

Morrison & Foerster Client Alert.

December 20, 2010

Department of Commerce Proposes “Dynamic Policy Framework” for Privacy; Requests Comments

By Reed Freeman and Julie O’Neill

On December 16, 2010, the Department of Commerce released a Green Paper on privacy, entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.

The Green Paper marks the culmination of the Department’s year-long review of privacy issues – involving consultations with commercial, civil society, governmental and academic stakeholders, the receipt of comments on privacy and innovation, and a public symposium – and it provides an initial set of recommendations to help further the discussion around a commercial data privacy framework.

This Green Paper represents the Obama Administration’s opening of a dialog on privacy (the Federal Trade Commission is an independent federal agency), and as such represents a first step in a discussion that could continue for months or years. To that end, the Department is not recommending legislation now, but rather is considering a variety of options to institutionalize privacy in the private sector, from voluntary codes of conduct enforced by the Federal Trade Commission, to the possibility of recommending baseline legislation later, and to self regulation.

The Department’s focus is on commercial data privacy. It makes no recommendations with respect to data privacy laws and policies that cover information maintained by the Federal Government, or those that cover specific industry sectors, such as **healthcare**, **financial services**, and **education**.

While making it clear that consumers’ privacy must be respected and that consumers must be given informed choice over the use of their data, the Green Paper takes a reasonably business-friendly approach. In fact, the Department acknowledges that its objectives include:

- Promoting entrepreneurship, innovation and economic development;
- Giving Internet companies more consistency, uniformity and predictability in the privacy protections expected by consumers and required by law;

Beijing

Paul D. McKenzie 86 10 5909 3366
Jingxiao Fang 86 10 5909 3382

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365
Antonio Seabra Ferreira 32 2 340 7367

Hong Kong

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

Los Angeles

Mark T. Gillett (213) 892-5289
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Chris Coulter 44 20 7920 4012
Suzanne Horne 44 20 7920 4014

New York

Gabriel E. Meister (212) 468-8181
Joan P. Warrington (212) 506-7307
John F. Delaney (212) 468-8040
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Bryan Wilson (650) 813-5603
Christine E. Lyon (650) 813-5770

San Francisco

Roland E. Brandel (415) 268-7093
James McGuire (415) 268-7013
William L. Stern (415) 268-7637
Jim McCabe (415) 268-7011

Tokyo

Daniel P. Levison 81 3 3214 6717
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.

Andrew M. Smith (202) 887-1558
Cynthia J. Rich (202) 778-1652
Julie O’Neill (202) 887-8764
Nathan David Taylor (202) 778-1644
Obrea O. Poindexter (202) 887-8741
Reed Freeman (202) 887-6948
Richard Fischer (202) 887-1566
Kimberly Strawbridge Robinson (202) 887 1508

Morrison & Foerster Client Alert.

- Increasing efficiencies for online companies by bringing industry players together with all other stakeholders to fashion cohesive and consistent privacy principles; and
- Reducing barriers to trade and commerce that stem from disparate privacy standards and requirements in different countries.

The Department has emphasized that the Green Paper is part of a continuing dialogue, and it has therefore requested comments on it. **Comments are due by January 28, 2011.** A Department official has indicated that the Department plans to act as quickly as possible after reviewing the comments it receives.

The paper sets forth a series of policy recommendations for a comprehensive framework for commercial data privacy.

The recommendations, set forth below, are presented under four broad categories:

- (A) Enhance consumer trust online through recognition of revitalized Fair Information Practice Principles;
- (B) Encourage the development of voluntary, enforceable privacy codes of conduct;
- (C) Encourage global interoperability; and
- (D) Ensure nationally consistent security breach notification rules.¹

A. Enhance consumer trust online through recognition of revitalized Fair Information Practice Principles (FIPPs).

The paper recommends that the government recognize a full set of FIPPs, such as those developed by the Department of Homeland Security, as the foundation for its policy with respect to commercial data privacy. Except to generally note that the emphasis should be on substantive privacy protection for consumers, *the paper sets forth no details as to how the Department believes the FIPPs should be implemented and enforced* (e.g., through legislation, other formal means, or via a private right of action). Instead, it seeks comment on those issues.

