

White House Outlines Consumer Privacy Bill of Rights

By Andrew Martin

In late February 2012, the White House outlined a consumer data privacy framework that includes a “Consumer Privacy Bill of Rights” in a report entitled “[Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.](#)” In it, the administration sets out a plan for a four-element approach to protection of consumer privacy: 1) enumerate the consumer privacy rights; 2) encourage industry developed codes of conduct; 3) strengthen FTC enforcement power; and 4) ensure interoperability with international privacy rules and regulations.

The Consumer Privacy Bill of Rights sets out seven individual rights that consumers have with respect to commercial uses of their personal data:

- Individual Control – consumers have the right to control both the kinds of data they share with a company and how the company uses that data.
- Transparency – consumers have the right to accessible, easy-to-understand policies governing the security practices of the commercial companies.
- Respect for Context – consumers have the right to expect companies to use their data in such a way that is consistent with the context in which the consumer is engaging with the individual company.
- Security – consumers have the right to reasonable, responsible protection of their data.
- Access and Accuracy – consumers have the right to access and correct their personal data held by a company.
- Focused Collection – consumers have the right to have companies impose reasonable limits on the kinds of data they collect from the consumer.
- Accountability – consumers have the right to have companies held accountable for any violation of their rights under the Consumer Privacy Bill of Rights.

Without legislative authority, however, the bill of rights outlined by the administration amounts to little more than an interesting academic exercise. Cognizant of the fact that there is little likelihood of passing sweeping, federal privacy legislation during an election year, the administration instead suggests that stakeholders (including individual companies, industry groups, consumer advocacy groups, State Attorneys General, and federal civil and criminal law enforcement), work to develop codes of conduct that will protect consumers’ right to privacy. The paper proposes empowering the FTC to, if not outright *enforce* the codes of conduct, at least strongly consider a company’s adherence to the codes of conduct in the event of any investigation or enforcement action.

Despite the fact that actual enforcement of the consumer privacy bill of rights is not imminent, companies doing any sort of business online should take this time to review their data privacy and security policies. Knowing how a business stands today with respect to these privacy and security issues will help to ease the transition to where it needs to go tomorrow.



About the author Andrew Martin:

As an associate attorney with extensive prior experience advising information technology start-ups, Andrew’s practice focuses on finding solutions for his clients’ intellectual property issues. Due to his extensive experience in the software and technology industries, Andrew understands both the practical and legal issues involved in IP licensing agreements and disputes. In addition to licensing, Andrew helps his clients find new ways to use existing technologies to assist his clients in areas such as data privacy compliance. Andrew uses his diverse background which includes founding a record label and working for a world-wide concert promoter when counseling the firm’s entertainment clients.

Get in touch: amartin@scottandscottllp.com | 800.596.6176