importance of customer demand in driving modifications to products and services).

[94] *See* DMA Comment at 11 ("[I]t is likely that constant appearances of notice boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms").

[95] For a general discussion of the important role that required disclosures play in helping to achieve regulatory goals, see Cass R. Sunstein, *Informational Regulation and Informational Standing:* Adkins *and Beyond*, 147 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 613 (1999) (surveying federal statutes that use "information as a regulatory tool" by requiring either the government or private firms, or both, to publish information about

Enhanced transparency, as described below, would improve on the current notice-and-choice framework and broaden the focus to include a more holistic focus on the purposes of personal data collection and use, and include—for example—publishing the results of evaluations and accountability measures.[96] Other FIPPs can support enhanced transparency's more substantive focus. In particular, the principles of purpose specification and use limitation lead organizations to commit to collecting data for specific purposes, and using it only in ways that are consistent with achieving those purposes. The auditing and accountability principle requires organizations to develop ways to verify to internal and external observers that they are adhering to the limits they set for themselves.

One comment succinctly explained this lack of transparency not merely as a problem for consumer understanding but also as responsible for a loss of consumer trust: "User trust requires user understanding. Privacy-related interactions need to be simple and understandable to everyday users. Unfortunately, today's interfaces [*i.e.*, privacy policies] tend to display large complex statements or technical jargon that nobody understands, if they say anything about privacy at all."[97] Moreover, transparency is critical to the well-informed choice or individual participation that most FIPPs include as a principle. Without access to comprehensible information about what data an organization collects, what it does with that information, and how well it adheres to its stated policy, individual choice is much less meaningful.

Commenters presented several options to remedy the general lack of transparency surrounding current privacy practices. An obvious response would be reduced length and greater simplicity and clarity. One commentator suggested that technology should play a role in bringing greater transparency to privacy practices.[98] Simplifying user interfaces to

---

the environmental impacts of activities, product ingredients, potential side effects of pharmaceuticals, etc.). *See also* Bamberger and Mulligan, *Privacy on the Books*, *supra* note 92, at 50-51 (discussing the implications of Sunstein's work for information privacy regulation).

[96] Online behavioral advertising, for example, helps to provide the revenue to support these services. Facebook Comment at 7; Go Daddy Comment at 2; ITIF Comment at 4; NAI Comment at 1-8; TIA Comment at 6. Enhanced transparency in this context might be aimed at providing consumers with a clearer picture of who buys and sells advertising, and how various markets for ads work in practice.

[97] W3C Comment at § III.

[98] *See* W3C Comment at § III ("User trust requires user understanding. Privacy-related interactions need to be simple and understandable to everyday users. Unfortunately, today's interfaces tend to display large complex statements or technical jargon that nobody understands, if they say anything about privacy at all. . . . At this point, research into privacy user interfaces and experiences lags far behind user needs."); CDT Comment at 25-29.

present the facts about an organization's information practices would go a long way toward improving the current situation.[99] Providing this information is critical to allowing consumers to make informed choices about their online interactions.[100] This commenter cautioned, however, that previous efforts along these lines were not widely adopted and that additional research on the technical and human-computer interaction fronts is necessary.[101]

A group of online advertisers recently launched an "enhanced notice" campaign to present more information about ads in the context in which ads are viewed.[102] Advertisers that participate in this program will display an icon that links to privacy policies and opt-out mechanisms in or near online ads.[103] This voluntary effort is just getting underway and warrants close observation and analysis.

Moving toward the goals of enhanced transparency, as set forth above, however, may require an approach that goes beyond providing users with more direction toward privacy policies and means to manage their profiles. A complementary approach would encourage companies to enhance transparency through privacy impact assessments (PIAs).[104] As discussed by several commenters, PIAs require organizations to identify and evaluate privacy risks arising from the use of personal information in new technologies or information practices.[105] PIAs could also bring about

---

[99] W3C Comment at § III.a.

[100] Several commenters discussed tools for managing choices to opt in or out of specific organizations' information collection programs. *See, e.g.*, DMA Comment at 10; Future of Privacy Forum Comment at 12; Google Comment at 3, 8.

[101] The intersection of data privacy and information system usability is already an active area of research. For example, researchers conducted a "cognitive walkthrough" and laboratory user study to understand how actual user experiences with peer-to-peer software (leading to an incorrect assumption that no files were shared by default) sharply conflicted with the software's default setting (*all* files on the user's hard drive were shared by default). *See* Nathan S. Good and Aaron Krekelberg, Usability and Privacy: A Study of Kazaa P2P File-Sharing, in Proceedings of the SIGCHI Conference on Human Factors in Computing (CHI '03). For an extensive list of research publications on privacy and usability, see the CyLab Usable Privacy and Security Laboratory (CUPS) Home Page, http://cups.cs.cmu.edu/ (last visited Dec. 2, 2010).

[102] *See infra* note 103.

[103] IAB, Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410. *See also supra* Section II.A (discussing enhanced notice).

[104] *See* GS1 US Comment at 5 (discussing development of a framework for PIAs); HP Comment at 5 (describing an internal tool to pose questions concerning privacy to employees working on projects that involve personal information); IAPP Comment at 13.

[105] *See also* Sunstein, *Informational Regulation*, *supra* note 95.

useful transparency. If prepared in sufficient detail and made public, PIAs could create consumer awareness of privacy risks in a new technological context, where norms are not yet clear. PIAs could also help organizations to decide whether it is appropriate to engage in the particular activity at all, and to identify alternative approaches that would help to reduce relevant privacy risks.

Commenters provided helpful examples of how PIAs could bring about enhanced transparency in practice. An industry standards organization pointed to the example of PIAs for radio frequency identification (RFID) tags, readers, and writers;[106] the European Commission recommended that EU Member States and RFID users develop a framework to assess the privacy risks (and safeguards) of using RFID applications.[107] The industry's proposed framework would require RFID users to report the types of data that RFID tags and applications collect and process, and whether this information gives rise to particular privacy risks, such as tracking an individual's movements.[108] In addition, a joint comment of civil liberties groups discussed the value of PIAs in the context of the "smart" electric grid. These groups wrote that a PIA that required electric utilities to relate their proposed system design and associated information flows to FIPPs would not only provide consumers and regulators with a comprehensive picture of how a system uses personal information, but also allow the utility to identify privacy issues at an early stage and "guard against risks and protect consumer privacy at the lowest possible cost."[109]

---

[106] GS1 US Comment at 5-6.

[107] Commission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification, at 6 (May 12, 2009), http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf. This recommendation further states that "[t]he level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application."

[108] Industry Proposal: Privacy and Data Protection Impact Assessment Framework for RFID Applications at § 2.3 (Mar. 31, 2010) (draft), http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf .

[109] Joint Comment of CDT and the Electronic Frontier Foundation 24-25, submitted as an attachment to the Comment of the Samuelson Law, Technology and Public Policy Clinic. Note that NIST recommends that all entities conduct a privacy impact assessment "before making the decision to deploy and/or participate in the Smart Grid" as well as additional assessments "following significant organizational, systems, applications, or legal changes—and particularly, following privacy breaches and information security incidents involving personal information, as an alternative, or in addition, to an independent audit." NIST, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid (NISTIR 7628), at 2 (Aug. 2010), http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

These examples highlight the promise of PIAs for enhancing transparency while promoting innovation. First, because the main purpose of PIAs, as discussed in these comments, is to induce organizations to think through how their information systems or practices comport with FIPPs, PIAs are potentially as flexible as FIPPs themselves. Second, PIAs do not impose any requirements or constraints on technical design or information practices. Finally, as these two comments noted, PIAs can provide high-level guides to organizations' information practices. If PIAs were published, they would provide consumers with a road map to an organization's collection and use of personal information. This picture would complement the atomic, transaction-by-transaction view that consumers obtain through more traditional forms of notice. This information could help inform consumers who are choosing whether to use a new technology. PIAs could also promote more privacy-aware decision-making within organizations.

Questions for Further Comment:

1) What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

2) What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

3) What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

4) What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?

5) Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

6) What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?

7) What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves data from multiple sources being presented through a single user interface?

8) Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?

2. Aligning Consumer Expectations and Information Practices Through Purpose Specification and Use Limitations.

Enhancing transparency, though critically important to improving privacy protections, may not be sufficient. Plain, accessible statements about information collection and use do not necessarily bring these practices into line with consumers' expectations. An entity that clearly states that

it intends to do anything and everything with the data it collects may be transparent, but it may not be providing adequate protection for consumer privacy.

