BILLING CODE 3510–60–P

DEPARTMENT OF COMMERCE

Office of the Secretary

National Telecommunications and Information Administration

International Trade Administration

National Institute of Standards and Technology

Docket No. 100402174-0175-01

RIN 0660-XA12

Information Privacy and Innovation in the Internet Economy

AGENCY: Office of the Secretary, U.S. Department of Commerce; National Telecommunications and Information Administration, U.S. Department of Commerce; International Trade Administration, U.S. Department of Commerce; and National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice of Inquiry.

SUMMARY: The Department of Commerce's Internet Policy Task Force is conducting a comprehensive review of the nexus between privacy policy and innovation in the Internet economy. The Department seeks public comment from all Internet stakeholders, including the commercial, academic and civil society sectors, on the impact of current privacy laws in the United States and around the world on the pace of innovation in the information economy. The Department also seeks to understand whether current privacy laws serve consumer interests and fundamental democratic values. After analyzing the comments responding to this Notice, the Department intends to issue a report, which will contribute to the Administration's domestic policy and international engagement in the area of Internet privacy.

DATES: Comments are due on or before [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Written comments may be submitted by mail to the National Telecommunications Administration at U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725,Washington, DC 20230. Submissions may be in any of the following formats: HTML, ASCII, Word, rtf, or pdf. Online submissions in electronic form may be sent to privacy-noi-2010@ntia.doc.gov. Paper submissions should include a three and one-half inch computer diskette or compact disc (CD). Diskettes or CDs should be labeled with the name and

organizational affiliation of the filer and the name of the word processing program used to create the document. Comments will be posted at http://www.ntia.doc.gov/advisory/privacyinnovation.

FOR FURTHER INFORMATION CONTACT: For questions about this Notice contact: Joe Gattuso, Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230, telephone (202) 482-1880; email jgattuso@ntia.doc.gov. Please direct media inquires to NTIA's Office of Public Affairs at (202) 482-7002.

SUPPLEMENTARY INFORMATION:

Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education and political and cultural life, the Department has made it a top priority to ensure that the Internet remains open for innovation. The Department has created an Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment. The Task Force leverages expertise across many bureaus at the Department, including those responsible for domestic and international information and communications technology policy, international trade, cybersecurity standards and best practices, intellectual property, business advocacy and export control. This is one in a series of inquiries from the Task Force. The Task Force is conducting similar reviews of cybersecurity, global free flow of information goods and services, and online copyright protection issues. The Task Force may explore additional areas in the future.

Background: The Department has launched the Privacy and Innovation Initiative to identify policies that will enhance: 1) the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy; 2) the public confidence necessary for full citizen participation with the Internet; and 3) uphold fundamental democratic values essential to the functioning of a free market and a free society.

Innovation in the information economy continues to drive U.S. commerce. Entrepreneurs and innovators in the United States are developing novel information applications and creative ways of delivering existing goods and services via the Internet. American technology companies have created hundreds of thousands of new online applications, revolutionizing how consumers and businesses interact, transact, and use information. Beyond the boundaries of electronic commerce, the Internet is transforming critical sectors of the U.S. and global economy and society, such as health care, energy, education, the arts and political life. In all these sectors, proper use of personal information can play a critical, value-added role, so establishing consumer trust and assuring flexibility for innovators is vital.

Recognizing that economic, social, and political participation in the Internet is essential for all citizens, the United States must establish an environment respectful of long-standing privacy principles and individual privacy expectations, even as they evolve.

Contribution of this NOI to the Internet Policy Task Force: Responses to this Notice will assist the Task Force in preparing its report on Privacy and Innovation in the Information

Economy. The purpose of this report will be to identify and evaluate privacy policy challenges, and to analyze various approaches to meet those challenges. The Task Force's report may include options and recommendations for general regulatory, legislative, self-regulatory and voluntary steps that will enhance privacy and innovation, though the Task Force does not expect to recommend detailed legislative or regulatory proposals at this point. The Task Force is hopeful that the dialogue launched here and the research conducted will contribute to Administration-wide policy positions and global privacy strategy.

