wiley

ALERT

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

February 24, 2012

On February 23, 2012, the Obama Administration released "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (Privacy Report or Report), a comprehensive plan designed to promote trust in the digital economy and extend baseline privacy protections to commercial sectors that existing federal privacy laws do not cover.

Most notably, the Report calls for Congress to pass a "Consumer Privacy Bill of Rights," which would define seven rights for consumers utilizing the Internet: (1) individual control, (2) transparency, (3) respect for context, (4) security, (5) access and accuracy, (6) focused collection and (7) accountability. Even without legislation, the Report proposes for the National Telecommunications and Information Administration (NTIA) to meet with Internet companies and consumer advocates to develop voluntary, but enforceable, codes of conduct based on the Consumer Privacy Bill of Rights. The Federal Trade Commission (FTC) would handle enforcement through its authority to prohibit unfair or deceptive acts or practices. The Report also proposes to increase global interoperability between the privacy framework developed in the United States and other countries.

Consumer Privacy Bill of Rights

The Consumer Privacy Bill of Rights aims to give consumers more control over the commercial uses of their personal data, which the Privacy Report defines as data "linkable to a specific individual" (including identifiers on smartphones) through the following seven

Authors

Henry Gola
Partner
202.719.7561
hgola@wiley.law

Practice Areas

Media
Privacy, Cyber & Data Governance
Telecom, Media & Technology

rights:

1. **Individual Control:** To enable consumer control over commercial use of their personal data, companies should present simple and prominent choices for personal data use and disclosure. In addition, consumers would have a right to control how companies collect and use personal data, and what personal data companies share with others. The Administration encourages consumer-facing companies to "act as stewards of personal data that they and their business partners collect from consumers."

2. **Transparency:** Companies should present consumers with easily understandable and accessible information about the relevant privacy and security risks.

3. **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 data were provided. This idea that a consumer's expectations about privacy are guided by the nature of their interaction with a business is a central element of the Administration's approach.

4. **Security:** Companies should assess and maintain reasonable privacy and security safeguards to control unauthorized access or other harm to personal data.

5. **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.

6. **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 unless under independent legal obligations to retain the data, companies should also securely dispose of personal data when no longer needed.

7. **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.

The Privacy Report calls upon the NTIA to convene open stakeholder meetings to define an appropriate code of conduct based upon the principles in the Consumer Privacy Bill of Rights. The Report contemplates that there may be 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, the Administration expects that this commitment would be enforceable under Section 5 of the FTC Act, because the company's representation would become subject to the FTC's jurisdiction over deceptive or misleading trade practices. The Report also contemplates that codes of conduct will be modifiable due to changes in "technology, consumer expectations, and market conditions."

Do-Not-Track

In conjunction with the White House release of the Report, leading Internet companies and online advertising networks 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.

Companies-including Google, Yahoo! Microsoft, AOL and the Digital Advertising Alliance-representing the delivery of nearly 90 percent of online behavioral advertisements have agreed to comply with consumers' Do-Not-Track preferences. 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 it prohibits use for employment, credit, health-care or insurance purposes. Although several browsers already include Do-Not-Track indicators, the participation of advertisers and tracking companies in the agreement will help to ensure that the buttons will soon function the way that consumers expect. As in the case of the codes of conduct, the agreement will be subject to FTC enforcement.

Call for Consumer Privacy Legislation

The White House also called upon Congress to enact the Consumer Bill of Rights into law. The United States does not have a general consumer privacy law, instead relying on various sector-specific laws affecting areas such as healthcare, education, communications, financial services and online data collection from children. 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 federal legislation not modify existing federal sector-specific privacy statutes unless those statutes set inconsistent standards. However, the Administration recommends that federal legislation preempt state laws that set lesser privacy standards.

Promotion of Cross-Border Data Flows

Finally, 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 multistakeholder process and foster international enforcement cooperation.