LOWENSTEIN SANDLER PC CLIENT ALERT

PRIVACY LAW

ATTORNEY ADVERTISING

WHITE HOUSE PROPOSES A CONSUMER PRIVACY BILL OF RIGHTS: WILL A MULTI-STAKEHOLDER APPROACH TO DEVELOPING ENFORCEABLE CODES OF CONDUCT ALLOW THE U.S. TO PRESERVE INTERNET INNOVATION (AND PERHAPS AVOID FEDERAL REGULATION)?

By Mary J. Hildebrand, Esq., and Katherine A. Varker, Esq.

March 1, 2012

Can the U.S. build consumer trust and global interoperability without creating restrictive regulations that stifle innovation? That is what the Obama administration is attempting to do in the recently released Commerce Department report *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promotional Innovation in the Global Digital Economy (the "Commerce Department Report").* According to a White House press release, the Consumer Privacy Bill of Rights, which was included as part of the report, is designed to "improve online consumer privacy while also ensuring the Internet remains a forum for economic growth."

The Consumer Privacy Bill of Rights

The Consumer Privacy Bill of Rights contains many familiar concepts that are based on the U.S.-developed and globally recognized Fair Information Practice Principles (FIPPs). (See the *Privacy Act of 1974*, Pub. L. No. 93-579 [5 U.S.C. Section 552a] and the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the Asia-Pacific Economic Cooperation's *Privacy Framework*.) The proposed framework is concerned solely with how private sector entities handle personal data in commercial settings. Consequently, the administration is making an effort to maintain flexibility and adaptability so that companies can develop codes of conduct based on these principles that take into account consumer expectations about privacy in particular market segments.

The seven principles of the Consumer Privacy Bill of Rights are:

Individual Control: *Consumers have a right to exercise control over what personal data companies collect from them and how they use it.* "Personal data" is defined as "any data, including aggregations of data, which is linkable to a specific individual." And, for the first time in the U.S., personal data would include online identifiers, such as IP addresses. In addition to disclosing the ways personal data is used in the privacy notice, this principle would require companies to offer "just in time" consent; more choices about personal data collection, use, and disclosure; and ways to withdraw or limit consent. Companies that have a direct relationship with the consumer would be expected to provide more choices.

Transparency: *Consumers have a right to easily understandable and accessible information about privacy and security practices.* Not only should privacy notices be in plain language, but they should be presented when they are relevant—not just relegated to the main privacy notice. If the use of personal data is not something that the consumer has come to expect from the relationship with the company, then notice of such use should be more prominently displayed. Companies may also be expected to disclose what kinds of personal data they obtains from third parties, identify the third parties, and describe how they use this data.

Respect for Context: *Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.* If companies will use or disclose personal data for

Lowenstein Sandler
ATTORNEYS AT LAW

other purposes, they should provide heightened Transparency and Individual Control. If a company "reuses" the personal data for some other purpose, even more Transparency and Individual Control are necessary. This principle also takes into consideration the age and sophistication of the consumers who engage with the company (e.g., children and teenagers vs. adults).

Security: *Consumers have a right to secure and responsible handling of personal data.* The level of security required may depend on the scale, scope and sensitivity of the personal data that the company maintains.

Access and Accuracy: *Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.* This is for market sectors that are not already covered by existing federal privacy laws such as HIPAA and the Fair Credit Reporting Act.

Focused Collection: *Consumers have a right to reasonable limits on the personal data that companies collect and retain.* Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle and should securely dispose of the personal data once they no longer have a need for it.

Accountability: *Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.* This principle includes company accountability to enforcement authorities as well as employee accountability to the company. Chief Privacy Officers appointed by the company have a potentially important role to play in teaching employees how to handle personal data in a manner that is consistent with privacy principles. Further, if the company transfers personal data to a third party, the company remains accountable for compliance, so each company must ensure that such recipients are under enforceable contractual obligations to adhere to these principles.

The Framework for Developing Enforceable Consumer Data Privacy Rights

The Consumer Privacy Bill of Rights establishes a guideline for how Internet companies should handle personal data but is not legally enforceable. The administration's framework for developing enforceable consumer data privacy rights in the U.S. is based on the following key elements:

1. Establishing a **Consumer Privacy Bill of Rights**
2. Developing **Enforceable Codes of Conduct** through a multi-stakeholder process
3. **FTC enforcement** of consumers' data privacy rights through its authority to prohibit unfair or deceptive trade practices
4. Increasing **global interoperability** between U.S. consumer data privacy rights and other countries' frameworks in order to reduce barriers to the flow of information

The Multi-Stakeholder Approach to Develop Enforceable Codes of Conduct

The administration has asked the Department of Commerce to work with stakeholders (such as companies, trade groups, academics, civil and criminal law enforcement representatives, and foreign government officials) to create and implement enforceable codes of conduct based on the Consumer Privacy Bill of Rights. The administration is also calling on Congress to give the Federal Trade Commission (FTC) and state attorneys general specific authority to enforce the codes of conduct.

Companies may benefit from having consistent rules that they can count on, rather than worrying that they may be the subject of an FTC action. John Kerry suggested that "instead of continuing the now monthly exercise of publicly scolding companies, we need to make Congress establish common sense rules of the road that protect consumers." And the administration is clearly weary of Europe saying that U.S. data privacy rights are not "adequate." If the U.S. is successful in establishing a process that "works efficiently … on a global scale," then it would reduce barriers to the international flow of information. (See Commerce Department Report, page 23.)

But does the very nature of the Internet defy legislation? The administration acknowledges that "due in part to its reliance on multi-stakeholder processes, the United States Internet policy has generally avoided fragmented, prescriptive and unpredictable rules that frustrate innovation and undermine consumer trust." (See Commerce Department Report, page 24.) Rep. Mary Bono Mack (R-Calif.), chairman of the Energy and Commerce Subcommittee on Manufacturing and Trade, warned against enacting tough privacy regulations as was done in Europe. "Protecting consumer privacy online and preserving American innovation are not mutually exclusive," she said, adding, "any rush to judgment could have a chilling effect on our economy and

potentially damage, if not cripple, online innovation." She plans to hold a hearing in March 2012 on the White House's Consumer Privacy Bill of Rights and wants to hear from all stakeholders before enacting legislation.

Consumer Watchdog's John Simpson says he is skeptical of the multi-stakeholder process but is "willing to make a 'good faith' effort to try." And that is what the administration seems to be encouraging—if the multi-stakeholder process yields the practices and technology necessary to implement legally enforceable codes of conduct for each market segment based on the Consumer Privacy Bill of Rights, then there would be no federal regulation at the end of the process. The codes of conduct would not bind companies unless they chose to adopt them. But there would be strong incentives to do so—beyond building consumer trust—in any enforcement action based on conduct covered by a code, the FTC would consider a company's adherence to a code favorably. (See Commerce Department Report, page 24.)

All companies that handle personal data are considered stakeholders in this process, with the opportunity to influence the outcome of the administration's efforts to establish enforceable consumer privacy rights in the U.S. Each market segment is different, and by participating in the dialogue over the coming months, you may be in a position to help tailor the codes of conduct to be least restrictive to your business.

Please contact either of the attorneys below with questions related to this alert or for more information about Lowenstein Sandler's Privacy Law Group:

Mary J. Hildebrand
Chair, Privacy Practice Group
973 597 6308
mhildebrand@lowenstein.com

Katherine A. Varker
Counsel
973 422 6430
kvarker@lowenstein.com

Lowenstein Sandler
ATTORNEYS AT LAW