Creating better alignment between consumer expectations and actual information practices is also an important consideration. Focusing on the principles of purpose specification and use limitations can help to align practices with expectations.[110] Purpose specification and use limitations would not involve externally imposed, prescriptive rules that govern how companies can use personal information. Rather, they would require companies to provide clear notice of their practices and would prevent companies from deviating from the purposes and uses to which they commit.

The purpose specification principle requires an organization to state specific reasons or objectives for collecting personal information. For example, an Internet service provider (ISP) might want to collect customer usage records—the addresses of sites visited, grouped by customer name and account number—to prepare bills, detect fraud, and settle billing disputes. In that case, the ISP would state these three purposes in a disclosure to customers. The use limitation principle would then enforce the ISP's commitment to use the personal information it collects only to fulfill these three purposes.[111] Thus, purpose specification and use limitation, working together, provide consumers with positive and negative assurances: consumers know how their information will be used, and they know that it will not be used in other ways.

The combined force of the purpose specification and use limitation principles stands in contrast to the related principles of collection limitation and data minimization. The current privacy policy framework has created an environment in which "creative re-use of existing information" has led to innovations;[112] and if the information is collected under sufficiently broad statements in a privacy policy, the legal risk—in contrast to the privacy risks—from this re-use may be minimal. The same logic applies to data minimization.

---

[110] An alternative would be to carefully regulate certain clearly harmful uses of personal data but then allow greater flexibility and reduce burdens on the collection of personal data in general. The few commenters that discussed such an approach rejected it because, in their view, it would freeze business models and thwart innovation. *See* NAI Comment at 9-10; National Cable and Telecommunications Association (NCTA) Comment at 7.

[111] An illustration of the use limitation principle is the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which limits the uses of consumer reports (as defined in § 1681a(d)) to those specified by statute. *See* 15 U.S.C. § 1681b.

[112] W3C Comment at § II.b.

Returning to our hypothetical ISP, suppose that company executives have grown concerned with security threats against its network equipment and customers' computers. The Chief Executive Officer (CEO) approves a proposal to provide the same Internet usage records described above to in-house researchers, so that they can analyze network traffic and develop security countermeasures. This use of personal information has the clear potential to bring privacy and security benefits to the ISP and its customers. The proposed use, however, would also be contrary to the ISP's specified purposes for collecting the information in the first place.

We want to encourage such re-use, but not at the expense of user privacy.[113] As valuable as that re-use may be, failures in current transparency regimes may come as a surprise to users. Yet at the same time, that re-use may actually add value that the user appreciates. Consumers need to know that when their data are re-used, the re-use will not cause them harm or unwarranted surprise.[114] Transparent notices will allow consumers to access and understand these commitments (or detect their absence). Within the current privacy policy framework, such retroactive privacy policy changes have, at times, attracted enforcement actions by the FTC or State Attorneys General.[115] Providing consumers with notice of a change and an opportunity to consent to new uses of existing data may address the legal issues that companies face when making retroactive privacy policy changes, but these steps do little to clarify whether certain kinds of changes are especially likely to bring social benefits (or harms) and thus should be subject to lesser (or greater) scrutiny.

---

[113] Material retroactive changes to privacy policies have attracted FTC enforcement actions on the ground that the changes are unfair. *See* Complaint, In re Gateway Learning Corp., FTC File No. 042-3047 (July 7, 2004), http://www.ftc.gov/os/caselist/0423047/040707cmp0423047.pdf.

[114] As noted at the beginning of our report, commercial data privacy policy must cover a continuum of harms, ranging from minor nuisances to identity theft and other forms of economic harm. *See also* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, NEW YORK TIMES, Aug. 4, 2009 (quoting the Director of the FTC Bureau of Consumer Protection, David Vladeck, as viewing an individual "dignity" interest in some kinds of personal data).

[115] *See, e.g.*, *id.*; August Horvath, John Villafranco and Stephen Calkins, ABA SECTION OF ANTITRUST LAW, CONSUMER PROTECTION LAW DEVELOPMENTS 78-79 (2009) (reviewing FTC and state enforcement actions).

Questions for Further Discussion:

1) Are purpose specifications a necessary or important method for protecting commercial privacy?

2) Currently, how common are purpose specification clauses in commercial privacy policies?

3) Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?

4) What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

4) How should purpose specifications be implemented and enforced?

5) How can purpose specifications and use limitations be changed to meet changing circumstances?

3. Evaluation and Accountability as Means to Ensure the Effectiveness of Commercial Data Privacy Protections

Finally, the value of transparency, purpose specification, and use limitations ultimately depends on how well organizations follow the practices to which they are bound. Auditing and accountability play a critical role. Audits compare actual data use against specified uses, and accountability is the capacity of an organization, or an enforcement authority, to discipline deviations from specified information uses or privacy policies. A means of verifying—to people within an organization and to those outside—that an organization has observed its stated limits on data use is essential to building and maintaining consumer trust.[116]

Before any audit can take place, of course, the data about how information was used must exist. Moreover, a company (or an auditor) must have a way to compare usage data against rules that are derived from its purpose specifications. In other words, audits depend on some degree of technical infrastructure that can account for how information has been used, and how it should have been used. Only after information use can be accounted for can an organization be held accountable.[117]

---

[116] *See* IBM Comment at 7 (discussing IBM's internal and external audit approach).

[117] *See* Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Gay Sussman, *Information Accountability*, COMMUNICATIONS OF THE ACM, vol. 51, no. 6, at 82 (June 2008).

Questions for Further Comment:

1) Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?

2) Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?

3) Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?

4) How should performance against stated policies and practices be assessed?

5) What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

C. Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTC-Approved Codes of Conduct

1. Promote the Development of Flexible but Enforceable Codes of Conduct

Recommendation #3: Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up FTC enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

Comments that discussed FIPPs pointed to a few difficulties with using them in practice. FIPPs are designed to be comprehensive and general; thus, there may be contexts in which certain principles do not apply, leading to a waste of resources when businesses must demonstrate compliance with each principle. Conversely, in some contexts, FIPPs might not be sufficiently protective. In addition, some commenters pointed to the risk that over-reliance on the procedural aspects of FIPPs

can cause privacy practices to ossify.[118] Finally, adopting a FIPPs-based framework would not necessarily help companies determine when they have adequately implemented the principles, leaving the complaint about the lack of certainty in the current commercial data privacy framework unaddressed. Though one commenter noted that this uncertainty may have the salutary effect of forcing companies to elevate privacy to higher levels of management and to adopt a proactive stance toward privacy,[119] others expressed a desire for clear rules.

To meet these goals of specificity, dynamism, and certainty, we recommend promoting the creation of voluntary, enforceable codes of conduct. Of course, the current commercial data privacy framework accommodates such codes. A recent (2008) example is a self-regulatory code of conduct for online behavioral advertising, including a basic framework of attestation to the code, complaint mechanisms, periodic compliance reviews, and a self-enforcement mechanism.[120] This code continues to be updated to meet the challenges of increasingly sophisticated online advertising technologies, with the goal of providing sensible protections for consumers.[121] Unfortunately, this is the *only* significant example of a voluntary code of conduct developed through a collaborative industry effort.

Addressing the diverse commercial data privacy challenges of the digital economy requires not only more efforts to develop best practices but also incentives for all stakeholders, including industry consumer advocacy groups, Administration officials, and possibly State consumer protection authorities to help develop them. All of these groups need

---

[118] *See* Paul M. Schwartz, *Privacy and Preemption*, 118 YALE LAW JOURNAL 902 (2009).

[119] Mulligan Comment at 4-5.

[120] NAI Comment at 10-11; *see* NAI's Self-Regulatory Code of Conduct (2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf. To join NAI, a company must publicly represent that its "business practices are compliant with each element" of the Code. *Id* at 11. Member companies must have cooperate with NAI compliance reviews. NAI may penalize companies that fail to resolve compliance issues, or refer them to the FTC for enforcement. *Id.* NAI is also actively participating in the formulation of industry-wide self-regulatory principles for online behavioral advertising, across a broad spectrum of associations representing thousands of advertisers, publishers and marketers. *See* Press Release, Interactive Advertising Board, Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising (July 2, 2009), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

[121] NAI Comment at 9; NAI's Self-Regulatory Code of Conduct, *supra* note 124, at 3.

incentives to contribute to the effort, and to do so with a sense of urgency.[122]

There are several plausible options for providing these incentives. One option is for Executive Branch officials, both in the proposed Privacy Policy Office and the Federal Trade Commission, to expend more effort to persuade industry to develop voluntary, enforceable codes of conduct. (State consumer protection authorities could contribute to this effort.) These officials might emphasize the benefits to consumers and businesses of such activities. The history recounted above provides reason to doubt whether this approach, on its own, would provide more incentives than companies currently have to develop voluntary, enforceable codes of conduct. Still, this bully pulpit authority could be combined with either of the options discussed below.