Contribution of Online Commerce to the U.S. Economy: Between 1999 and 2007, the United States economy enjoyed an increase of over 500 percent in business-to-consumer online commerce.[1] Taking into account business-to-business transactions, online commerce in 2007 accounted for over $3 trillion dollars in revenue for U.S. companies.[2] The economic benefits provided by the information economy increased even during our economic downturn. During 2008, industry analysts estimate that sales of the top 100 online retailers grew 14.3 percent.[3] In contrast, the U.S. Census Bureau estimates a 0.9 percent decrease in total retail sales over that time period.[4] In 2009, U.S. mobile commerce sales grew over 200 percent compared to the previous year, reaching $1.2 billion.[5] Analysts expect this impressive growth to continue in 2010, projecting $2.4 billion in mobile commerce.[6] Online sales growth and expanding information systems are creating new jobs focused on the information economy and directly impacting our economic recovery.

In addition to the growth of online commerce, the Internet, the World Wide Web, and associated information systems have lead to an unprecedented growth in productivity over the last decade.[7] More businesses are using the Internet to provide electronic records to customers and trading partners, and enterprises are shifting to a digital back office and greener business environment. Although this has spurred additional green innovation, the fact that increasingly more data is being stored electronically and aggregated creates new challenges in the privacy arena.

Sustaining the growth of digital commerce and U.S. commerce generally will require continued innovation in how information is used and shared across the Internet. Commerce today depends on online communication and the transmission of significant amounts of data. Key to the current inquiry, the Department believes this development places data protection in a new light.

The Nexus between Privacy and Commerce, and the Department's Role: Consumers have expressed concern regarding new or unexpected uses of their personal information by online applications. 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

[1] U.S. Census Bureau, "E-Stats," May 28, 2009.
[2] *Id.*
[3] Mark Brohan, "The Top 500 Guide," *Internet Retailer*, June 2009.
[4] U.S. Census Bureau, "Quarterly Retail E-Commerce Sales: 4th Quarter 2008," Feb. 16, 2010, Table 4.
[5] "U.S. M-Commerce Sales to Hit $2.4 Billion This Year, ABI Research Says," *Internet Retailer*, Feb. 16, 2010.
[6] *Id.*
[7] Executive Office of the President of the United States, Council of Economic Advisors of the President, *2010 Economic Report of the President*, at Chapter 10**,** Feb. 2010.

the same time, companies need clear policies that enable the continued development of new business models and the free flow of data across state and international borders in support of domestic and global trade. Our challenge is to align flexibility for innovators along with privacy protection.

The Department has played an instrumental role in developing policies that have helped commerce over the Internet flourish. Over the past two decades, the National Telecommunications and Information Administration (NTIA), in its role as principal adviser to the President on telecommunications policies, has worked closely with other parts of government on these issues.[8] In 1993, the White House formed the Information Infrastructure Task Force (White House Task Force), chaired by the Secretary of Commerce, to develop telecommunications and information policies to promote the development of the Internet. The Privacy Working Group of the White House Task Force, led by NTIA, published a report entitled *Privacy and the National Information Infrastructure*. In the report, NTIA analyzed the state of privacy in the United States as it relates to existing and future communications services and recommended principles to govern the collection, processing, storage and use of personal data.[9] In 1997, the White House Task Force noted NTIA's findings in publishing *A Framework for Global Electronic Commerce*, proposing five principles for international discussion to facilitate the growth of Internet commerce.[10]

Over subsequent years, the Department has worked in a number of international fora to develop privacy and security guidelines that foster international trade. ITA administers the U.S.–European Union (EU) Safe Harbor Framework, 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.[11] ITA also administers the U.S.–Swiss Safe Harbor Framework, which was implemented in 2008. The Department played a significant role in the development of the 1980 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines, the 2005 Asia Pacific Economic Cooperation (APEC) Privacy Framework and the launch of the Trilateral Committee on Transborder Data Flows in 2008. ITA also is involved in bilateral Internet commerce and privacy policy initiatives with India, Japan, China, Korea and other key countries. In addition, ITA works closely with the Department's National Institute of Standards and Technology (NIST) and U.S. industry in developing international standards covering cybersecurity and data privacy.

Today, there is a domestic and global reassessment of approaches to privacy given the fundamental changes in the information economy. The Federal Trade Commission (FTC)

---

[8] 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* Connecting America: The National Broadband Plan, http://download.broadband.gov/plan/national-broadband-plan.pdf, page 55.

[9] *See* National Telecommunications and Information Administration, "Privacy and the National Information Infrastructure: Safeguarding Telecommunications-Related Personal Information," Oct. 1995, http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

[10] *See* President William J. Clinton and Vice President Albert Gore, Jr. "A Framework for Global Electronic Commerce," Washington, DC. 1997, http://clinton4.nara.gov/WH/New/Commerce/read.html.

