WSGR ALERT

JANUARY 2011

DEPARTMENT OF COMMERCE PROPOSES NEW PRIVACY FRAMEWORK, RECOMMENDS CREATION OF NEW PRIVACY POLICY OFFICE

On December 16, 2010, the Department of Commerce's Internet Policy Task Force issued a "green paper" detailing its proposed privacy policy framework, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[1] Released just after the Federal Trade Commission (FTC) issued its report on privacy, the Commerce Department's report presents a framework focused on five major topics: expanding Fair Information Practice Principles; promoting voluntary, enforceable privacy codes of conduct; encouraging global interoperability of privacy regimes; standardizing security breach notification rules; and revising the Electronic Communications Privacy Act. Although the FTC and the Department of Commerce are proposing new frameworks for analyzing consumer privacy issues, the reports differ in scope: the Commerce Department's report addresses online privacy, while the FTC's report applies to privacy in both online and offline contexts. Both agencies are seeking public comment on their proposals.

Fair Information Practice Principles (FIPPs)

The Department of Commerce makes several recommendations regarding FIPPs. First, the department recommends that an expanded set of FIPPs be used to establish a baseline commercial data privacy framework. These FIPPs would essentially be a guiding set of principles that would establish the minimum level of online privacy protection nationwide. Although the department does not lay out a specific set of FIPPs, it does cite favorably principles adopted by the Department of Homeland Security (DHS). The DHS FIPPs include transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.[2] In endorsing this approach, the department notes that the notice-and-choice model employed by many businesses today was the subject of much criticism at a public symposium it held prior to releasing the report. The department does not take a position on whether these FIPPs should be imposed by new legislation, but seeks public comment on this topic.

Second, the Commerce Department recommends that expanded FIPPs should focus on greater transparency, more detailed purpose specifications and use limitations, and auditing. Specifically, the department criticizes current privacy policies as being overly long, too complex, and a generally poor method of conveying privacy information to consumers. In addition to advocating for simpler, clearer notices, the department looks favorably on privacy impact assessments, which require companies to identify and evaluate privacy risks, as a complementary approach to increasing transparency. Additionally, the department suggests using purpose specifications—which require companies to state the reasons they are collecting data—and use limitations—which require companies to use the data collected for only the stated reasons—to better align consumer expectations and actual data practices. Finally, the department argues that companies need to better audit their privacy practices to ensure that they are living up to their stated practices.

Third, the department states that expanded FIPPs should supplement, rather than supplant, existing sectoral privacy regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act should continue to govern privacy protections in their covered industries (healthcare and finance, respectively). In the department's view, FIPPs would fill perceived gaps in the current sectoral approach.

Voluntary, Enforceable Privacy Codes of Conduct

To supplement FIPPs and provide a framework with more practicality and certainty, the Commerce Department advocates for the creation of voluntary, enforceable codes of conduct (CoCs). The department argues that these CoCs should focus on emerging technology issues not adequately covered by baseline FIPPs, and points to the Network Advertising Initiative's CoC for behavioral advertising as an example. To promote the development and adoption of CoCs, the department suggests several possible approaches, including public statements of

[1] The full report is available at http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.
[2] This FIPPs model is very similar to the "Privacy by Design" model endorsed by the FTC in its privacy report.

Continued on page 2...

Department of Commerce Proposes New Privacy Framework . . .

Continued from page 1...

administration support, increased FTC enforcement, and legislation that would provide a safe harbor for companies that comply with approved CoCs. To qualify for safe-harbor status, the department states that these CoCs should undergo an open, multi-stakeholder process and be approved by the FTC.

The Department of Commerce also recommends creating a Privacy Policy Office (PPO) within itself. The purpose of the PPO would be to convene multi-stakeholder discussions of various information privacy issues, including industry CoCs. The PPO would not have any enforcement authority and would focus solely on commercial data privacy practices (as opposed to, for example, government practices). As currently proposed, the PPO would work with the FTC on policy issues, such as Do Not Track.