The second option to increase voluntary code development incentives is to increase the level of FTC enforcement of violations under current law. As discussed elsewhere in this report, FTC enforcement is integral to commercial data privacy protection; and so it will remain. We are, however, acutely aware that the FTC is an independent agency that sets its own enforcement and policy priorities under its available resources.

Third, a safe harbor for companies that commit and adhere to an appropriate voluntary code of conduct could provide incentives to develop codes. As a threshold matter, the "carrot" offered by a safe harbor has force only if there is a corresponding "stick." That is, a safe harbor is only as effective as the perceived threat of legislative, regulatory, or other legal risk faced by the company in absence of the ability to resort to safe harbor protection. Given potential safe harbor, companies will have the opportunity to lower compliance and regulatory risks, which should provide ample incentive to participate in developing voluntary codes.[123] A voluntary code of conduct would have to meet certain requirements to make adopters eligible for safe harbor: development through an open, multi-stakeholder process and approval by the FTC for sufficiency. FTC approval might come through a request by a party to assess how the code meets FIPPs' stipulations. Or, FTC approval could be determined in the context of resolving a specific

[122] *See* Statement of Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, National Telecommunications and Information Administration, Hearing on "Do-Not-Track" Legislation: Is Now the Right Time?, Subcommittee on Commerce, Trade and Consumer Protection, Committee on Energy and Commerce United States House of Representatives, Dec. 2, 2010 ("With or without legislation, the centerpiece of Internet privacy protection will have to be to increase the sense of urgency and incentives for the development of voluntary but *enforceable* codes of conduct.") (hereafter "Weitzner Testimony").

[123] Section II.C.2 details a role for an Executive Branch Privacy Policy office in developing voluntary codes.

complaint when the company being investigated asserts a safe harbor defense. In any event, FTC approval of a voluntary enforceable code of conduct as sufficient would establish a presumption that an entity that demonstrates compliance with the code would not be subject to an enforcement action under FIPPs-based commercial data privacy legislation. For companies that do not align themselves with a voluntary code of conduct, the default would be for the FTC to enforce the FIPPs through a transparent and predictable process.

The approach taken to resolve issues between the United States and the European Union (EU) when the EU passed its Data Protection Directive in 1995 illustrates how safe harbors have been successful. Since the legal and regulatory framework in the United States differs from the legal framework in Europe, a solution was negotiated—the U.S.-EU Safe Harbor Framework—which permitted transborder data flows to the United States for commercial purposes, with FTC enforcement as a backstop. The United States and the EU negotiated a compromise based on seven principles broadly derived from elements of the Data Protection Directive that resembled the OECD Guidelines. This compromise enabled data to continue to flow from Europe to the United States. It is widely regarded as a successful option for bridging the divide between the different approaches to privacy protection between the United States and the EU when it comes to cross-border transfers for commercial purposes.

Qualifying for a safe harbor would not mean that a company is immune from enforcement actions, but companies that accept the relevant voluntary, enforceable code would be safeguarded so long as their practices do not deviate from the code's approved provisions. Failing to comply with the voluntary, enforceable code's provisions could lead to an enforcement action by the FTC or a State Attorney General, just as a company's failure to follow the terms of its privacy policy or other information practice commitments may lead to investigation and enforcement under current policy.

2. Create a Privacy Policy Office Convening Business with Civil Society in Domestic Multi-Stakeholder Efforts

The Dynamic Privacy Framework requires an authority to convene businesses and civil society to develop effective, consensus-based voluntary codes of conduct in a wide variety of commercial contexts. Identifying areas in which such codes are needed and bringing together the stakeholders will be critical to the Dynamic Privacy Framework's success. In addition, building international acceptance for the principles of this Dynamic Privacy Framework will require extensive and expert global outreach. A new privacy office within the Department of Commerce, working together with the FTC and other agencies, would be helpful.

Recommendation #4: Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy policy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach for commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO have any enforcement authority.

A PPO would build on strengths of the existing commercial data privacy policy framework while executing several functions that many commenters deemed necessary to improving commercial data privacy protections. Some commenters noted that industry standards and self-imposed privacy policies play a valuable role in protecting privacy, since industry is responsive to pressure from consumers, privacy advocates, and regulators.[124] Similarly, a number of commenters noted that privacy-

[124] *See* Advertising Agencies Comment at 4 ("Self-regulation is responsive to government and consumer concerns, . . ."); Comment of Alan Charles Raul at 6 (noting that "there is an extensive community of privacy advocates that routinely scrutinizes privacy policies and often raises (effective) objections when such policies are perceived to over-reach"); Google Comment at 2 (stating that "there are real and effective protections established under U.S. privacy laws and regulations" but also stating that "the U.S. would benefit from a unified, principles-based legal framework specific to privacy"); Microsoft Comment at 1-2 (suggesting that baseline legislation should "be flexible, technology neutral and . . . build upon the current framework of technology tools, sound business practices, self-regulation and enforcement"); NCTA Comment at 2 (noting that "[c]onsumers are entitled to certain fundamental norms and ground rules that respect their legitimate privacy interests" and pointing to increasing availability of "self-managed preference profiles" for targeted advertising); NAI Comment at 8-9 (noting that NAI released for public comment a draft of its 2008 Code of Conduct); Thomas M. Lenard and Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, 2 POLICY & INTERNET 149, 178 (2010), submitted as an attachment to the Technology Policy Institute Comment (stating that "a major adverse effect of self-regulation (or mandatory privacy legislation) would be to take privacy out of the competitive marketplace. . . . Consumers' preferences for privacy are not homogeneous and there is no reason why firms shouldn't provide varying levels of privacy, just as they provide a variety of product and service characteristics."); P&G Comment at 2 (noting role for "privacy comments from consumers and employees" to assess P&G's Global Privacy Policy).

by-design and technological approaches, such as icons on advertisements or profile management dashboards, could be used to implement industry standards.[125] Two commenters suggested that the Commerce Department develop privacy best practices.[126] Still others suggested that privacy education campaigns for consumers and businesses, run by the Administration, the FTC, or public-private partnerships would better enable consumers to manage their personal information on the Internet.[127] Finally, one commenter noted that the Commerce Department "should continue to provide leadership within the domestic agenda and with our major trading partners internationally. The Department is well positioned to advocate policy that will create meaningful consumer protections and at the same time allow for innovation and economic growth."[128]

The PPO would work with its peer agencies to serve these functions. Most importantly, it would consistently engage key multi-stakeholder institutions in the development of not only technology but also public policy solutions that provide industry with guidance on how to deal with

---

[125] Advertising Agencies Comment at 3 (discussing industry development of technical standards for a "standard, clickable icon" to direct consumers to online behavioral advertising data collection and use notices); AT&T Comment at 10-12 (discussing AT&T's use of privacy-enhancing technologies); CDT Comment at 25-27 (discussing privacy by design and privacy-enhancing technologies as means to help implement FIPPs); Google Comment (Attachment) at 4-6 (discussing privacy enhancements through data portability and a privacy "control panel" for Google users); Microsoft Comment at 7-8; Intel Comment at 4 ("Intel believes that a Privacy by Design principle should encourage the implementation of accountability processes in the development of technologies" but should "avoid mandatory compliance to detailed standards"); TechAmerica Comment at 4 (suggesting that the privacy by design principle "should encourage the implementation of accountability processes in the development of technologies" and "avoid mandatory compliance to detailed standards").

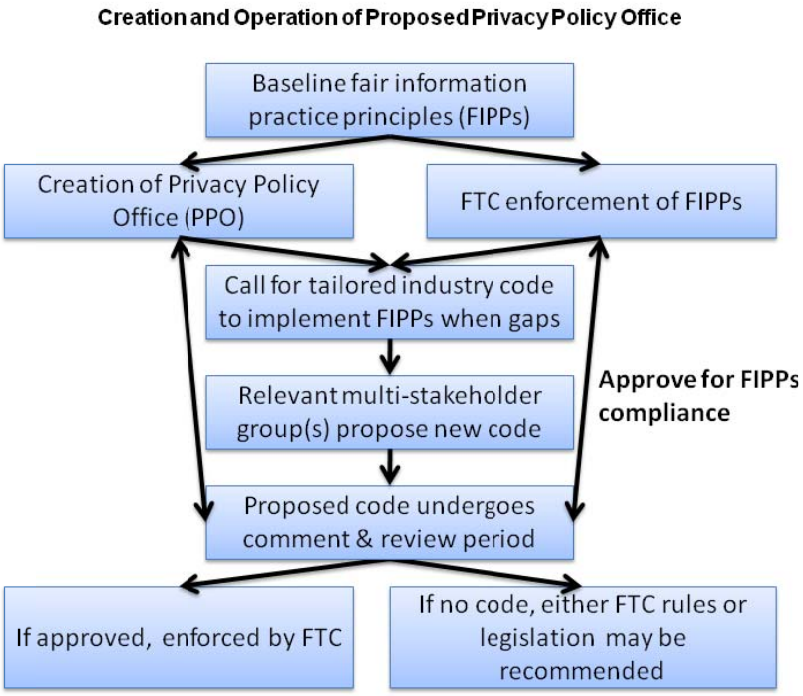
[126] *See* Comment of Alan Charles Raul at 3 (stating that the "Commerce [Department] should consider convening councils of interested parties throughout the U.S. including businesses, state attorney generals, consumer regulators, insurance commissioners, etc., to help elaborate best practices and narrow perceived differences in applicable substantive standards for privacy, data protection and Cybersecurity"); CDT Comment at 5.