[11] For more information on the U.S.-EU Safe Harbor Framework, *see* http://www.export.gov/safeharbor/.

recently hosted a series of public roundtables to explore the privacy challenges posed by the wide array of 21st century technology and business practices that collect and use consumer data. The goal of the roundtables was to determine how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation. The FTC accepted public comments on these issues through April 14, 2010, and FTC staff is now reviewing the comments received.[12] The Department of Commerce has participated in these sessions and will continue to collaborate with the FTC going forward. The National Broadband Plan (Plan), which the Federal Communications Commission released on March 16, 2010, makes recommendations for government action to address online privacy issues.[13] Specifically, the Plan recommended clarifying the relationship between users and their online profiles; developing trusted "identity providers" to help consumers manage their data; and creating principles to require that customers provide informed consent before service providers share certain types of information with third parties.[14] The Plan also urged the creation of a number of Internet privacy-related innovations to enhance our nation's energy, education, health care, and government performance.[15]

Internationally, the OECD's Committee on Consumer Policy (CCP) recently launched a review of the 1999 *Guidelines for Consumer Protection in the Context of E-Commerce*.[16] The OECD Working Party on Information Security and Privacy (WPISP) is conducting a 30th anniversary study of the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[17] The APEC Electronic Commerce Steering Group is developing a system for cross-border data flows among APEC members to implement its 2005 Privacy Framework.[18] The United States, Canada and Mexico recently finalized a report highlighting the need to address impediments to transborder data flows.[19] Finally, the European Commission is evaluating and considering changes to its 1995 *Directive on Data Protection*.[20] Given the global reevaluation of data privacy policies, the Task Force is seeking to determine whether current privacy frameworks, or frameworks that are in development, create barriers to innovation on the Internet and, if so, how they might be addressed.

REQUEST FOR COMMENT:

---

[12] *See* Federal Trade Commission, Exploring Privacy: A Roundtable Series, http://www.ftc.gov/bcp/workshops/privacyroundtables/.

[13] *See* Connecting America: The National Broadband Plan, http://download.broadband.gov/plan/national-broadband-plan.pdf.

[14] *Id.* at 55–56 (Recommendations 4.14–4.16).

[15] *Id.* at 208. 234–35, 252, 253, 286 (Recommendations 10.4, 11.11, 12.2, 12.5, 14.6, 14.7).

[16] *See* OECD, Conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy, Washington, DC, Dec. 8–10, 2009, http://www.oecd.org/document/20/0,3343,en_21571361_43348316_43410324_1_1_1_1,00.html.

[17] *See* OECD, The 30th Anniversary of the OECD Privacy Guidelines, http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html.

[18] *See* APEC, Data Privacy Pathfinder Projects Implementation Work Plan, http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.

[19] *See* Office of Technology and Electronic Commerce, Trilateral Committee on Transborder Data Flow, http://spp.gov/pdf/Eng_Statement_of_Free_Flow.pdf.

[20] *See* European Commission, Freedom, Security, and Justice, Data Protection, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

This Notice of Inquiry seeks comment on the impact of the current privacy framework on Internet commerce and innovation, both from the commercial and consumer perspective, as well as ways in which it may be necessary to adjust today's privacy framework to preserve and even enhance innovation and privacy in our new web-centric information environment.

The questions below are intended to assist in framing the issues and should not be construed as a limitation on comments that parties may submit. The Department invites comment on the full range of issues that may be presented by this inquiry. Comments that contain references, studies, research and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

1. The U.S. Privacy Framework Going Forward

Prior to releasing this Notice, the Department conducted listening sessions with a wide range of stakeholders in order to understand the questions most pertinent to stakeholders in the commercial, academic and civil society sectors and that have the greatest bearing on innovation and consumer expectations. During the course of those conversations, the Department heard that the customary notice and choice approach to consumer protection may be outdated, especially in the context of information-intensive, highly interactive, Web-based services. According to some, online interactions and web-based information linkages have become so complicated that it is increasingly difficult to provide consumers truly meaningful notice and choice. In lieu of, or in addition to notice and choice, some have advanced the notion that sophisticated data managers migrate to a "use-based" model.[21] These assertions raise several questions.