The department recommends that the FTC remain the lead consumer privacy enforcement agency for the U.S. government, but suggests that there is room for additional or concurrent state enforcement of data privacy practices. Furthermore, the department suggests that any federal data privacy law not completely preempt state laws, but leaves the degree of preemption and the extent of state enforcement open for public comment.

Global Interoperability

The Department of Commerce advises the U.S. government to engage other global privacy enforcement authorities in developing a framework for mutual recognition of commercial data privacy systems. The lack of such a framework, the department argues, is both costly and confusing. Companies that operate across multiple jurisdictions are required to not only pay the cost of compliance in those different areas, but also must anticipate the legal obligations that may arise as they transfer information across international borders.

The Commerce Department believes the best way to address this problem is to create a system of cross-border privacy rules, preferably within the framework already established by the Asia-Pacific Economic Cooperation (APEC) Data Privacy Pathfinder project. As the 2011 APEC host, the department believes that the U.S. is in a unique position to promote acceptance of a self-regulatory system that would clarify the obligations and requirements on businesses seeking to transfer data between businesses stationed in APEC nations. The department also believes that the implementation of a clear and understandable framework will encourage companies to act responsibly, as APEC will create a mechanism for enforcement if they do not.

National Requirements for Security Breach Notification

The Department of Commerce recommends that the U.S establish a comprehensive commercial data security breach notification framework for electronic records. Under the department's vision, this framework would serve as a national baseline; if states wanted to build on that framework, they would be permitted to do so in limited ways. The department suggests that guidance for this new framework be taken from the state systems that currently operate as the primary source of law in this area. Furthermore, the department supports the implementation of a national framework to unify the minimal requirements for data security, as well as the clarification of the requirements each business must satisfy to protect the data in its possession. The department's recommendation, however, only applies to current state security breach notification laws; it makes no recommendation regarding breach notification laws for specific sectors, such as healthcare. The department seeks comment on what factors breach notification should be predicated upon.

Amending the Electronic Communications Privacy Act (ECPA)

The Department of Commerce recommends that Congress reconsider existing legislation, particularly the ECPA, to ensure privacy protection in cloud computing and location-based services. The ECPA was enacted in 1985 to balance personal and proprietary privacy interests against the government's law-enforcement needs. The department suggests that the current state of information technology has outgrown the ECPA, leading to inconsistent interpretations of the law. The department, therefore, seeks to rebalance the ECPA in light of new technologies and interests, with the aim of both protecting consumer expectations of privacy and effectively punishing unlawful access and disclosure. The department seeks comment on the way to most effectively strike this balance.

Implications

The Department of Commerce's proposed framework could influence a number of important online data privacy decisions. Of particular note is the Internet Policy Task Force's proposal to create a new Privacy Policy Office within the Department of Commerce. Also, the department's push for global interoperability could result in significant changes to domestic policies if U.S. policymakers adopt the stricter privacy regulations found abroad. Finally, businesses will want to pay close attention to the potential creation of a nationwide security breach notification statute, as it could either greatly simplify the complex web of state requirements currently in place, or add yet another layer of complexity.

The report also raises and seeks comment on several issues of significance to companies that collect, use, or disclose data about consumers. For example, the Department of Commerce seeks comment as to how FIPPs should be defined and enforced, and whether any potential legislation should include a private right of action for violations. Additionally, the department seeks comment on whether companies should be required to undertake privacy impact assessments, and what the scope of those audits would be. The department seeks public comment on these and other matters on or before January 28, 2011. The complete list of issues for public comment can be found in Appendix A to the report.

Continued on page 3...

Department of Commerce Proposes New Privacy Framework . . .

Continued from page 2...

Wilson Sonsini Goodrich & Rosati's privacy and data security practice includes over 20 attorneys—including Lydia Parnes, the former director of the FTC's Bureau of Consumer Protection—who routinely advise clients on all aspects of risk management associated with the collection, use, and disclosure of information. If you have questions in these areas or on the report itself, please contact Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Tonia Klausner at tklausner@wsgr.com or (212) 497-7706; Sara Harrington at sharrington@wsgr.com or (650) 493-4915; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; or Matt Staples at mstaples@wsgr.com or (206) 883-2583.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on January 5, 2011. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com