[127] *See, e.g.*, Advertising Agencies Comment at 4(stating that "[c]onsumer and business education is critical to protecting consumers online"); *id.* ("[C]onsumer education is vital to demystifying online advertising practices and informing consumers of the availability of choice and tools to control one's online experience."); AT&T Comment at 14 (suggesting cooperation between the government and private sector to "increase education of both consumers and the Internet industry"); Microsoft Comment at 2; CBBB Comment at 3; FTC Comment at 3-4 (discussing FTC's efforts to educate consumers and businesses). In a joint comment, several online advertising groups noted that the IAB had launched an education campaign designed to inform consumers about how they can manage their online experience.

[128] HP Comment at 6.

commercial data privacy issues where consumer expectations are unknown because of new and innovative technologies. A dynamic system in which both private and public stakeholders participate would yield privacy practices that are more responsive to evolving consumer privacy expectations than would a traditional rulemaking system. After all, the rate at which new services develop, and the pace at which consumers form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months. In contrast, a rulemaking can take years and often results in rules addressing services that may be long abandoned. An example of a challenge to which the PPO, multi-stakeholder groups, and the Dynamic Privacy Framework may be conducive is enabling Internet users to express a uniform and persistent choice to opt out of online behavioral advertising—a concept known as "Do Not Track."[129] For these reasons, a PPO-convened group composed of leaders from key multi-stakeholder institutions and U.S. government officials could address new commercial data privacy challenges as they arise and develop guidelines for voluntary, enforceable commercial data privacy codes as needed to ensure that no harm occurs while expectations form around new technologies. The diagram below summarizes how the PPO, multi-stakeholder groups, voluntary codes of conduct, and the FTC would interrelate.

[129] FTC staff recommends the creation of a Do Not track capability. *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 63-69 (preliminary staff report), Dec. 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. *See also* Weitzner Testimony, *supra* note 122, at 10 (stating that "[t]he technical mechanism [of Do Not Track] may take some work to implement, but is presumably manageable. . . . [A]greement on what is meant by the 'do-not-track' sign on, say, the user's browser, is a more complex task, requiring agreement on policy and best practices among a number of players including users, advertisers, marketers, technology companies, and other intermediaries.").



The PPO would work with the FTC, which will continue to make independent policy contributions to the domestic and global privacy dialogue.[130] The PPO and FTC would identify areas where new industry privacy codes are needed to implement the FIPPs, based on rising consumer complaints, industry initiatives, research, or input from multi-stakeholder groups. The Task Force seeks additional input, as described

[130] Since 1995, the FTC has addressed consumer privacy concerns through enforcement, rulemaking, policymaking, and education. In addition to bringing hundreds of enforcement actions in the privacy area, it has hosted workshops and issued reports on issues such as behavioral advertising, peer-to-peer file sharing, and mobile technologies; completed rulemakings in particular areas affecting consumer privacy such as spam; made independent legislative recommendations on privacy issues, such as the need for data breach legislation; and educated millions of consumers and businesses on how to protect privacy. The FTC also has the authority compel companies in particular industries to provide data for FTC research and investigations.

below, on the "carrots and sticks" through which to encourage the development of these industry codes.

Recognizing that there are other significant sources of privacy expertise and authority around the Executive Branch, the PPO's work would complement that of other existing government stakeholders. For example, the role of the PPO would be distinct from the roles of the Office of Management and Budget or the Chief Privacy Officers of Federal agencies relating to Federal government collection and use of information. Similarly, the PPO would not intersect with the Privacy and Civil Liberties Oversight Board's mission to protect privacy and civil liberties in government collection and use of terrorism-related information. The PPO would work closely with OMB and other agencies and would complement other Executive Branch officials by seeking to strengthen the Administration's expertise in commercial data privacy policy. We recommend that the PPO could be housed in the Commerce Department. NTIA serves as the President's principal adviser on telecommunications and information policies,[131] Secretary Locke has created the Internet Policy Task Force to bring together additional capabilities of the Department in Internet and commercial data privacy policy, and the Commerce General Counsel co-chairs the National Science & Technology Council interagency Subcommittee on Commercial Data Privacy and Internet Policy Principles.[132] An Executive Memorandum or Order could delineate the precise boundaries of the PPO's functions and its relation to existing Administration privacy offices.

The PPO should leverage the expertise of private-sector privacy experts, particularly chief privacy officers (CPOs). The rapidly developing privacy profession—experts who "raise privacy awareness" in organizations facing rapidly changing technologies, consumer expectations, and regulations[133]—would provide a source of expertise that can bridge the divide between the PPO and attitudes toward privacy in the broader world.[134] CPOs as a group have diverse backgrounds—technical, legal,

---

[131] 47 U.S.C. § 902 (noting NTIA has "the authority to serve as the President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry."); *see also* FCC, Connecting America: The National Broadband Plan at 55.

[132] See National Science and Technology Council, Charter of the Subcommittee on Privacy and Internet Policy (P^2I), Oct 2010, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-privacy-subcommittee-charter.pdf; U.S. Dept. of Commerce, White House Council Launches Interagency Subcommittee on Privacy & Internet Policy, Oct. 24, 2010, http://www.commerce.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy.

[133] *See* IAPP Comment at 5.

[134] *See* IAPP Comment at 5.

and business, among others[135]—and thus could provide a convenient cross-section of expertise in PPO consultations. In addition, as privacy leaders within their respective organizations, private-sector CPOs could provide the PPO with valuable insight into how privacy policy changes are affecting day-to-day business. Thus, CPOs will serve as a critical resource in multi-stakeholder privacy policy development efforts.

Finally, education is critical to inform consumers of the privacy choices they face, to notify them of privacy tools to control their online experiences, and to clarify online profiling practices. For this reason, the PPO must take a leading role, along with the FTC and industry, in providing consumer privacy education. Private-sector CPOs, whose role we discussed above, would be natural collaborators in the educational effort.[136] As part of this education campaign, the Executive Branch could partner with industry leaders in delivering online public service announcements providing details about online advertising and tools that consumers use to manage their online privacy.

[135] *See id.* at 6.

[136] *See supra* notes 133-35 and accompanying text.

Questions for further comment: The Task Force seeks further comment on how best to encourage the development of voluntary enforceable industry codes in line with the FIPPs when the PPO or FTC determine that more tailored guidance is needed.

1) Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?[137]

2) How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

3) Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?

4) How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

3. Enforcing FIPPs and Commitments to Follow Voluntary Codes of Conduct

Recommendation #5: The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

The Dynamic Privacy Framework would also build on the strong enforcement expertise that the FTC and other agencies have developed. The FTC would remain the Federal government's primary enforcer of consumer privacy protection. Baseline commercial data privacy legislation could give the FTC a specific statutory basis for bringing privacy-related enforcement actions. This enforcement activity would, in turn, clarify the principles and allow them to evolve through case-by-case adjudication. In any case in which FTC enforcement of baseline privacy legislation intersects with cybersecurity or the protection of proprietary information or critical infrastructure in a specific industry sector, coordination with the interested agencies would be necessary.

[137] *See supra* note 61, which notes the FTC's practice of consulting with other federal agencies when developing rules that may affect those agencies' missions and responsibilities.

Solidifying the FTC's privacy enforcement role is consistent with many commenters' recommendations. Indeed, a majority of commenters that recommended a comprehensive baseline requested that the FTC be given the role of enforcement authority over privacy practices, including voluntary industry-wide standards.[138] Conversely, a number of commenters noted that FTC enforcement without other government action, such as baseline principles, legislation, or independent audits, is not a sufficient solution.[139] Others suggested that individual States, and their Attorneys General, should also enforce privacy rules.[140] Some commenters noted that evaluating whether a company's privacy policies meet the principles could be done by a non-governmental independent third-party or by a company's Chief Privacy Officer using internal or external audits.[141] According to some commenters, individuals should have a private right of action in addition to government or industry enforcement when companies violate their privacy policies.[142]

[138] CIPL Comment ; CDT Comment; Mulligan Comment; FTC Comment; Future of Privacy Forum Comment; Google Comment; NetChoice Comment; NAI Comment; Comment of Professor Robert Sprague; Intel Comment.

