SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

Skadden

PRIVACY UPDATE

An Overview of Legislative, Regulatory and Technology Developments in the Privacy Sector

3.7.12

INSIDE

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi**, 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

Four Times Square, New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

White House Releases Framework for Data Privacy

On February 23, 2012, the White House released its much-anticipated report on data privacy. The report, entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*[1] is a nonbinding framework for the use and handling of personal data by private-sector entities in commercial settings (Framework). The overall theme of the Framework echoes one that was included in the Department of Commerce and FTC privacy reports that were issued in 2011; namely, that protecting data privacy and providing greater certainty in this area is essential to help grow the online sector.

The Framework includes a proposed "Consumer Privacy Bill of Rights" intended to act as a "legal baseline" governing consumer data privacy in the United States. The Obama administration plans to encourage stakeholders to implement the Consumer Privacy Bill of Rights through codes of conduct and to work with Congress to have these rights enacted through data privacy legislation. However, tacitly acknowledging that it has been difficult to get data privacy legislation enacted, the administration notes that even if legislation is not enacted, companies should abide by these principles to increase consumer trust and thereby promote innovation. The Framework also calls for "international interoperability" to harmonize data protection regimes and subtly calls on the EU to accept the U.S. approach to data privacy.

I. Consumer Privacy Bill of Rights

The White House's proposed Framework sets forth seven core principles of consumer privacy, many of which form the basis of privacy laws in other countries. Although the administration couches these principles as "rights," they have no legal effect unless and until Congress encompasses them into data privacy legislation. Significantly, these principles are broad in nature, and the administration has stressed that it did not want to adopt a single set of "rigid requirements" and instead wanted companies to have the flexibility to determine how to best comply given their individual circumstances.

These rights relate to the use and handling of "personal data," which is defined as "any data, including aggregations of data, which is linkable to a specific individual." Significantly, "personal data" also includes data that is linked to a specific device. This is consistent with the growing trend that personal information can be deciphered merely by tracking activity taking place on a device (*e.g.*, a smartphone) — even if the name of the user remains unknown.

a. **Individual Control: Consumers have a right to exercise control over what personal data organizations collect from them and how they use it.** At the time of collection, companies should present consumers with choices about the collection, use and disclosure of their personal data that is commensurate with the scope and

1 Available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

nature of the personal data in question. The broader and more detailed the data collection and the longer it is retained, the more granular and customized the consumer options should be.

b. **Transparency:** **Consumers have a right to easily understandable information about privacy and security practices.** Companies should clearly describe (1) what personal data they collect, (2) how they will use it, (3) how long they will retain it before deleting or anonymizing it, and (4) whether and for what purposes they will share personal data with third parties.

c. **Respect for Context:** **Consumers have a right to expect that organizations will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data**. If a company uses or discloses personal data in a manner inconsistent with the context in which the company and consumer interact, then the company should provide greater transparency and individual choice at the time of data collection. This right does not foreclose a company's ability to use personal data previously collected in new and innovative ways, so long as the new use is the subject of appropriate — and perhaps higher — measures of transparency and individual choice. In addition, companies may infer consent to collect and use personal data to achieve objectives specifically requested by consumers to conduct standard direct marketing (where consumers can opt out at any time).

d. **Security:** **Consumers have a right to secure and responsible handling of personal data**.

e. **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 are inaccurate**.

f. **Focused Collection:** **Consumers have a right to reasonable limits on the personal data that companies collect and retain.** Companies should therefore tailor their collection of personal data for specific purposes.

g. **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.** A company that handles personal information should, at minimum, train and monitor its employees to ensure that they adhere to the Consumer Privacy Bill of Rights. In some instances, this may require full audits of a company's privacy practices.

II. Legislative Approach

The Framework urges Congress to enact comprehensive privacy legislation by adopting the Consumer Privacy Bill of Rights and granting the FTC the authority to directly enforce such legislation. Interestingly, although federal legislation appears to be the administration's preferred approach for adopting the Consumer Privacy Bill of Rights, it is included last in the Framework, after the code of conduct approach discussed below. This placement may be an acknowledgement by the administration that enacting federal data privacy legislation may be challenging at best.

The Framework notes that Congress cannot simply convert the Consumer Privacy Bill of Rights into legislation. Rather, greater specificity would be required as to how companies must comply with it. In addition, the Framework suggests that Congress enact privacy legislation with the following effects:

a. Preempt state privacy laws to the extent that they are inconsistent with the Consumer Privacy Bill of Rights as enacted and applied;

b. Avoid modification of existing sector-specific federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, which effectively protect personal data by imposing legal obligations that are tailored to the types of personal data used and the standard practices in those industries; and

c. Unify the various security breach notification laws, which require companies to notify consumers in the event of unauthorized disclosure of certain categories of their personal data, by creating a national standard to replace the various local laws currently in effect and preempt any future state legislation.

