wiley

NEWSLETTER

White House Announces Consumer Bill of Rights While Internet Companies Agree to "Do-Not-Track"

March 2012

Culminating a year-long process, the Obama Administration, on February 23, 2012, released a comprehensive plan designed to promote trust in the digital economy and extend baseline privacy protections to commercial sectors in the networked world that existing federal privacy laws do not cover. Most notably, the report—*"Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy"* (Report)—announces the Executive branch's intent to encourage private businesses to implement voluntarily, and for Congress to pass legislation enacting a "Consumer Privacy Bill of Rights."

The Administration's framework for consumer privacy in the networked world consists of four elements:

- The Consumer Privacy Bill of Rights, which would define seven rights for consumers utilizing the Internet;
- Enforceable codes of conduct developed through multi-stakeholder processes convened by the Department of Commerce;
- Enforcement by the Federal Trade Commission (FTC) through its jurisdiction over deceptive and unfair trade practices; and
- Increasing global interoperability between the U.S. framework and other countries' frameworks.

Authors

Henry Gola
Partner
202.719.7561
hgola@wiley.law

The Seven Privacy Principles

At the heart of the Administration's approach is what it calls the "Consumer Privacy Bill of Rights." This concept is comprised of seven privacy principles, which in turn build upon widely recognized fair information practice principles that originated in the United States some 40 years ago. These principles are:

- Individual control: To enable consumers to control commercial use of their personal data, companies should present simple and prominent choices for personal data use and disclosure. In addition, consumers should have a right to control how companies collect and use personal data, and what personal data companies share with others.
- Transparency: Companies should present consumers with easily understandable and accessible information about the relevant privacy and security risks.
- Respect for Context: Companies should use and disclose personal data only in ways that a consumer would expect based on the context in which the consumer provides the data. The idea that the context of consumers' interaction with a business should shape their reasonable expectations about privacy is a central element of the Administration's approach.
- Security: Companies should assess and maintain reasonable privacy and security safeguards to control unauthorized access or other harm to personal data.
- Access and Accuracy: Companies should allow consumers reasonable access to the personal data collected and provide methods to correct inaccurate data and allow requests that data be deleted. In addition, companies should ensure the reasonable accuracy of the personal data they keep.
- Focused Collection: In conjunction with the "Respect for Context" consumer right, the Administration recommends that companies should collect only the personal data needed for the specified purpose. And absent an independent legal obligations to retain the data, companies should also securely dispose of personal data when no longer needed.
- Accountability: Companies and their employees should be accountable to enforcement authorities and consumers, conduct full audits of their privacy policies, and ensure that disclosure of data to third parties is subject to contractual provisions adhering to the Consumer Privacy Bill of Rights.

Expected Next Steps

Even without legislation, the Department of Commerce will begin to meet with Internet companies and consumer advocates to develop voluntary, but enforceable, codes of conduct based on the Consumer Privacy Bill of Rights. In time, we may see different codes for different industries. Once a code of conduct is complete, companies may choose to adopt it. If a company does adopt a code, its commitment would be enforceable under § 5 of the FTC Act, because the company's representation would become subject to the FTC's jurisdiction over deceptive or misleading trade practices.

Because the United States does not have a general consumer privacy law, the White House also called upon Congress to enact the Consumer Bill of Rights into law. Federal consumer privacy legislation would apply more broadly and establish more consistent privacy protections across the economy, as well as ensure that

the principles apply to all companies. The Administration recommends that such a federal law not modify federal sector-specific privacy statutes now in effect—such as those affecting healthcare, education, communications, financial services and online data collection from children—unless those statutes set inconsistent standards. However, the Administration recommends that federal legislation preempt state laws that set lesser privacy standards.

To address international data flows, the Report aims to pursue mutual recognition of privacy laws with other countries, develop international codes of conduct through a multi-stakeholder process and foster international enforcement cooperation. This approach, which builds on the U.S. regulatory approach to consumer privacy and efforts in other international forums, can be viewed as the U.S. response to the proposed European Union privacy regulation. Look for many continued discussions on this topic.

"Do-Not-Track" Undertakings

In conjunction with the White House release of the Report, leading Internet companies and online advertising networks—including Google, Yahoo! Microsoft, AOL and the Digital Advertising Alliance—announced their commitment to embed effective "Do-Not-Track" buttons in web browsers within nine months. This technology would enable consumers to choose not to be tracked across websites for profiling or behavioral advertising purposes.

The agreement will still allow consumer web browsing behavior to be used for commercial "market research" and "product development" as well as law enforcement but prohibits its use for employment, credit, healthcare or insurance purposes. As in the case of the codes of conduct, the agreement will be subject to FTC enforcement.

Importantly, the relationship between this commitment and the efforts of a W3C working group to define a workable Do-Not-Track signal for browsers illustrates that the eventual result remains unclear. For example, the Digital Advertising Alliance, while supporting a Do-Not-Track header, issued a statement later the same day indicating that it was unlikely to change its position on certain details, signaling that difficult implementation issues remain to be hurdled.