[139] CDT Comment at 5 (noting that FTC Act § 5 serves as a catch-all privacy law for the "vast majority of consumer data" and that the FTC has limited enforcement resources).

[140] Data Foundry Comment; State Privacy and Security Coalition Comment.

[141] CIPL Comment; Future of Privacy Forum Comment.

[142] *See* CIPL, Data Protection Accountability: The Essential Elements: A Document for Discussion (prepared for the Galway Project) (attachment to the Centre's main comment).

Question for further comment:

1) Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?

2) What should be the scope of FTC rulemaking authority?

3) Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

4) Should non-governmental entities supplement FTC enforcement of voluntary codes?

5) At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.

6) What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?

D. Encourage Global Interoperability

Recommendation #6: The U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' commercial data privacy frameworks. The United States should also continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks.

Disparate approaches to commercial data privacy can create barriers to both trade and commerce, harming both consumers and companies. A significant number of respondents discussed difficulties in complying

with the multiplicity of foreign data protection rules and regulations. They cited six related challenges above all: 1) restrictions on transferring data between jurisdictions; 2) the lack of a recognized U.S. government privacy authority to represent the interests of U.S. industry in international privacy discussions; 3) difficulty providing a clear articulation of the U.S. approach to privacy policy; 4) obstacles to implementing global information management systems given conflicting foreign data privacy requirements;[143] 5) jurisdictional ambiguity and security concerns over data held in the cloud; and 6) significant costs to track and comply with data protection laws in each country. Respondents also noted gaps in protection for consumers whose data are transferred across borders, since it is not always clear who has jurisdiction over data and what protections exist for foreign consumers.

To overcome these obstacles, respondents recommended a number of options with the majority advocating for greater harmonization and international interoperability. The options discussed included:

- The creation of a global privacy standard;[144]
- Adoption of a treaty or convention to govern cross-border data flows;[145]
- An enhanced U.S. privacy framework that can be more easily supported abroad;[146]
- Increased Department of Commerce international advocacy for U.S. interests in bilateral and multilateral privacy discussions;[147]
- More focused and coordinated U.S. government representation of the U.S. position on privacy internationally;[148]
- The creation of accountability certifications, such as Binding Corporate Rules, to enable cross-border data flows;[149]
- Application for adequacy status from the European Union,[150] implementation of the APEC Privacy Framework;[151] and

[143] *See infra* Section II.B.

[144] P&G Comment.

[145] Salesforce.com Comment.

[146] CDT Comment; NetChoice Comment (citing remarks of Professor Fred H. Cate at the May 7, 2010, Department of Commerce Symposium on Privacy Policy and Innovation in the Internet Economy).

[147] Comment of Alan Charles Raul; CIPL Comment ; IBM Comment; Microsoft Comment; NetChoice Comment; Visa Comment.

[148] TechAmerica Comment.

[149] HP Comment; NetChoice Comment.

[150]Comment of Alan Charles Raul; Comment of Professor Paul M. Schwartz. "Adequacy" is a standard that national laws must meet in order to satisfy the Data Protection Directive. The current U.S.-EU Safe Harbor Framework requires companies to show that their data protection practices are "adequate" to provide protection that is consistent

- The development of a U.S. framework that furthers harmonization of privacy laws, including with the EU Directive.[152]

A number of the recommendations concerning international harmonization and standards, while potentially achievable, would entail longer-term negotiations and multilateral discussions over a significant period of time. Others, such as more focused government representation of the U.S. position on commercial data privacy, might be achieved more quickly. We should pursue long-term and short-term goals simultaneously, in order to ensure comprehensive international engagement.

Commenters widely commended the APEC Privacy Framework as an option for achieving greater interoperability.[153] Briefly, the APEC Privacy Framework, endorsed in 2004, was developed cooperatively by APEC member economies. Modeled on the OECD Guidelines, the APEC Privacy Framework includes nine high-level principles concerning the collection, use, and handling of personally identifiable information. Implementation of these principles would create effective privacy protections, and thus improve consumer confidence online, while also avoiding the creation of unnecessary barriers to the flow of information. Because the APEC Privacy Framework was developed, in part, specifically to facilitate regional data transfers, it also includes guidance for the international implementation of the nine privacy principles, including through a mechanism of "cross-border privacy rules" for businesses.

In 2007, APEC initiated a formal Data Privacy Pathfinder to develop such a cross-border privacy rules system for the APEC region, and stakeholders have worked on the various aspects of that system since then. Essentially, the system would be a self-regulatory framework or seal program for businesses to transfer consumer data across the APEC region pursuant to more harmonized and consistent privacy protections

---

with such a law. *See* Letter from John F. Mogg to Robert LaRussa(July 28, 2000), http://www.export.gov/static/sh_en_EUletter27JulyHeader_Latest_eg_main_018403.pdf.

[151]CIPL Comment; Intel Comment.; HP Comment; IBM Comment; NetChoice Comment; P&G Comment; Salesforce.com Comment; TechAmerica Comment.

[152] Marketing Research Association Comment at 6-7 (stating that the United States "should establish a privacy law framework that harmonizes international laws, particularly with respect to the EU Data Directive" but "should not endorse a federal privacy law framework based on the European Union").

[153] For example, the Telecommunications Industry Association comment described the APEC Privacy Framework and the Cross Border Privacy Rules as "reflect[ing] an approach to privacy regulation that protects privacy while preserving the flexibility necessary for innovation." TIA Comment at 3. Procter & Gamble noted that, "the development of the APEC Privacy and Security Framework and the subsequent Pathfinder Pilot—both of which included P&G as a participant—is an excellent example of the positive leadership role the Department can play in privacy policy." P&G Comment at 3.

that track the APEC Privacy Principles. Businesses that want to participate would apply to an APEC-recognized "accountability agent" that would review the companies' privacy policies and practices in light of the APEC cross-border privacy rules program requirements, and could certify the company for participation.

The current goal is to secure the system's endorsement during the 2011 APEC year, which is being hosted by the United States. One commenter noted that the Department of Commerce would be in an ideal position to press for completion of these projects at that time.[154] Ultimately, this project will encourage companies to commit to a significant level of protection of the data that they process about their customers, and will encourage companies to act responsibly when dealing with personal data. There is also the promise of economic benefit to consumers because of cost-savings that result from increased efficiencies in data management and compliance operations for both data controllers and data processors. The APEC cross-border privacy rules system also advances the accountability concept in a meaningful way, because it incorporates specified accountability requirements for participating businesses and provides for effective domestic and cross-border government backstop enforcement.

Thus, identifying and working toward greater interoperability among global data protection frameworks deserves significant attention. It may be possible to reduce barriers to cross-border data flows and increase consumer privacy protection through a combination of increased cooperation among privacy enforcement authorities and mutual recognition of other countries' privacy frameworks. Though two countries may not have identical laws, regulators have shown that they can develop mechanisms for cross-border enforcement operations. In addition, mutual recognition of substantively similar commercial data privacy laws around the world can build increased practical protection for consumers and reduce barriers and compliance costs for businesses.

In order to explore these ideas further, the Task Force recommends the U.S. continue to support the APEC Data Privacy Pathfinder project as a model for the kind of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks. Countries have the opportunity to take this work to the next level by translating these principles into actual binding trade commitments that would steer the world toward global privacy protection interoperability. In particular, the principles could be the basis on which countries enter into mutual recognition of each others' commercial data privacy systems and build cross-border regulatory

[154] IBM Comment at 6.

cooperation. Such regulatory cooperation would enable a country whose citizens' privacy interests are harmed by a company operating in another country to seek redress on behalf of its citizens. The U.S. government should encourage countries to take advantage of this opportunity to build on the significant progress already made to pave the way for a new global framework for privacy protection that will decrease the cost of doing business globally, provide consumers with consistent levels of protection worldwide, and contribute to global economic growth.

E. National Requirements for Security Breach Notification

> **Recommendation #7:** Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.