Does the existing privacy framework provide sufficient guidance to the private sector to enable organizations to satisfy these laws and regulations? Are there modifications to U.S. privacy laws, regulations and self-regulatory systems that would better support innovation, fundamental privacy principles and evolving consumer expectations? If so, what areas require increased attention, either in the form of new laws, regulations or self-regulatory practices? What is the state of efforts to develop a self-regulatory privacy framework? Are there certain minimum or default requirements that should be incorporated either into self regulation or to law? What is the proper goal of privacy laws and regulations: should the focus on commercial data privacy policy be on satisfying subjective consumer expectations or is it also necessary to enact objective privacy principles?

Those addressing the utility of self-regulation should differentiate between practices defined and monitored unilaterally by an enterprise, and practices and monitoring systems developed by third-parties. If a third-party develops best practices, what mechanisms would be available for users and civil society to provide feedback? How will industry sectors enforce best-practice regimes when it might not be in their economic interest to do so?

[21] Use-based rules regulate the types of uses (or purposes) for which personal information may be employed as opposed to regulating what personal data can be collected.

Is the notice and choice approach to consumer data privacy still a useful model? Are there alternative approaches or frameworks that might be used instead of notice and choice? Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use.[22] Describe how a use-based privacy system would work? How should policy makers determine what constitute harmful uses of personal information in this model? Are there examples from existing privacy laws and regulations that suggest strengths and weakness of the 'use-based' model? Is this "use-based" model for commercial data privacy a workable approach for companies and consumers? What is the relationship between use-based privacy rules and proposed accountability systems?

2. U.S. State Privacy Laws

Most U.S. states have data breach laws or private sector data privacy laws, and some have both.[23] These and other state laws and regulations govern how companies can collect, use and disclose personal data about citizens of each state. The Task Force seeks input on how different state-level laws and regulations affect companies' compliance costs and product development processes. The agencies seek comment on whether a diversity of state privacy laws has a positive, negative or neutral impact on the privacy rights of Internet users.

What, if any, hurdles do businesses face in complying with different state laws concerning privacy and data protection? Is there harmonization among state laws governing data protection? Please describe any significant differences that exist between the states. How does complying with multiple states' laws affect organizations' business activities and ability to operate online? What types of existing state laws have the greatest impact on companies' business models? What approaches do companies take to comply with privacy laws in multiple states? Have state laws that attempt to regulate location privacy had an impact on the development of business models or the way in which businesses introduce new products in various markets? [24] What future directions in state law are anticipated? Does the variety of technology-specific state laws help individual Internet users exercise their rights, or does it create confusion for consumers? Have technology-specific state privacy laws affected online innovation and business development and, if so, how?

3. International Privacy Laws and Regulations

A variety of foreign laws govern how companies collect, use and share personal data. There are national laws, sub-national laws, a region-wide Directive in the European Union in addition to

---

[22] For more information on the use-based model, see e.g., The Business Forum for Consumer Privacy "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," Dec. 7, 2009, http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf.

[23] For a list of state data breach and data privacy laws see The National Conference of State Legislatures, Telecommunications and Information Technology, http://www.ncsl.org/Default.aspx?TabID=756&tabs=951,71,539#539.

[24] Locational privacy (also known as "location privacy") is an individual's ability to move in public space with the expectation that his or her location will not be systematically and secretly recorded for later use.

member-state laws and, in many countries, laws under development. The Task Force seeks input on how international data privacy laws and regulations affect global Internet commerce, companies' compliance costs and product development process, and Internet users.

What, if any, hurdles do businesses face in complying with different foreign laws concerning privacy and data protection? What types of foreign privacy laws have the greatest impact on companies' business models? What approaches have businesses used to comply with laws in multiple foreign jurisdictions? Do foreign laws that contain content-based restrictions impede global trade or foreign investment? For example, are there laws that restrict the types of information that may be transferred, displayed, published or posted online which have deterred businesses from entering certain markets or from engaging in certain cross-border activity? Are laws that permit governments to have access to personal information an impediment to innovation or global trade and investment? If so, are the laws themselves actually an impediment, or is it the application and enforcement of such laws that are of concern? What challenges do businesses face when trying to transfer data across borders? What lessons have been learned from the U.S.–EU Safe Harbor Framework that could be applied in the global context? What mechanisms do organizations use to enable cross border data transfers? To what extent if any do privacy laws outside the United States create third party liability for Internet intermediaries such as search engines, content hosting services, Internet service providers or others?[25]

How does the multiplicity of international privacy laws impact Internet users? What models for protection of individual privacy rights across borders have proven effective in the global environment of the Internet? Can countries with difference privacy rules cooperate to protect the privacy interests of their citizens?

