COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Global Privacy & Data Security

February 27, 2012

WHITE HOUSE UNVEILS COMPREHENSIVE PRIVACY PROTECTION FRAMEWORK

On February 23, the White House released its long-awaited comprehensive privacy framework in a report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." The White House framework builds upon the recommendations in the Department of Commerce Internet Policy Task Force's December 2010 report and upon more than 100 stakeholder comments in response to that report.

The framework presents a baseline for consumer privacy protections in the United States in a "Consumer Bill of Rights" that is to be implemented through voluntary industry codes of conduct, mutual recognition and enforcement by international partners, and federal legislation. Participation is currently voluntary, but the White House will push for federal legislation that makes compliance with the Consumer Bill of Rights mandatory. In the meantime, the White House will look to the FTC to incentivize participation in voluntary codes of conduct by looking upon compliant companies favorably in enforcement actions.

The principles embodied in the Consumer Bill of Rights—the White House calls it a "blueprint" for privacy protection—are intended to be flexible and technology-neutral to assure continued innovation. At the same time, the principles are intended to give consumers clear guidance on what they can expect from companies that handle their data.

The White House has a multipronged plan for putting the principles in action. The Commerce Department's National Telecommunications and Information Administration (NTIA) will soon convene stakeholder discussions to develop codes of conduct that comply with the Consumer Bill of Rights. The White House will also work with Congress to enact legislation based on the Consumer Bill of Rights and with global partners to ensure the interoperability of the framework. The White House will rely on the FTC to enforce both the industry codes of conduct and federal privacy law under its proposed legislative scheme.

CONSUMER BILL OF RIGHTS

The Consumer Bill of Rights is the foundation upon which the White House's privacy framework is based. It outlines, in broad strokes, seven principles that companies must embrace in collecting and using personal data. Personal data is defined broadly as "any data, including aggregations of data, which is linkable to a specific individual."

The idea that privacy protections must be dynamic and scalable, rather than static and defined, is a theme that appears throughout the report. Companies are afforded discretion in implementing the principles in a manner that makes sense for the context. Accordingly, many of the principles call for an incremental approach to privacy protection that takes into account the specific circumstances of the company, the consumers, the relationship, and the types of data involved.

Individual Control

- Control required in each situation depends on the type of data collected and the intended uses.
- Ordinary or expected uses—such as analyzing data to improve performance—may require little to no control.
- Consumer-facing companies must provide adequate control over information shared with third parties.
- Must provide a means to limit or withdraw consent commensurate with the means of obtaining consent.

Individual Control requires that companies give consumers choices that are appropriate given the nature of the personal data and the intended uses.

Uses that are ordinary, expected, and present no risk of harm may call for minimum consumer controls—such as when a company uses personal data to analyze how customers use its services.

Consumer-facing companies are expected to give appropriate choices about their own collection and use as well as the uses of the third parties they share data with.

Non-consumer-facing companies may need to compensate where it is not possible to provide meaningful Individual Control with heightened Transparency.

Individual Control requires that companies provide consumers with a means to limit or withdraw consent in a manner that is as accessible to the consumer as the mechanism used to obtain consent.

Transparency

- Practices should be disclosed in plain language statements.
- Unexpected uses call for more visible and explicit disclosures.
- Disclosures should be device-appropriate.
- Data brokers and other third parties must provide heightened disclosures.

Consumers have a right to clear and accessible information about privacy and security practices.

Personal data uses that are inconsistent with the context of the company-consumer relationship require more prominent disclosures than commonly accepted uses.

The disclosures must be provided in a form that is easy to read on the devices that customers use to access a company's services.

Non-consumer-facing companies like data brokers must compensate for the lack of a direct relationship with particularly explicit explanations of how they acquire, use, and disclose personal data.

Respect for Context

- Uses should be limited to fulfilling purposes consistent with the context in which the data was collected.
- Inconsistent uses require heightened Transparency

Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context.

Companies may infer consent to use personal data to achieve objectives that consumers have specifically requested or to use personal data in common ways—for example, to fulfill orders or to combat fraud.

Reusing personal data in a manner inconsistent with the

and Individual Control.
- Context should inform which uses are most prominently disclosed to consumers.
- Protections required in a given context depends on the age and sophistication of consumers.

circumstances of the collection requires heightened measures of Transparency and Individual Control that may be more stringent than was necessary at the time of collection.

Companies should look to context to determine which personal data uses are likely to raise the greatest consumer privacy concerns, which would affect the uses that are most prominently disclosed in privacy notices.

Protections that are necessary in a particular context depends on the sophistication of a company's consumers, taking into account the age of the consumers.

Security

- Security control measures must be adopted based on the sensitivity of data collected and the risk of harm.

Consumers have a right to secure and responsible handling of personal data.

Appropriate security control measures depend on a company's line of business, the kinds of personal data it collects, the likelihood of harm to consumers, and other factors.

Access and Accuracy

- Companies are encouraged to share data they collect in usable form to promote innovation and transparency.
- Opportunities to access and correct data must be afforded where there is a nontrivial risk of harm from inaccurate data.