Adopting comprehensive baseline commercial data privacy principles would leave other closely related issues unaddressed. State privacy laws still present challenges to businesses that must comply with several dozen variations on the same theme. As one commenter complained, the State law "maze" is costly and confusing for businesses and consumers alike. In particular, numerous respondents discussed State security breach notification (SBN) laws.[155]

Nearly all of the NOI comments that addressed Federal laws or regulations strongly favored preemption. Agreement on this issue crystallized around SBN laws. A business group was unequivocal in its recommendation, framed by the fact that nearly every State has its own SBN law: "Our members are happy to comply with whatever policies are enacted into law, but they simply do not wish to have to comply, nor should they have to, with an ever-shifting 'patchwork' of different State laws that can actually change, as between the various States, several times in any given year."[156]

---

[155] Our recommendation is limited to state SBN laws. We make no recommendation on federal laws pertaining to security breach notification in specific sectors, such as healthcare. See also *infra* Section II.F, which further discusses the relationship between the Dynamic Privacy Framework and federal sector-specific data privacy laws.

[156] National Business Coalition Comment at 4.

Several other commenters discussed the need for a Federal SBN law that would consolidate and draw upon the most successful aspects of the various existing State laws, such as notice requirements and a safe harbor for implementing reasonable security measures.[157] Indeed, the many State laws, and years of experience with them, provide valuable data for constructing a national SBN law. For example, one commenter noted that the United States is a world leader on data security and data breach notification rules, and that much of the development of current data breach notification rules has occurred at the State level. An IT company noted that data breach notification laws "have created solid foundations for improved organizational behavior and consumer protections. But as the number of State laws and statutes grow, so does the complexity in business compliance processes and costs. [The company] believe[s] that many of the best practices that exist in State laws should form the basis of Federal legislation to ensure a predictable and uniform standard across the U.S."[158] Another commenter expressed its belief that a nationally consistent data breach notification 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."

Question for Further Comment:

1) What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?

F. Relationship Between a FIPPs-Based Commercial Data Privacy Framework and Existing Sector-Specific Privacy Regulation

Recommendation #8: A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections.

A baseline commercial data privacy framework should leave in place existing sectoral laws. Arguments to the contrary do not go to the core

[157] *See, e.g.*, HP Comment at 2; OTA Comment at 5; State Privacy and Security Coalition Comment at 10-11.

[158] HP Comment at 2.

objective of providing comprehensive commercial data privacy protection. The sectoral approach may not be adequate,[159] and a comprehensive baseline would have certain advantages. On the other hand, there are numerous merits in the United States' sectoral approach to commercial data privacy. One commenter, for instance, stated that "[t]he major sectoral programs, HIPAA and GLBA, have provided consumer protections for privacy and data protection, but they clearly do not extend across all industries. … [Federal privacy law] needs to take into account, co-exist with, and complement those sectoral laws."[160] Some commenters acknowledged the specialized expertise of regulatory agencies for specific sectors. As one such commenter stated, "any new privacy framework or protection should preserve the values that are derived from regulating privacy with an understanding of the industry to which that framework or protection will apply."[161] Other commenters also noted that the sectoral approach results in laws that are necessarily more narrowly tailored to particular industries and have terms that, by their nature, are more specific.[162]

Commenters noted, however, that the sectoral approach is emblematic of the lack of a perceptible, cohesive commercial data privacy policy, which creates complexity and costs for businesses and confuses consumers. According to one commenter, "[d]espite successes [of the sectoral approach to privacy protection], further consistency and comprehensiveness in US privacy regulation will help strengthen user privacy and promote continued innovation."[163] A similar view, expressed

---

[159] *See, e.g.*, Google Comment at 4; Microsoft Comment at 7..

[160] HP Comment at 4. Other sectoral privacy laws that are relevant to baseline commercial data privacy legislation include: the Fair Credit Reporting Act (15 U.S.C. *et seq.*); ECPA (18 U.S.C. § 2701 *et seq.*); the Video Privacy Protection Act (18 U.S.C. § 2710); the Communications Act of 1934 (particularly 47 U.S.C. §§ 222 and 551); Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277 (15 U.S.C. § 6501 *et seq.*; *see also* 16 C.F.R. part 312); the Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. § 1232g *et seq.* and 34 C.F.R. part 99); the Individuals with Disabilities Education Act (20 U.S.C. § 1400 *et seq.*); and Part C of Title XI of the Social Security Act (42 U.S.C. §1320d *et seq.*). In addition, HIPAA and GLBA have associated privacy regulations that must be taken into account. *See* 45 CFR parts 160 and 164 (HIPAA Privacy and Security Rules); 16 CFR part 313 (GLBA Privacy Rule).

[161] Visa Comment at 3. *See also* TRUSTe Comment at 5 ("We believe that it is important to acknowledge specialized expertise of regulatory agencies for specific sectors. At the same time, it is important to distinguish between specialized experience in a particular business area requiring specialized regulation, for example financial services, and common, national priorities and best practices for business protection of consumer privacy.").

[162] *See* DMA Comment at 3 (mentioning online child privacy, financial information privacy, and healthcare information privacy); Comment of Alan Charles Raul at5.

[163] Google Comment at 4.

in a separate comment, is that "baseline privacy protections that apply across sectors that are not specific to any one technology, business model or sector [are] preferred."[164]

In these commenters' views, the current sectoral approach addresses a patchwork of particularized concerns, echoing an earlier view that the Federal statutory scheme is a "jigsaw puzzle" in which the pieces do not always fit together.[165] Commenters argue that this puzzle results from the sectoral approach having been created backwards. Rather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of ad hoc legislation. Commenters noted that this approach confuses consumers and creates large gaps in consumer protection.[166] For example, one commenter stated that "American consumers and companies currently face a confusing patchwork of privacy standards that differ depending on the type of data and the data collector; the vast majority of consumer data is not covered by any privacy law." Another commenter noted that the current sectoral approach "unintentionally results in unnecessary confusion for most individuals."[167]

Overall, commenters found value in the sectoral approach, but recognized that there were significant shortcomings, particularly in areas not covered by a sectoral regulation and where new technologies are emerging. Many commenters would support a Federal commercial data privacy policy that would not "preempt the strong, sectoral laws that already provide important protections to Americans, but rather [would] act in concert with the protections afforded by a baseline privacy law."[168]

---

[164] Microsoft Comment at 7.

[165] Ellen Alderman and Caroline Kennedy, *The Right to Privacy* (1997).

[166] *See, e.g.*, ARMA International Comment at 14 (sectoral approach "well intended effort" but it "create(s) silos in the management of records and information throughout an organization that result in inefficiencies"); CDT Comment at 4-5 ("American consumers and companies currently face a confusing patchwork of privacy standards that differ depending on the type of data and the data collector; the vast majority of consumer data is not covered by any privacy law."); Google Comment at 2 (stating that "the US would benefit from a unified, principles-based legal framework specific to privacy").

[167] ARMA International Comment at 14.

[168] CDT Comment at 5.

Questions for Further Comment:

Are there lessons from sector-specific commercial data privacy laws—their development, their contents, or their enforcement—that could inform U.S. commercial data privacy policy?

G. Preemption of Other State Laws

Recommendation #9: Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

The discussion of how a comprehensive commercial privacy baseline would relate to State laws raises issues more general than security breach notification laws. Some commenters argued that national consistency in commercial information privacy protections would make compliance simpler for businesses, and could help consumers better understand what privacy protections cover their information on the Internet. For example, according to one commenter, "[a] simple, and ideally preemptive, Federal policy on privacy will give both industry and consumers a framework they can understand and manage."[169] Likewise, another commenter supported a preemptive national privacy framework that will "provide all American consumers with the same protections no matter where they may reside."[170]

In contrast, other commenters disfavored preemption, arguing that State legislatures are in a better position to create regulations, both because State legislatures are better able to respond to consumer concerns, and because State legislatures are better able to create innovative approaches to regulation of quickly developing technologies. Some commenters responded that inconsistency and uncertainty creates inefficiencies that can hinder innovation. For example, one commenter stated that "there are regular calls and proposals for additional legislation and regulation [in various States], which make it difficult to predict the path of regulation. The piecemeal approach to the regulation of privacy means

[169] Qwest Comment at 3.

[170] Visa Comment at 3.

that companies like [the commenter] must constantly monitor for legislative and regulatory developments in different jurisdictions."[171]

Commenters suggested options to create a carefully crafted and narrowly tailored preemption provision that would provide greater uniformity while maintaining the ability of States to respond to consumer issues. One suggestion was to narrowly tailor preemption and to ensure that the Federal law provides at least as much protection as the best State laws, and to limit preemption to State laws addressing the same subject matter.[172] Another suggestion, supported by several commenters,[173] was to empower State Attorneys General to enforce the Federal law,[174] and to preserve State unfair and deceptive trade practices statutes. Continuing State enforcement would provide greater resources in addition to allowing interpretations of the law to develop through a wide range of cases.

[171] Datran Comment at 15.