How might privacy regimes in the United States and others jurisdictions across the globe be harmonized?

4. Jurisdictional Conflicts and Competing Legal Obligations

Today, cloud computing models allow organizations to collect, store, access and process data in separate locations around the world. This can create challenges for both companies and regulators in determining where data is located and who has jurisdiction over that data. In addition, different regulators may attempt to assert jurisdiction over data or a company's business practices, which may create conflicting or competing legal obligations. For example, one jurisdiction may require a company to retain its data, while another may ask that data be expunged after its use. The Task Force seeks information on any jurisdictional conflicts companies and regulators face as a result of data privacy laws, how they are reconciled and what, if any, effect they have on trade and foreign investment.

[25] *See, e.g.*, 47 U.S.C. § 230(c) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

Do organizations face jurisdictional disputes as a result of domestic or foreign privacy laws? Please describe the types of jurisdictional disputes that arise as a result of privacy laws. What, if any, conflicting legal obligations do companies face as a result of data privacy laws? How do companies address jurisdictional conflicts and any resulting conflicting legal and regulatory obligations? How do such conflicts affect the cost of doing business? Do jurisdictional issues affect global sales of U.S. companies when the U.S. company stores data from non-U.S. customers inside the United States? Does cloud computing, or other methods of globally distributing and managing data, raise specific issues with respect to jurisdiction of which Commerce and regulators should be aware? Have jurisdictional conflicts had any impact on U.S. consumers?

5. Sectoral Privacy Laws and Federal Guidelines

The U.S. privacy framework is composed of sectoral laws combined with constitutional, statutory, regulatory and common law protections, in addition to industry self-regulation. Sectoral laws govern the handling of personal data considered most sensitive. For instance, the Communications Act includes privacy protections that telecommunication providers and cable operators must follow when handling the personal information of subscribers.[26] The Health Insurance Portability and Accountability Act (HIPAA) stipulates how "covered" health care entities can use and disclose data.[27] The Fair Credit Reporting Act (FCRA) governs how consumer reporting agencies share personal information.[28] The Gramm-Leach-Bliley Act (GLBA) covers certain data held by financial institutions.[29] The Children's Online Privacy Protection Act (COPPA) protects information collected online about children under 13.[30] In addition to these sectoral laws, the Federal Trade Commission Act (FTC Act) provides the FTC authority to combat "unfair or deceptive" business practices.[31] The FTC also provides guidance for businesses regarding privacy and security practices.[32] These laws and guidelines affect U.S. economic activity by controlling how organizations can use data to develop new products and services or improve existing ones. The laws and guidelines differentiate between categories of

[26] *See* 47 U.S.C. § 551 (2006) (Protection of Subscriber Privacy).

[27] *See* 42 U.S.C. § 1320 (2006) ("A covered entity may not use or disclose protected health information" except as permitted by statute.). For information on HIPPA, *see* http://www.hhs.gov/ocr/privacy/.

[28] *See* 15 U.S.C. § 1681r ("Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined under title 18, imprisoned for not more than 2 years, or both."). For information on the FCRA, *see* http://www.ftc.gov/os/statutes/fcrajump.shtm.

[29] *See* 15 U.S.C. § 6801–09, 6821–27 (2006). *See e.g.*, 15 U.S.C. § 6801a (2006) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."). For information on the GLBA, *see* http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

[30] *See* 15 U.S.C. § 6501–06 (2006). *See, e.g.*,15 U.S.C. § 6502a (2006) ("It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the [statute]."). For information on the COPPA, *see* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

[31] *See* 15 U.S.C. § 41–58 (2006). *See, e.g.*, 15 U.S.C. § 45(a) (2006) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."). For information on the FTC Act, *see* http://www.ftc.gov/ogc/stat1.shtm.

[32] *See* Federal Trade Commission, Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

data (*e.g.*, health care, financial and other), and they differentiate between data subjects (*e.g.*, children and others). The Task Force seeks input on how the U.S. privacy framework affects business innovation, accountability and compliance related to the use of personal information.

How does the current sectoral approach to privacy regulation affect consumer experiences, business practices or the development of new business models? How does the sectoral approach affect individual privacy expectations? What practices and principles do these sectoral approaches have in common, how do they differ? Are there alternatives or supplements to the sectoral approach that should be considered? What can be done to make the current framework more conducive to business development while ensuring effective privacy protections?

