

## E-ALERT | Global Privacy and Data Security

December 17, 2010

### DEPARTMENT OF COMMERCE RELEASES PRIVACY REPORT

The Department of Commerce (DoC) yesterday released its much-anticipated “green paper” on online privacy, entitled “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.” The paper is part of an ongoing examination of privacy practices in the commercial sector by DoC’s Internet Policy Task Force, which was established in April of this year.

The DoC report recommends adoption of a comprehensive national framework for commercial data privacy that would be built around a set of Fair Information Practice Principles (FIPPs), which the DoC report refers to as “a privacy bill of rights.” Although it was rumored that the report would endorse baseline privacy legislation, it stops short of doing so and instead seeks comment on the best means of implementing the FIPPs framework. It also calls for the development of voluntary industry privacy codes, the creation of a Privacy Policy Office within DoC, and consideration of data breach legislation and reform of the Electronic Communications Privacy Act (ECPA).

The DoC report follows on the heels of the Federal Trade Commission’s release of its own report on consumer privacy. Both reports reflect a general belief that the federal government should take a greater role in establishing and protecting consumer privacy rights in the online world. Notably, while the FTC’s approach emphasizes “privacy by design” and a “do-not-track” mechanism in connection with online behavioral advertising, the DoC’s report does not recommend architectural changes, but instead urges companies to improve disclosures and abide by self-created limitations on data collection and use.

DoC views its green paper as initiating further discussion, and it includes a range of questions concerning the report’s recommendations. (A full list of the questions included in the DoC report is attached to this e-alert.) The deadline for comments has not yet been set, but comments likely will be due in mid-February, shortly after the deadline for filing comments on the FTC report.

The DoC report makes the following recommendations:

#### Support for Fair Information Practice Principles

##### **FIPPs Framework: A Shift From Notice-and-Consent**

The report recommends a framework based on the concept of “Fair Information Practice Principles,” or “FIPPs,” which are a set of broad privacy principles that would guide industry efforts to implement privacy initiatives. DoC claims that its proposed framework would improve upon the current “notice-and-choice” model of commercial data protection, which DoC faults for being dependent on consumers’ ability to

understand and act on individual companies’ privacy notices. Building upon previous FIPPs models developed by other government agencies, including the FTC’s FIPPs model from the mid-1990s, DoC recommends the adoption of several key principles and requests comment on how (and by whom) these principles would be enacted and enforced.

**Key Principles:**

- **Enhanced Transparency**

The “enhanced transparency” principle centers on increased clarity, rather than increased quantity, of information. Companies would carry out the principle by providing information about their privacy practices in a clearer, more comprehensible manner than DoC believes is typical in existing privacy notices. To promote clear privacy notices, the report suggests that companies could publish the results of evaluations and other accountability measures. The report also suggests encouraging companies to conduct privacy impact assessments, the results of which would be made public, before introducing new technologies.

- **Purpose Specification and Use Limitation**

The “purpose specification” principle would require an organization to disclose to consumers its reasons for collecting personal data. The “use limitation” principle would require the organization to adhere to its stated purposes. The effect of the two principles in combination would be to limit organizations’ ability to use data in ways that were not disclosed when the data was collected.

- **Evaluation and Accountability**

The principles above, as well as other FIPPs which are developed, would be backed up by an “evaluation and accountability” principle. Under this principle, companies would be expected to perform internal and external audits comparing actual data use against the specified uses.

- **Retention of Federal Sectoral Laws**

The report recommends that the FIPPs-based commercial data privacy framework not preempt existing sectoral privacy laws, such as HIPAA in the healthcare sector and the Gramm-Leach-Bliley Act in the financial sector.

- **Partial Preemption of State Law**

While the report avoids specifics, it suggests that at least some preemption of state law would be appropriate, but it stops short of calling for a total preemption of state privacy regulation.

**Promotion of Voluntary but Enforceable Codes of Conduct**

**Praise for NAI**

The report encourages federal and state agencies to promote the creation of voluntary, enforceable codes of conduct. It praises the existing Network Advertising Initiative behavioral advertising code but laments that thus far it is the only significant example of a voluntary privacy code developed through industry collaboration.