[172] CDT Comment at 12 ("Any preemption of state law in a new baseline federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements.").

[173] *See* National Business Coalition Comment at 4-5; NetChoice Comment at 8; State Privacy and Security Coalition Comment at 6-8 (recommending that the Commerce Department provide further guidance to States on Dormant Commerce Clause and First Amendment issues); Walmart Comment at 7 (calling FTC and state Attorney General enforcement "workable" but pointing to need to address "potential penalties").

[174] This could be implemented in a manner similar to the CAN-SPAM Act, which allows a state Attorney General to bring a civil action in federal court on behalf of the citizens of the state. 15 U.S.C. §7706(f).

Questions for Further Comment:

1) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

2) How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?

3) To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?

4) Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

H. Electronic Surveillance and Commercial Information Privacy

Recommendation #10: The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.[175]

Commenters drew attention to privacy issues surrounding new technologies, such as cloud computing systems, that were broader than the security breach notification issues discussed above. In particular, numerous commenters stated that the laws regulating law enforcement

[175] *See* Statement of Cameron Kerry, General Counsel, U.S. Department of Commerce, The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age, Before the Senate Judiciary Committee (111th Cong., 2d Sess.) (Sept. 22, 2010), http://judiciary.senate.gov/pdf/10-09-22KerryTestimony.pdf; Statement of James A. Baker, Associate Deputy Attorney General, U.S. Department of Justice, The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age, Before the Senate Judiciary Committee (111th Cong., 2d Sess) (Sept. 22, 2010), http://judiciary.senate.gov/pdf/10-09-22BakerTestimony.pdf.

access to Internet communications (and records associated with customer accounts) may undermine consumer trust. Although electronic surveillance was not the focus of the Notice of Inquiry, several commenters raised the issue of Electronic Communications Privacy Act (ECPA) reform.[176] In light of these responses, we seek further comment and data from the public concerning ECPA's effects on the adoption of cloud computing and location-based services. We also seek comment from members of the law enforcement community on how potential ECPA amendments would affect their investigations. Enacted in 1986, ECPA created statutory privacy protections for the then-emerging technologies of wireless communications and networked computers. ECPA was designed "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."[177] The statute criminalizes (1) unauthorized access to communications systems[178], and certain disclosures of the content and related records for wire and electronic communications by a service provider.[179]

Generally speaking, ECPA creates different rules for intercepting communications versus obtaining access to stored communications (with greater restrictions on interceptions) as well as different rules for obtaining communications content versus non-content data (with greater restrictions on obtaining content). A service provider that inappropriately discloses communications covered by ECPA may face civil liability.[180] While ECPA defines the standards for government access to stored communications and records, it also plays a significant role with respect to privacy in the commercial sector by defining limits for disclosures to other third parties. Specifically, ECPA generally prohibits the disclosure to third parties of content of electronic communications such as email[181] but broadly authorizes disclosures of non-content customer records to "any person other than a governmental entity."[182]

One commenter noted that ECPA "remains a critical and indispensable aspect of the U.S. privacy framework" but questioned whether it needed

---

[176] *See, e.g.*, Digital Due Process Comment (discussing ECPA throughout its comment); ACLU Comment at 4-9; CCIA Comment at 6-7; CDT Comment at 32-37; Google Comment at 4; Microsoft Comment at 3-4.

[177] H.R. REP. 99-541 at 3, *reprinted in* 1986 U.S.C.C.A.N. 3557.

[178] 18 U.S.C. § 2701.

[179] 18 U.S.C. § 2702.

[180] *See* 18 U.S.C § 2707 (creating civil liability for certain improper disclosures of stored communications).

[181] 18 U.S.C. § 2702(a).

[182] 18 U.S.C. § 2702(c)(6).

to be updated in light of recent technological changes.[183] ECPA was originally adopted in the mainframe computing environment. In today's environment of cloud computing, Web-based email and applications, and social networking, individuals and U.S. businesses use remote computing resources to a far greater extent than they did 25 years ago.

Commenters also suggested that ECPA's provisions have been interpreted inconsistently, raising the possibility that "the vast amount of personal information generated by today's digital communication services may no longer be adequately protected."[184] This comment applies to communications contents (*e.g.*, the body of an email message) as well as transactional data (*e.g.*, the sender and recipient of an instant message). Transactional records play a critical role in enabling innovation in the digital environment. For example, data on the location of a given mobile device help network and applications providers to provide more customized service offerings. But they also record with increasing detail how individuals interact with remote services and content, as well as where they are and who they know.

The social importance and economic value of recent digital communications innovations and new types of information, such as geolocation data collected from cell phones and content (text, voice, and video) stored in cloud computing systems, cannot be overstated.[185] These technologies allow companies tremendous flexibility in how they manage and store data, relate to customers, and assemble their workforces. They are also providing new avenues for everything from forming friendships to organizing for political action. In some commenters' views, uncertainty about how ECPA applies to these types of data may hinder the adoption of new technologies by individuals and businesses and impedes innovation.[186] Major technology companies echoed these concerns, noting that ECPA, "has been overtaken by technological change, and … no longer strikes the right balance between consumers' privacy interests and the government's legitimate need to access user

---

[183] *See* Mulligan Comment at 3.

[184] Digital Due Process Comment at 2.

[185] *See* ACLU Comment at 2-3 (discussing American consumers' adoption of cloud computing technologies, online social networking, and mobile phones); Computer and Communications Industry Alliance (CCIA) Comment at 6-7 (discussing uncertainty as to ECPA's application to geolocational data); CDT Comment at 34 (discussing uncertainty as to ECPA's application to cloud-stored content).

[186] *See* Digital Due Process Comment at 2 ("Concern about the privacy afforded personal and business information can hold back adoption of emerging technologies, discouraging innovation."); CDT Comment at 34 (noting that this uncertainty "can hold back consumer use of emerging technologies").

information when it comes to new developments like cloud computing."[187]

As the Administration begins the work of examining ECPA's ongoing role in the digital communications environment, they face the question of whether changes in the technology environment since 1986 warrant changes in the statute to preserve the balance Congress struck—and has maintained over time—between the privacy expectations of citizens and the legitimate needs of law enforcement. The Commerce Department is participating with the Department of Justice and other agencies in efforts to develop principles and strategic directions based on a complete understanding of all sides of these issues.[188]

[187] Microsoft Comment at 3. Microsoft also stated: "We believe such [ECPA] reform is vital to bring the statute up-to-date and into alignment with current technological realities and that this should involve extensive stakeholder input. We also believe these reforms of ECPA would complement prior calls for omnibus federal privacy guidelines" *Id.*; *see also* Google Comment at 4 (noting that the "advent of 'cloud computing' . . . is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers").

[188] Cameron Kerry and Christopher Schroeder, White House Council Launches Interagency Subcommittee on Privacy & Internet Policy (Oct. 24, 2010), *available at* http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy).

Questions for Further Discussion:

1) The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.

2) The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what commercial data privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.

3) The Task Force seeks information from the law enforcement community regarding the use of ECPA today and how investigations might be affected by proposed amendments to ECPA's provisions.

III. Conclusion

The Commerce Department Internet Policy Task Force offers these policy options to establish an effective and efficient system for creating privacy protection rules that will benefit all stakeholders in the Internet economy. The Dynamic Privacy Framework seeks to address the privacy challenges discussed in this report with the following objectives:

(1) promoting entrepreneurship, innovation, and economic development;

(2) protecting informed choice and individual privacy in order to promote user trust;

(3) giving existing and emerging Internet companies more consistency, uniformity, and predictability in the privacy protections expected by consumers and required by law;

(4) increasing efficiencies for online companies by bringing industry players together with consumers to fashion cohesive and consistent practices; and

(5) reducing barriers to trade and commerce that stem from disparate privacy standards and requirements in different nations.

In many areas, the current combination of sectoral laws and general FTC Section 5 enforcement works well to protect the privacy of individuals. In other areas, however, technology is changing so rapidly, and is so quickly and widely adopted, that different approaches may need to be considered. The Dynamic Privacy Framework suggested here would combine successful elements of existing U.S. commercial data privacy law with clearer and more effective privacy protection while enabling innovation. In this section we provide a practical illustration of how the Dynamic Privacy Framework would work.

First, a revitalized set of FIPPs, coupled with a PIA requirement (discussed in Section II), would provide more uniform commercial privacy protection across industries and data uses. Second, the Framework calls for the creation of a commercial data-focused Privacy Policy Office, as described in Section II above. The PPO would help identify areas in which new industry or use-specific privacy codes are needed to implement the FIPPs, based on rising consumer complaints, industry initiatives, research, or input from multi-stakeholder groups. Where a company does not choose to be bound by the relevant voluntary codes, FTC and State consumer protection enforcement will continue to ensure that consumers and their personal data are treated fairly.

