WSGR ALERT

FEBRUARY 2012

WHITE HOUSE PROPOSES CONSUMER PRIVACY BILL OF RIGHTS, SEEKS ADOPTION OF PRIVATE CODES OF CONDUCT, AND PUSHES FEDERAL PRIVACY LEGISLATION

Signaling the United States' commitment to global privacy leadership, the White House has released its long-awaited report on consumer privacy. The report outlines a comprehensive and systematic framework for approaching consumer privacy in a networked world.[1] The framework outlines a four-tiered approach designed to redefine and strengthen privacy in the United States. It contains four key parts: (1) a proposed Consumer Privacy Bill of Rights; (2) a "multistakeholder process" by which government, industry, advocates, academics, and others will develop enforceable codes of conduct to implement that Bill of Rights; (3) legislative action to give the Federal Trade Commission (FTC) a statutory basis to enforce the Bill of Rights; and (4) increased cooperation and coordination with foreign countries on privacy issues.

Consumer Privacy Bill of Rights

The centerpiece of the framework is the proposed Consumer Privacy Bill of Rights, which establishes baseline consumer privacy protections and applies to commercial uses of personal data.[2]

The proposed Consumer Bill of Rights describes seven specific consumer data privacy rights that private entities are encouraged to adopt and honor:

Individual Control. Companies should give consumers control over how their personal data is collected, used, and disclosed. Such control should be easy to use; accessible; reflect the scale, scope, and sensitivity of the data; and provide clear and simple choices presented at times and in ways that allow consumers to make meaningful decisions about the collection, use, and disclosure of their personal data. Companies also should offer consumers the means to withdraw or limit consent that are as accessible and easy to use as the methods for granting consent in the first place.

Transparency. Companies should provide "clear descriptions" of the personal data they collect, their reasons for collecting that data, the ways in which the data will be used, how long it will be retained, and the circumstances under which companies could share it with third parties.

Respect for Context. The collection, use, and disclosure of personal data should be consistent with (1) the relationship the company has with the consumer and (2) the original context in which the data was provided by the consumer. If companies use or disclose personal data for purposes that are inconsistent with this context, they should disclose such changes and give consumers certain choices about those uses.

Security. Companies must assess the privacy and security risks associated with their personal data practices and maintain "reasonable safeguards" to control the risks of data compromise.

Access and Accuracy. Companies should use reasonable measures to ensure that they maintain accurate personal data. They also should provide consumers with reasonable access to personal data and the means to correct inaccurate personal data or request its deletion or use limitation.

Focused Collection. Companies only should collect personal data they need to accomplish purposes specified under the "Respect for Context" principle. Also, unless they are under a legal obligation to retain data, companies should securely dispose of or de-identify personal data once they no longer need it.

Accountability. Companies should be accountable to enforcement authorities and consumers for respecting these rights, and they should hold employees responsible for the same through proper training and internal policies. Companies also should conduct full privacy audits where

[1] The proposal, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, is available at http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf.

[2] "Personal data" is defined broadly in the framework as "any data, including aggregations of data, which is linkable to a specific individual," including "data that is linked to a specific computer or other device."

Continued on page 2...

White House Proposes Consumer Privacy Bill of Rights . . .

Continued from page 1...

appropriate. Companies that disclose personal data to third parties should, at minimum, ensure that recipients are under enforceable contractual obligations to adhere to the Bill of Rights' principles unless they are required by law to do otherwise.

Multistakeholder Approach

The second key aspect of the Obama administration's approach is the development of sector-specific voluntary codes to implement the general principles of its Consumer Privacy Bill of Rights. The administration proposes involving "individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups" in a process of developing voluntary codes of conduct that would implement the Consumer Privacy Bill of Rights.

The possible adoption of voluntary codes could have a significant impact on information-centric companies. Such companies should play an early and active role in the code-development process.

Legislative Action

The administration also is proposing that it work with Congress to pass legislation codifying the Consumer Privacy Bill of Rights, arguing that a national, uniform privacy framework provides greater consistency to consumers and companies alike. Notably, the administration's proposal calls for the legislation to create a national standard under which companies must notify consumers of unauthorized disclosures of certain kinds of personal data. This would replace the various—and sometimes inconsistent—security breach notification laws existing today in 47 states, the District of Columbia, and several U.S. territories.

International Cooperation

Finally, the administration expressed the United States' commitment to continued collaboration on the international level, with the goal of increasing the interoperability of global privacy laws. The administration believes that such efforts will provide more consistent protections for consumers and lower compliance burdens for companies.

Implications

The administration's privacy framework is highly relevant to technology and growth companies. First, it presents the most current blueprint of the administration's thinking about how industry should approach consumer privacy issues and, as such, provides guidance on best practices.

Second, it provides a playbook on the administration's approach to helping information-centric U.S. businesses maintain access to international markets. It also provides an alternative, collaborative approach to the international arena, addressing proposals that some in the business community have perceived to be overreaching and increasingly threatening to technology innovation.

Conclusion

The administration has launched the opening salvo in what is likely to be a lengthy process of negotiation between it, the private sector, and Capitol Hill. The policy picture is likely to grow even more complex with the final version of the FTC's staff report on consumer privacy,[3] which is expected to be released imminently.

Companies should start considering options for engaging in the multistakeholder process envisioned by the administration. Companies also should prepare to adapt to the compliance procedures that may be necessary if new standards emerge, including the possibility of new federal legislation.

Wilson Sonsini Goodrich & Rosati's attorneys regularly assist clients with all aspects of their privacy and information governance needs, including the development of and compliance with self-regulatory programs and other private codes of conduct. For additional information regarding the Consumer Privacy Bill of Rights, participation in the development of voluntary codes of conduct to implement its principles, or any other questions, please contact Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Donald Vieira at dvieira@wsgr.com or (202) 973-8857; Matthew Staples at mstaples@wsgr.com or (206) 883-2583; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; or Brock Dahl at bdahl@wsgr.com or (650) 849-3363.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on February 28, 2012. 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

[3] The WSGR Alert discussing the FTC's preliminary staff report, *Protecting Consumer Privacy in an Era of Rapid Change*, is available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert_do_not_track_mechanism.htm.