III. Multistakeholder Processes to Develop Enforceable Codes of Conduct

The Framework acknowledges that implementing the Consumer Privacy Bill of Rights across a wide array of industries requires more specific practices. Therefore, if federal legislation is not enacted, the Framework proposes a transparent, nongovernmental process amongst companies, industry groups, privacy advocates, state attorneys general and others to develop industry-specific codes of conduct that implement the Consumer Privacy Bill of Rights. These codes of conduct would be updated periodically in response to changes in technology, consumer expectations and market conditions to ensure the continued protection of consumer privacy. The Department of Commerce's National Telecommunications and Information Administration would mediate this process.

Once a code of conduct is adopted and approved by the FTC, a company that chose to adopt the code would be in a safe harbor against FTC or state enforcement action. If a company failed to adhere to the code after it said it would adopt it, that company could be subject to an FTC enforcement action through the FTC's authority to prohibit unfair or deceptive acts or practices. The Framework encourages Congress to grant the FTC the authority to review and approve codes of conduct and grant safe harbor status to companies that comply.

IV. International Interoperability

The Framework also includes a section on "international interoperability," which encourages cooperation and coordination among different countries to create a uniform data privacy approach, and to allow personal data to seamlessly cross international borders. There are two interesting and subtle points in this section. First, the Framework mentions the proliferation of cloud computing and the need to protect data that may be sent anywhere in the world. In recent months, a number of foreign-based cloud computing providers have questioned whether it is "safe" to store data in a U.S.-based cloud, given that the Patriot Act might provide the U.S. government access to foreign data stored in a U.S. cloud. The administration's statement that cloud computing issues need to be addressed is perhaps an acknowledgment that the scope of the Patriot Act and other legislation needs to be better defined so that it does not forestall the growth of the U.S. cloud computing industry.

Second, to date, the EU has held that the U.S. does not provide an "adequate" level of data protection, since there is no comprehensive federal data privacy legislation. As a result, companies looking to transfer data from the EU to the U.S. must rely on the so-called "model contract clauses" offered by the EU certify to the U.S.-EU Safe Harbor or take one of the other permitted approaches. The section of the Framework dealing with International Interoperability seems to suggest that the EU reconsider its position if the U.S. adopts the code of conduct approach to the Consumer Privacy Bill of Rights, even if no omnibus federal legislation is enacted.

Practice Points

Although the Framework has no binding legal effect, it provides useful guidance on the areas on which companies should focus when establishing their privacy policies. For example, the Framework envisages companies seeking out innovative ways to recognize consumer choices through mechanisms that are simple, persistent and scalable.

Under the Consumer Privacy Bill of Rights, consumer-facing companies would not be able to abdicate their responsibility to consumers by outsourcing the collection and processing of data to third parties. Engaging a third party to perform such tasks is permitted but requires certain disclosures, namely:

i. the purposes for which the company provides the data to the third party;

ii. the nature of the third party's activities; and

iii. whether the third party is bound to limit its use of the data to achieve those purposes.

Companies that do not deal directly with consumers but which deal in personal data — *e.g.*, data brokers — also are an intended target of the Consumer Privacy Bill of Rights. These third-party handlers of personal data are nonetheless expected to seek innovative methods to provide consumers with effective control and the ability to access and correct their personal data. In addition, to satisfy their transparency obligations, third-party companies are expected to provide explicit explanations of how they acquire, use and disclose personal data.

Companies that take a "wait and see" stance toward privacy — choosing to act only after being required to do so by Congress — may find themselves at a competitive disadvantage compared to other companies that have adopted a proactive approach to data privacy. In addition, privacy practices may become an important point of distinction as competitors seek to promote their products and services over that of their competitors. Companies and other stakeholders interested in shaping the regulations and legal contours of consumer privacy in their industry also should consider participating in the multi-stakeholder processes that the administration is considering.

California Attorney General Reaches Agreement With Mobile Platform Providers

Since 2004, any operator of a commercial website or online service that collected information about California residents was required to conspicuously post its privacy policy. This state law, the California Online Privacy Protection Act (the California Privacy Act), effectively operated as a national requirement to include such a privacy policy since most sites that collect data also collect data from California residents. Last month, California took another important step in the national privacy debate when the California Attorney General, Kamala Harris, entered into a "Joint Statement of Principles" with the leading mobile platform operators. Although not legally binding, under the joint statement, these operators (Amazon, Apple, Google, Hewlett Packard, Microsoft, and Research in Motion) agreed to privacy principles designed to ensure that the "app industry" conspicuously post privacy policies with their apps where legally required to do so. It should be noted that, under the California Privacy Act, almost all apps developers would be required to do so; but few, in practice, comply with this requirement.

Under the joint statement, the platform operators agreed that in the application submission process for a new or updated app, they will prompt app developers to provide the text of, or a link to, their policies. Once this text or link is provided, the mobile operators will make it accessible from the app store. Users also will be presented with the opportunity to report apps that don't comply with their stated policies, and the platforms will develop a mechanism for responding to these reports.

Through the joint statement, Harris has addressed the fact that many mobile apps lack privacy policies by targeting the platforms through which these apps are distributed to the public. The Joint Statement also represents an interesting use of an industry code of conduct to help drive compliance with an existing piece of legislation.