The Dynamic Privacy Framework could provide mechanisms that allow consumers and businesses to learn from one another. Widespread use of

PIA's, for example, might lead companies to consider consumer reactions to products or features that are similar to those that they plan to introduce.

Thus, the Dynamic Privacy Framework can help accelerate the current iterative process (reform of privacy practices following complaints from individuals and privacy watchdog groups, FTC investigations, and Congressional hearings). Moreover, putting the Framework in action provides a means to update best practices rapidly and gain acceptance for them across an industry.

In this way, the Dynamic Privacy Framework suggested here would allow companies to innovate and create new and useful technologies, but would also facilitate anticipation and quick resolution of commercial data privacy issues while creating guidelines to help prevent the repetition of privacy violations.

Over the past decade, there have been wholesale changes in how Americans use information technology, as well as a pervasive shift in the amount of sensitive information that we entrust to third parties. A key goal is to protect informed choice and to safeguard the ability of consumers to control access to personal information. While this paper outlines some suggestions and direction for possible future consideration, it should be seen as one step in an ongoing conversation, rather than a statement of settled Administration policy views. Through this paper, the Task Force intends to spur further discussion with affected stakeholders both inside and outside of the U.S. government that we hope will lead to the development of a further document that reflects the policy views of the Obama Administration as a whole and that will help us develop an action plan in this important area.

To get there, and consistent with the Administration's general commitment to Open Government and use of the dispersed knowledge of the American people, the continued engagement from all stakeholders is critical. Accordingly, the Commerce Department's Internet Policy Task Force is seeking further comment on the issues enumerated in this report and whether current privacy laws serve consumer interests, innovation and fundamental democratic values. The Department intends for the comments responding to this green paper to contribute to the Administration's domestic policy and international engagement in the area of privacy.

Appendix A: Summary of Recommendations and Questions for Further Discussion

1. The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

    a. Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?
    b. How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement actions?
    c. As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?
    d. Should baseline commercial data privacy legislation include a private right of action?

2. To meet the unique challenges of information intensive environments, FIPPs regarding **enhancing transparency**; encouraging greater detail in **purpose specifications** and **use limitations**; and fostering the development of verifiable **evaluation** and **accountability** should receive high priority.

    a. What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.
    b. What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?
    c. What are the elements of a meaningful PIA in the commercial context? Who should define these elements?
    d. What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?
    e. Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

f. What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?
g. What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?
h. Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?
i. Are purpose specifications a necessary or important method for protecting commercial privacy?
j. Currently, how common are purpose specification clauses in commercial privacy policies?
k. Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?
l. What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?
m. How should purpose specifications be implemented and enforced?
n. How can purpose specifications and use limitations be changed to meet changing circumstances?
o. Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?
p. Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?
q. Are technologies available to help companies monitor their data use, to support internal accountability mechanisms?
r. How should performance against stated policies and practices be assessed?
s. What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

3. Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped up FTC

enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

4. Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration's lead on international outreach on commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO would have any enforcement authority.

    a. Should the FTC be given rulemaking authority triggered by failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified time period?
    b. How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?
    c. Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by a multi-stakeholder process to produce an approved code of conduct?
    d. How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

5. The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

    a. Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?
    b. What should be the scope of FTC rulemaking authority?
    c. Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigations still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

d. Should non-governmental entities supplement FTC enforcement of voluntary codes?
e. At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante "seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until enforcement action is taken against the code.
f. What steps or conditions are necessary to make a company's commitment to follow a code of conduct enforceable?

6. The U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' commercial data privacy frameworks. The United States should also continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks.

7. Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.

   What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?

8. A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections.

   Are there lessons from sector-specific commercial data privacy laws—their development, their contents, or their enforcement—that could inform general U.S. commercial data privacy policy?

9. Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State

jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

a. Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?
b. How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are useful criteria for comparatively assessing how protective different laws are?
c. To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?
d. Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

10. The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

a. The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.
b. The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.

c. The Task Force seeks information from the law enforcement community regarding the use of ECPA today and how investigations might be affected by proposed amendments to ECPA's provisions.

Appendix B: Acknowledgements

The Internet Policy Task Force extends its thanks to all of our colleagues throughout the Executive and Legislative branches who have provided valuable feedback and consultation during the development of this report. We offer special thanks to all of the individuals and private sector organizations who participated in our public Symposium on Privacy and Innovation, and those who submitted written comments to the Notice of Inquiry that served as the basis for this report.

Symposium panelists

- Anne Toth, Vice President of Policy and Head of Privacy, Yahoo
- Dan Burton, Senior Vice President, Global Public Policy, Salesforce.com
- David Hoffman, Director of Security Policy and Global Privacy Officer, Intel
- Deborah Estrin, Professor, University of California
- Deirdre Mulligan, Professor, UC Berkeley
- Dorothy Attwood, Senior Vice President, Public Policy, and Chief Privacy Officer, AT&T
- Ed Felten, Professor, Princeton University
- Fred Cate, Professor, Indiana University
- Harriet Pearson, Vice President, Security Counsel and Chief Privacy Officer, IBM
- Jessica Rich, Assistant Director, Division of Privacy and Identity Protection, Federal Trade Commission
- Jim Halpert, Partner, DLA Piper
- Joel Kelsey, Federal and International Affairs Policy Analyst, Consumers Union
- Jules Polonetsky, Chief Privacy Officer, Future of Privacy Forum
- Larry Irving, Vice President of Global Government Affairs, HP
- Lee Peeler, Executive Vice President, National Advertising Self-Regulation, Council of Better Business Bureaus
- Leslie Harris, President and Chief Executive Officer, Center for Democracy and Technology
- Mike Zaneis, Vice President, Public Policy, IAB
- Nicole Wong, VP and Deputy General Counsel, Google Inc.
- Nuala O'Connor Kelly, Chief Privacy Leader, General Electric
- Pam Dixon, Executive Director, World Privacy Forum
- Peter Cullen, Chief Privacy Strategist, Microsoft
- Phil Verveer, Deputy Assistant Secretary of State and U.S. Coordinator for International Communications and Information Policy

International Communications and Information Policy, State Department
Sandra Hughes, Global Privacy Executive, Procter & Gamble
Tim O'Shaughnessy, CEO, Living Social

Notice of Inquiry Respondents

Alan Charles Raul
American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, and Interactive Advertising Bureau
American Civil Liberties Union
American Federation of Musicians of the United States and Canada
ARMA International
AT&T Inc.
B. Roffmann
Center for Democracy and Technology
Centre for Information Policy Leadership
Coalition for Online Accountability
Computer and Communications Industry Association
Consumer Data Industry Association
Council of Better Business Bureaus
CTIA - The Wireless Association
Data Foundry Inc
Datran Media, LLC
Deirdre K. Mulligan
Digital Due Process
Direct Marketing Association
Dr. John H. Nugent, School of Management, Texas Woman's University
eBay Inc.
EDUCAUSE
Edward Robert McNicholas
Facebook, Inc.
Federal Trade Commission
Financial Services Forum
Fred H. Cate, Indiana University
Future of Privacy Forum
Go Daddy.com, Inc.
Google Inc.
GS1 US and GS1 EPC Global
Hewlett Packard Company
IBM Corporation
Information Technology and Innovation Foundation
Intel Corporation
International Association of Privacy Professionals

International Pharmaceutical Privacy Consortium
Ira Rubinstein, Information Law Institute, NYU School of Law
Katie Shilton & Deborah Estrin, UCLA CENS
Mark MacCarthy, Georgetown University
Marketing Research Association
Matthew Keck, Esq.
Microsoft Corporation
Miriam H. Wugmeister, Karin Retzer, and Cynthia Rich, Morrison and Foerster LLP
National Business Coalition
National Cable and Telecommunications Association
NetChoice
Network Advertising Initiative
Network Solutions, A. Statton Hammock, Jr.
Online Trust Alliance
PRISM International
Procter & Gamble Company
Professor Robert Sprague, University of Wyoming
Qwest
Retail Industry Leaders Association
Salesforce.com
Samuelson Law, Technology and Public Policy Clinic, University of California, Berkeley
School of Law
Software and Information Industry Association
Sören Preibusch, University of Cambridge
State Privacy and Security Coalition
Synaptic Laboratories Ltd.
TechAmerica
Technology Policy Institute, Thomas Lenard and Paul Rubin, Emory University
Telecommunications Industry Association
The Business Forum for Consumer Privacy
TRUSTe
United States Council for International Business
Verizon and Verizon Wireless
Visa Inc.
Walmart
World Wide Web Consortium (W3C)
Zix Corporation