Consumers have a right to access and correct personal data in a manner that is appropriate to the sensitivity of the data and the risk of harm from inaccuracy.

To advance the goals of innovation, transparency, participation, and collaboration, companies are encouraged to provide personal data in useful formats to properly authenticated individuals.

Because the use of inaccurate personal data may lead to harm, companies should provide consumers with access and correction facilities where appropriate based on the risk and nature of the harm.

Focused Collection

- Scope of data collection and retention time must be limited in light of a company's stated objectives.

Consumers have a right to reasonable limits on the personal data that companies collect and retain.

Companies should engage in considered decisions about the type of data they need to collect to accomplish their stated objectives.

Data should be securely disposed of or de-identified when no longer needed.

Wide-ranging data collection may be appropriate for familiar and socially beneficial Internet services and applications, such as search engines.

Accountability

- Employees should be trained and regularly evaluated in responsible data handling.
- Companies should conduct periodic audits or self-evaluations of privacy practices.
- Companies disclosing data to third parties remain accountable for the data.

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.

Companies should train employees to handle personal data consistently with the principles and should regularly evaluate employee performance in this area.

Companies should conduct regularly audits or self-evaluations of their own practices.

Companies that disclose data to third parties remain accountable for the data must ensure that the recipients are under enforceable contractual obligations to adhere to the principles.

IMPLEMENTATION

Under the White House's proposal, the Consumer Bill of Rights would be put into action on a number of levels. Stakeholders would develop codes of conduct that companies will be encouraged to adopt. International organizations would work together to ensure interoperability of the principles. Congress would adopt federal legislation that codifies the White House's proposed consumer privacy rights.

Developing Enforceable Codes of Conduct

The White House encourages a multistakeholder approach to developing industry-wide enforceable codes of conduct that comply with the Consumer Bill of Rights. Individual companies, industry groups, privacy advocates, consumer groups, State Attorneys General, and federal civil and criminal law enforcement representatives would collaborate to produce privacy solutions.

The federal government, through the Department of Commerce's NTIA, will work with participants to establish operating procedures that ensure an open, transparent process. The White House identifies two incentives for company participation. First, adopting a code of conduct will foster consumer trust. Second, in any enforcement action based on conduct covered by the code, the FTC will consider a company's compliance with the code favorably.

Once a code is adopted, a company's public commitment to adhere to a code of conduct will become enforceable under Section 5 of the FTC Act. In other words, acting at variance to the code of conduct in a material way would be considered an unfair or deceptive trade practice actionable under Section 5.

Promoting International Interoperability

Interoperability is a priority for the White House in implementing the Consumer Bill of Rights, because it recognizes that complying with varying privacy laws imposes heavy burdens on companies that transfer data across jurisdictions. Interoperability would be achieved by developing codes of conduct that include mutual recognition of privacy principles and enforcement cooperation.

Mutual recognition requires jurisdictions to embrace common privacy and security principles. Enforcement cooperation reinforces interoperability by fostering the development of privacy enforcement priorities, the sharing of best practices, and support for joint enforcement initiatives.

Federal Consumer Data Privacy Legislation

The White House calls on Congress to pass federal consumer data privacy legislation that is a more detailed version of the Consumer Privacy Bill of Rights. The legislation would not replace existing industry- or population-specific privacy legislation, such as HIPAA and COPPA. Under the White House's proposal, the FTC and state attorneys general would directly enforce consumer rights under the statute. (Needless to say, the outlook for passing legislation in the current election year is unlikely, but the White House is taking a long view on this issue.)

The White House also proposes legislation that authorizes the FTC to review industry-specific codes of conduct and grant companies that adhere to approved codes of conduct a safe harbor from enforcement under the legislation's provisions.

The proposed legislation would preempt inconsistent state laws, to avoid inconsistent requirements and to incentivize companies to adopt FTC-approved codes of conduct.

The proposed legislation would also establish a national security breach notification standard, in response to the burdens on companies from complying with the 47 individual state security breach notification laws.

* * *

Industry reaction to the White House's framework has been measured. Although industry members—such as the Software and Information Industry Association—welcome the opportunity to participate in developing voluntary codes of conduct, companies have voiced less support for federal legislation that makes compliance with the Consumer Bill of Rights mandatory.

If you have any questions regarding the White House framework or its impact on your business, please contact the following members of our Global Privacy & Data Security Practice Group:

Kurt Wimmer	202.662.5278	kwimmer@cov.com
Yaron Dori	202.662.5444	ydori@cov.com
Rob Sherman	202.662.5115	rsherman@cov.com
Lindsey Tonsager	202.662.5609	ltonsager@cov.com
Libbie Canter	202.662.5228	ecanter@cov.com
Josephine Liu	202.662.5654	jliu@cov.com
Stephen Satterfield	202.662.5659	ssatterfield@cov.com
Laura Brookover	202.662.5283	lbrookover@cov.com