The paper emphasizes that certain of the FIPPs should receive high priority:

- **Enhanced transparency**, provided through simple notices. The Department believes that many privacy policies are difficult for consumers to understand. It does not, however, want to see the imposition of comprehensive prescriptive rules because a one-size-fits-all framework is unlikely to work across business models and may be insufficiently flexible to adapt to new models and technologies.
 - The Department also posits that the “transparency” principle may require more than the provision of notice and control. One complementary approach, for example, would encourage businesses to enhance their overall transparency through privacy impact assessments (PIAs) that identify and evaluate risks arising from the use of personal information in new practices or technologies. (This proposal echoes the “privacy by design” approach proposed by the Federal Trade Commission in its own recent privacy report.) The Department supports the use of PIAs for several reasons, including because it does not impose any particular requirements or constraints on a company’s product design or information practices; rather, it gives the company itself the latitude to determine how its business comports with the FIPPs. The Department also raises the possibility of businesses’ publication of their PIAs, in an effort at further transparency.

¹ In addition to the proposals set forth below, the green paper recommends an Administration review of the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. It says that a goal of the review 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.

Client Alert.

- The alignment of consumer expectations and information practices through **purpose specification** and **use limitations**. These principles do not require externally imposed, prescriptive rules that govern how companies use personal information. Instead, they would require businesses to provide consumers with clear, specific notice of their data practices and prevent them from deviating from the promises made in any such notice.
- The development of **verifiable evaluation and accountability**, to ensure that businesses adhere to the promises they make.

B. Encourage the development of voluntary, enforceable privacy codes of conduct in specific industries through the collaborative efforts of multi-stakeholder groups, the FTC, and a Privacy Policy Office within the Department of Commerce.

In the Department's view, the adoption of baseline FIPPs is insufficient to protect privacy, particularly in the ever-developing, global Internet economy. It therefore proposes that various stakeholders – including both public, NGO, and private sector representatives – cooperate to create voluntary industry-specific codes of conduct to protect consumer privacy. Though “voluntary,” the codes would likely require FTC approval and would be enforceable by the FTC and state attorneys general. The Department seeks comment on various issues related to such codes, including whether they should be enforceable pursuant to a private right of action.

The Green Paper further recommends that the Administration consider various options to encourage the development of such codes of conduct. These could include public statements of Administration support, increased FTC enforcement of violations under current law, and/or legislation creating a safe harbor from enforcement for companies that adhere to approved codes of conduct.

The Department believes that it has an important role to play in this regard, as well as, more broadly, in providing the Administration with a renewed focus on commercial data privacy. To that end, it proposes the establishment of a Privacy Policy Office (PPO) within the Department. The PPO would have no enforcement authority (the FTC would continue in that role), but, guided by the FIPPs, it would convene multi-stakeholder meetings to examine new uses of personal information, identify areas for the development of best practices and codes of conduct, and otherwise serve as a center of data privacy policy expertise for the Administration.

C. Encourage global interoperability.

The Green Paper notes that there are an array of different privacy laws around the world, which makes it costly and difficult for U.S. companies to operate and compete globally. The Department believes that, as a leader in the global Internet economy, the U.S. should take the lead in working toward increased cooperation among privacy enforcement authorities around the world. According to the Green Paper, the U.S. should demonstrate to other countries – via Congressional leadership, continued FTC enforcement, and Administration engagement (led by the PPO) – that the U.S. has a strong privacy framework and is committed to strengthening it further.

The Green Paper further provides that the U.S. should work with other governments to find practical ways to overcome differences and promote low-friction, cross-border data flows through increased global interoperability of privacy frameworks. The Department believes that this could be achieved through agreements with other privacy authorities, modeled, for example, on frameworks pioneered by the Organisation for Economic Cooperation and Development and Asia-Pacific Economic Cooperation.

Client Alert.

D. Ensure nationally consistent security breach notification rules.

The Department recommends the consideration of a federal commercial data security breach notification law that sets national standards, addresses how to reconcile inconsistent state laws, and authorizes enforcement by state authorities. In its view, state breach notification laws have been successful in certain regards (such as in reducing identity theft), but the differences among the many state laws impose undue costs on businesses. The Department believes that a single federal law would not only provide consumers with clarity about how their personal information is protected, but it would also give businesses the ability to develop one data-management and breach-response strategy.

The Department raises numerous questions in connection with each of its proposals and requests comments from interested parties. The Department anticipates that its request for comments will spur further discussion among stakeholders and lead to the development of a series of Administration positions that will develop an action plan.

Comments are due to the Department's National Telecommunications and Information Administration by January 28, 2011.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.