PLEASE NOTE: Though it is not intended or expected, should any discrepancy occur between the document here and that published in the Federal Register, the Federal Register publication controls.
This notice is being made available through the Internet solely as a means to facilitate the public's access to this document.

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. 101214614-0614-01]

RIN 0660- XA22

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; National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice and request for public comments.

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. On April 23, 2010, the Department published a Notice of Inquiry seeking comment from all Internet stakeholders 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 now seeks further comment on its report entitled, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," available at http://www.ntia.doc.gov/internetpolicytaskforce/. Through this Notice requesting comments on the report, the Department hopes to spur further discussion with Internet stakeholders that will

lead to the development of a series of Administration positions that will help develop an action plan in this important area.

DATES: Comments are due on or before January 28, 2011.

ADDRESSES: Written comments may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., 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 privacynoi2010@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/internetpolicytaskforce/.

FOR FURTHER INFORMATION CONTACT: For questions about this Notice contact: Aaron Burstein, Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Washington, DC 20230; telephone (202) 482-1880; email aburstein@ntia.doc.gov; or Manu Bhardwaj, Office of Policy Analysis and Development, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Washington, DC 20230; telephone (202) 482-4985; email mbhardwaj@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 established the Internet Policy Task Force to identify leading public policy and operational challenges in the Internet environment. The Task Force leverages expertise across many bureaus, including those responsible for domestic and international information and communications technology policy, international trade, cyber security standards and best practices, intellectual property, business advocacy and export control.

Moreover, the Obama Administration has launched an initiative to develop an interagency policy structure for commercial data privacy issues. The Commerce Department's General Counsel Cameron Kerry and the Justice Department's Assistant Attorney General for the Office of Legal Policy Christopher H. Schroeder chair a recently launched subcommittee of the National Science and Technology Council that the White House has chartered to work on Privacy and Internet Policy issues. Through that vehicle, the Administration is engaging agencies throughout the U.S. Government in a conversation on commercial data privacy to ensure that the Administration speaks with one voice and takes advantage of its many areas of expertise to promote the development of strategic and comprehensive Internet privacy policies.

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; and 2) the public confidence necessary for full citizen participation with the Internet. On April 23, 2010, the Department published a Notice of Inquiry seeking 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.[1] Through that Notice of Inquiry,

[1] Notice of Inquiry, Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226 (Apr. 23, 2010), available at http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf. Comments received in response to this Notice of Inquiry are posted at http://www.ntia.doc.gov/comments/100402174-0175-01/.

the Department sought to understand whether current privacy laws serve consumer interests and fundamental democratic values. The Department also held a symposium on May 7, 2010, to discuss stakeholder views and to facilitate further public discussion on privacy policy in the United States.[2]

The Department has now prepared a report, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," as a vehicle to spur further discussion with Internet stakeholders on this important area of policy development. [3]

REQUEST FOR COMMENT:

This Notice seeks input on the report. The questions below, which also appear in Appendix A of the report, are intended to assist in identifying issues. They should not be construed as a limitation on comments that parties may submit. 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) Should baseline commercial data privacy principles, such as comprehensive FIPPs, be enacted by statute or 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 rule? What criteria are useful for deciding

[2] The Public Meeting Notice, 75 Fed. Reg. 19942 (Apr. 16, 2010), and the meeting agenda are available at http://www.ntia.doc.gov/internetpolicytaskforce/.

[3] The report is available at http://www.ntia.doc.gov/internetpolicytaskforce/.

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?

5) 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.

6) 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?

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

8) 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?

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

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

11) 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?

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

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

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

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

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

17) How should purpose specifications be implemented and enforced?

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

19) 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?

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

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

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

23) 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?

24) 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?

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

26) 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?

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

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

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

30) 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?

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

32) At what point in the development and 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.

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

34) 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.)?

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

36) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matter, leaving states free to regulate emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

37) How could a preemption provision ensure that federal law is no less protective than any existing state laws? What are useful criteria for comparatively assessing how protective different laws are?

38) To what extent should state Attorneys General be empowered to enforce national commercial data privacy legislation?

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

40) 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 links any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.

41) 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.

42) 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.

Dated: December 16, 2010.

/s/
_____
Gary Locke,
Secretary of Commerce.

/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.