White House Releases Online Privacy Paper

The White House has released a report titled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the Report)[1] detailing the Obama administration's framework to protect the privacy rights of individuals in a global digital economy. The framework consists of four main elements: (i) a Consumer Privacy Bill of Rights containing seven general privacy principles, (ii) an enforceable code of conduct developed through a "multistakeholder process" applying the general principles to particular business contexts, (iii) Federal Trade Commission (FTC) enforcement and (iv) international collaboration.

Defining a Consumer Privacy Bill of Rights

The Code of Fair Information Practices, commonly referred to as the fair information practice principles (FIPPs) serves as the basis for the Consumer Privacy Bill of Rights (CPBR). The US government developed the FIPPs in the early 1970s. Since then, the FIPPs have been incorporated into domestic sector-specific privacy laws[2] and international data privacy frameworks. The CPBR affirms the consumer rights embodied in the FIPPs, but applies them to modern privacy challenges by emphasizing the context of their application.[3] The CPBR consists of the following seven consumer data privacy rights.

Individual Control: Consumers have the right to exercise control over what personal data companies collect and how companies use such data. The first dimension to individual control is offering consumers a choice about data collection, use, and sharing that are appropriate for the scale, scope, and sensitivity of the personal data collected.

Companies that deal directly with consumers must provide "appropriate choices about what personal data the company collects," and, in contracting with third parties that gather data, must be "diligent in inquiring how those third parties" use personal data and adhere to the principles. Companies that collect personal data without direct consumer interaction—i.e., data brokers—should nonetheless, "seek innovative ways to provide consumers with effective Individual Control." If this is "impractical," however, these companies should ensure full compliance with the other elements of the CPBR.

The second dimension of Individual Control is "consumer responsibility." As is the case with social networks, the use of personal data may begin with a consumer's decision to make information available and to limit access. Companies must provide usable tools and clear explanations to enable customers to make meaningful choices from the outset.

Finally, the "right to withdraw consent" is a critical feature of this principle, but it is subject to three practical limitations: the principle presumes there is an ongoing relationship, extends only to data that the company has under

its control, and does not apply to data collected before implementation of the CPBR.

Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices. Companies should provide customers with "privacy notices" that are "clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties." The notice must be provided at a time and in a place that provides customers with a meaningful opportunity to exercise Individual Choice. Personal data uses that are inconsistent with the relationship or transaction between the company and customer deserve "more prominent disclosure." Companies that do not interface directly with consumers need to make available—e.g., on their website or a publicly accessible location—explicit explanations of how they collect, use, and share personal data.

Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. The use and disclosure of information should be consistent with the customer-company relationship as well as the context in which the information was originally disclosed. Companies that will use or disclose data for other purposes must, at the time the decision is made, provide "heightened Transparency and Individual Control." A final consideration is the consumer's age and sophistication.

Security: Consumers have a right to secure and responsible handling of personal data. The principle mandates risk assessments measuring privacy and security vulnerabilities. A company must maintain "reasonable safeguards to control risks" which may include "loss, unauthorized access, use, destruction, modification and improper disclosure."

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 is inaccurate. Companies should use "reasonable measures" to ensure personal data is accurate. Companies should also provide customers "reasonable access" to their personal information as well as means to correct, delete, or limit the use of inaccurate data. In determining the scope of their obligations under this principle, companies may consider the "scale, scope, and sensitivity" of the stored data, and the likelihood that use of the data may expose consumers to "financial, physical, or other material harm." The Report also emphasizes the presentation of the information to consumers in a usable format. This principle does not distinguish between consumer-facing companies and non-consumer-facing companies, but focuses on the degree of harm possible from improper use of the data actually maintained.

Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain. Companies should collect "only as much personal data as they need to accomplish purposes specified under the Respect for Context principle." Companies may "find new uses for personal data" as long as they take appropriate steps under the Transparency and Individual Choice principles. When maintaining data is no longer needed or authorized, that data must be securely deleted or de-identified, unless a company is legally obligated to retain such data.

Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to ensure the companies adhere to the CPBR. This principle promotes adherence to the CPBR by calling for accountability to "enforcement authorities and consumers." The Report takes no position on a private right of action. Beyond external accountability, companies are required to

prevent lapses in privacy commitments and to detect and remedy lapses. Companies must engage in self-assessment that, depending on the size, complexity and nature of a company's business, may be a self-assessment or an independent audit. Companies must also "train their employees as appropriate to handle personal data." A company that transfers personal data to a third party, "remains accountable and thus should hold the recipient accountable" by contract or other legally enforceable means.

Implementing the Consumer Privacy Bill of Rights: Multistakeholder Processes to Develop Enforceable Codes of Conduct

The multistakeholder process is designed to implement codes for specific practices, applying the CPBR. According to the Report, as demonstrated by previous success in similar contexts, this process provides the "flexibility, speed, and decentralization necessary to address internet policy challenges."

The Department of Commerce's National Telecommunications and Information Administration (NTIA) will convene the multistakeholder process. Step one is **deliberation**. In this phase, shareholders, with NTIA's assistance, will identify target markets and industry sectors. Also in this phase, NTIA will enlist the assistance of all stakeholders with an interest in defining the codes. A prerequisite to the substantive discussion will be to establish operating processes and procedures.[4] NTIA will help parties reach clarity on their positions and work towards consensus.

The next two steps are **adoption** by companies and **evolution** of the codes. The administration expects that a company's adoption of a code will become enforceable under Section 5 of the FTC Act (15 U.S.C. §45), as is the case with a company's public commitment to adhere to its privacy policies. Evolution of the codes is necessary to respond to "rapid changes in technology, consumer expectations, and market conditions." The evolution, spurred either by the shareholders or NTIA, would not result in government revision to the code, but rather, "stakeholder groups will make these changes with Federal Government input."

Building on the FTC's Enforcement Expertise

According to the Report, the FTC is the ideal agency to enforce the CPBR and the codes. The agency currently enforces companies' failure to (i) adhere to voluntary privacy commitments, such as privacy policies and (ii) use reasonable security measures to protect personal information. As an incentive to adopt the codes, the FTC will consider favorably a company's adoption of and adherence to an applicable code in any investigation or enforcement action.

Promoting International Interoperability

The administration believes the CPBR and multistakeholder process facilitate interoperable privacy regimes. It hopes to increase interoperability by pursuing mutual recognition;[5] using the multistakeholder process and codes in an international setting; and through enforcement cooperation.

Enacting Consumer Data Privacy Legislation

The Report urges Congress to: (i) codify the CPBR, (ii) grant the FTC direct enforcement authority, (iii) grant the FTC safe harbor designation authority to companies that follow an approved code, (iv) preempt inconsistent state laws, whether the requirements are weaker or "more stringent," (v) preserve effective, existing data privacy laws,[6] avoid duplicative laws, and amend inconsistent laws, and (vi) set a national standard for security breach notification. In particular, the Report proposes to eliminate duplicative federal privacy related statutes, including Sections 222, 338, and 631 of the Communications Act (47 U.SC et. seq.), which

apply to telecommunications carriers, satellite providers, and cable operators, respectively.

For more information about the Report, or any other matter raised in this Legal Update, please consult your regular Mayer Brown lawyer or the following lawyer.

Howard W. Waltzman
+1 202 263 3848
hwaltzman@mayerbrown.com

Endnotes

[1] The Report builds on the Department of Commerce Internet Policy Task Force's December 2010 report titled, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, as well as more than 100 response-submissions authored by various stakeholders.

[2] Appendix B to the Report compares the CPBR to applications of the FIPPs.

[3] Context is a major theme in the CPBR. The key elements of context include "the goals or purposes that consumers can expect to achieve by using a company's products or services, the services that the companies actually provide, the personal data exchanges that are necessary to provide these services, and whether a company's customers include children and adolescents."

[4] One major goal of the procedures is to have a mechanism to reach an orderly conclusion in the face of "inflexible stakeholder lines that prevent consensus."

[5] Mutual recognition between privacy frameworks is possible where there are common values, effective enforcement, and mechanisms that allow companies to demonstrate accountability.

[6] The Report cites HIPAA's Privacy Rules and Security Rules, specifically, and mentions privacy laws applicable to "education, credit reporting, financial services, and the collection of children's personal data," generally.