**Codes as Alternatives to FIPPs** The report suggests that codes of conduct can supplement or replace FIPPs where the comprehensive and general principles embodied in FIPPs are not appropriate. It also suggests that voluntary codes of conduct can promote regulatory certainty and leverage industry expertise to avoid inappropriate technological lock-in.

**Methods for Agencies to Encourage Codes:** The report recommends three methods by which DoC and other agencies can encourage the creation of voluntary but enforceable codes:

- **Persuasion by Agencies** (1) The report argues that federal agencies should expend more effort persuading industry to build voluntary codes. However, the report expresses skepticism that this method alone will be successful.
- **Heightened FTC Enforcement** (2) The report encourages the FTC to enforce current law more aggressively, thereby bringing more attention to privacy issues.
- **Safe Harbor** (3) The report favors the creation of a code that, if followed, would create a “safe harbor” from certain enforcement actions by the FTC or state attorneys general and from any FIPPs-based commercial data privacy legislation that is enacted. It suggests that to qualify for a safe harbor, a code must be created through an open, multi-stakeholder process and be approved by the FTC.

**Creation of Privacy Policy Office Within Department of Commerce**

**Privacy Office Roles:** The report recommends the creation of a new Privacy Policy Office to be housed within the DoC. The principal purpose of the Office would be to bring together stakeholders and other agencies to build new policy proposals and to assist industry in creating the voluntary codes of conduct described above. The Office also would coordinate efforts from the White House to engage in international outreach on commercial data privacy issues. In addition, it would work with the FTC to educate consumers and businesses about privacy issues. Consistent with the recommendations in the report, the proposal to create a Privacy Policy Office reflects an increased profile for privacy matters on the part of the Obama Administration.

**Relationship to Existing Agencies** Consistent with the FTC’s longstanding informal role as the nation’s “privacy watchdog” and the roles that other agencies play in industry-specific privacy regulation, the DoC report suggests that the Privacy Policy Office would not displace any existing federal agencies’ roles with respect to privacy. The report therefore proposes that the new office not be given rulemaking or enforcement authority. It also recommends retention of the Chief Privacy Officers currently employed by many agencies.

## International Cooperation

### Call for Mutual Recognition Framework

The report argues that the United States should expand its role in the international privacy space and recommends working toward increased international cooperation on privacy issues. It proposes development of a system “for mutual recognition of other countries’ commercial data privacy frameworks.” It also suggests that the U.S. should continue to support the APEC Data Privacy Pathfinder project, which is developing cross-border privacy rules for the Pacific region.

## Data Breach Legislation

### Proposal

The report recommends “consideration” of enacting a “comprehensive commercial data security breach framework for electronic records.” Such a law would include notification provisions and requirements for “strict data security protocols.” It proposes modeling the law on “the effective protections that have emerged from state security breach notification laws and policies.”

### Preemption

DoC suggests that the legislation, if enacted, should promote uniformity but also should allow states to build upon the law “in limited ways.”

## ECPA Reform

### Call for White House Review of ECPA

The report suggests that President Obama should review and consider recommending changes to ECPA, paying particular attention to cloud computing and location-based services. ECPA was enacted in 1986, and the report echoes criticisms that it is unclear and not well-suited to today’s technology environment.

\* \* \*

## COVINGTON & BURLING LLP

If you have questions regarding the DoC report or its impact on your business, or if you are interested in submitting comments, please contact the following members of our Global Privacy & Data Security Practice Group:

Erin Egan	202.662.5145	<a href="mailto:eegan@cov.com">eegan@cov.com</a>
Yaron Dori	202.662.5444	<a href="mailto:ydori@cov.com">ydori@cov.com</a>
Rob Sherman	202.662.5115	<a href="mailto:rsherman@cov.com">rsherman@cov.com</a>
Daniel Kahn	202.662.5539	<a href="mailto:dkahn@cov.com">dkahn@cov.com</a>
Stephen Satterfield	202.662.5659	<a href="mailto:ssatterfield@cov.com">ssatterfield@cov.com</a>

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to [unsubscribe@cov.com](mailto:unsubscribe@cov.com) if you do not wish to receive future emails or electronic alerts.

© 2010 Covington & Burling LLP, 1201 Pennsylvania Avenue, NW, Washington, DC 20004-2401. All rights reserved.

## Appendix to DoC Report

### Questions for Comment on Proposed Framework

## 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.