6. New Privacy-Enhancing Technologies and Information Management Processes

Researchers at universities, think tanks, international organizations and company laboratories are developing privacy-enhancing technologies and business methods to implement company privacy policies and user preferences and to increase company accountability. Researchers, for example, are considering consumer-targeted systems that employ text analysis and behavioral economics to create enhanced notification to consumers about privacy policies or to manage the information they are sharing. These technologies and ever-evolving, internal business processes have become an integral component of industry self-regulation. At the same time, researchers recognize the limitations of privacy-enhancing technologies related to consumer and industry adoption, new research demonstrating the possibility of data re-identification,[33] and the continued security risks posed by hackers and other forms of electronic intrusion. The Task Force seeks input on the development, use and acceptance of privacy-related technologies and business processes and their potential to enhance consumer trust in Internet commerce.

What is the state of development of technologies and business methods aimed at: 1) improving companies' ability to monitor and audit their compliance with their privacy policy and expressed user preferences; 2) using text analysis or similar technologies to provide privacy notices; and 3) enabling anonymized browsing, communication and authentication? Please describe any other ongoing efforts to develop privacy-enhancing technologies or processes of which the Commerce Department should be aware. How has recent research demonstrating the possibility of data re-identification affected anonymization research efforts? Have consumers or businesses readily accepted or used these technologies when they were made available? What steps can be taken to assure that privacy-enhancing business processes are robust, complied with and regularly updated? Do technology designers and implementers have the right balance of incentives to include privacy considerations at the design phase of their work? Have currently-available privacy-related technologies and processes increased user trust or companies' ability to manage personal information?

[33] Re-identification is the process by which personal data is matched with its true owner. In order to protect privacy of consumers, personal identifiers, such as social security numbers, are often removed from databases containing sensitive information. This de-identified data safeguards consumer privacy. However, computer scientists recently revealed that this "anonymize" data can be re-identified, such that the sensitive information may be linked back to an individual.

Finally, the FCC has raised a number of privacy-related recommendations for government action.[34] Specifically, the Plan recommends clarifying the relationship between users and their online profiles; developing trusted "identity providers" to assist consumers manage their data; and creating principles to require customers provide informed consent before service providers share certain types of information with third parties. What kinds of contributions to privacy and innovation could such identity providers make? What marketplace experience is there with such trusted third parties? Are there any services of this sort imagined by the FCC in operation today? Is any government action needed to encourage the marketplace in this direction?

7. Small and Medium-Sized Entities and Startup Companies

Small and medium-sized entities (SMEs) and startup companies face the same data protection laws and guidelines as their larger counterparts, but with fewer resources. The Task Force seeks input on how the issues outlined above might uniquely affect smaller companies and how these effects are managed.

How do existing privacy laws impact SMEs and startup companies? Please describe any unique compliance burdens placed on smaller companies as a result of existing privacy laws. Are there commercial or collective tools available to address such issues? How might privacy protections be better achieved in the SME environment? Have smaller companies been unable to engage in certain types of business activities as a result of existing privacy laws? Do foreign privacy laws pose a barrier to SMEs' international business plans? If such unique burdens do exist, what mechanisms do SMEs see as helpful for surmounting those challenges?

8. The Role for Government/Commerce Department

The U.S. privacy framework described above is multi-faceted. The combination of sector-specific laws for sensitive data, self-regulation, complemented by FTC enforcement authority, transparent privacy practices, and voluntary guidelines, have generated industry best practices, privacy seal programs and private sector innovation to enhance privacy disclosures and consumer choice regarding data usage. In many, though not all, cases, this has been formula for success for build on. Yet, surveys continue to indicate that consumers are concerned or confused about what happens to their personal information online. The Task Force seeks input on how to help address barriers to increased innovation and consumer trust in the information economy.

How can the Commerce Department help address issues raised by this Notice of Inquiry?

Dated: April 20, 2010.

/s/
Gary M. Locke,
Secretary of Commerce.

[34] *See supra* note 14.

_____/s/_____
Lawrence E. Strickling,
Assistant Secretary for Communications and Information.

_____/s/_____
Francisco J. Sánchez,
Under Secretary of Commerce for International Trade.

_____/s/_____
Patrick Gallagher,
Director, National Institute of Standards and Technology.