White House Introduces Discussion Draft of Consumer Privacy Bill of Rights

Although most states have enacted some form of data privacy and breach notification laws, and certain federal statutory schemes cover specific industry sectors, there are no privacy protections for *all* personal data. Given the increasing collection and use of personal data, and the frequent headlines regarding data breaches, the White House released its administration discussion draft of the Consumer Privacy Bill of Rights Act ("CPBR") on February 27, 2015. The CPBR has largely been met with criticism from both industry groups and consumer groups.

Industry groups contend the new law is not needed because there are already adequate privacy regulations. *See* Ana Radelat, ANA Pans Obama's Consumer Privacy Bill of Rights (Mar. 4, 2015), *available at http://adage.com/article/datadriven-marketing/ana-pans-obama-s-consumer-privacy-bill-rights/297440/.* *Industry groups also believe that the increased regulation would stifle innovation.* *See* Brendan Fasso, Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides (Feb. 27, 2015) *available at http://www.nationaljournal.com/tech/obama-s-privacy-bill-of-rights-gets-bashed-from-all-sides-20150227* ("Tech companies warned that the [CPBR] would impose burdensome regulations, potentially stifling exciting new online services that could benefit consumers.").

On the other hand, many privacy and consumer groups have complained that the bill does not go far enough to protect consumers. As the LA Times reported, representatives from the Center for Democracy and Technology, Consumer Watchdog, Electronic Frontier Foundation, and Public Knowledge have criticized the bill for not "adequately defining 'what constitutes sensitive information,' not being clear about whether it protects large categories of information like geolocation data, allowing companies to retain user data indefinitely for criminal investigations without placing clear limits on data retention for that purpose, and not offering heightened protection for information about children and teens." *See* Tracey Lien, *Consumer Privacy Bill of Rights Doesn't Go Far Enough, Critics Say,* LA TIMES (Mar. 3, 2015), *available at http://www.latimes.com/business/technology/la-fi-tn-consumer-privacy-act-criticism-20150303-story.html.* Additionally, the Electronic Privacy Information Center has called the bill "not helpful" and "unworkable" and complains about the lack of meaningful consumer protection, preemption of stronger state laws, and the creation of unnecessary burdens. *See* White House Consumer Privacy Bill of Rights, epic.org (Mar. 2, 2015) *available at* https://epic.org/privacy/white_house_consumer_privacy_.html.

Although this proposal will likely not be enacted, this article gives an overview of the Act as introduced. The Act is broken into four titles: Title I-Privacy Bill of Rights; Title II-Enforcement; Title III-Codes of Conduct to Implement the Consumer Privacy Bill of Rights; and Title I- Miscellaneous. We will continue to monitor the discussion of the proposal as well as other data privacy issues.

Overview of the CPBR

Applicability

Generally, the CPBR would apply to covered entities dealing with personal data.

Although subject to certain exceptions, a "covered entity" is defined as "a person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce." Exceptions include: governments, government employees, a natural person (unless acting in a commercial capacity), and any person that has 25 or fewer employees and would otherwise only be a covered entity because of the data the person processes related to job applications and employment. An exception also exists for any person that collects, creates, processes, uses, retains, or discloses personal data of fewer than 10,000 individuals and devices during any 12-month period, or has fewer than 5 employees, and does not knowingly collect, use, retain, or disclose information that is linked with personal data and includes medical history information, national origin, sexual orientation, gender, identity, religious beliefs or affiliation, income, assets or liabilities, precise geolocation information, unique biometric data, or Social Security number.

"Personal data" means data under the control of a covered entity, not otherwise generally available to the public, and linked, or linkable, to a specific individual or a device routinely used by the individual. "Personal data" includes: first name or initial and last name, postal or email address, a telephone or fax number, Social Security number, tax identification number, passport number, driver's license number, or any other unique government-issued identification number, any biometric identifier, any unique persistent identifier (including financial account numbers, credit card or debit card numbers, health care account numbers, unique vehicle identifiers such as license plate numbers and Vehicle Identification Numbers), unique identifiers or other uniquely assigned or descriptive information about computing or communication devices; or any data, linked or linkable, to any of the foregoing.

Exceptions to "personal data" include de-identified data, deleted data, employee information, and cybersecurity data.

Many of the provisions of the CPBR are written in the context of "privacy risk." "Privacy risk" is defined as "the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or other harm to an individual."

Title I-Privacy Bill of Rights

Title I, Section 101. Transparency.

If enacted, the CPBR would require each covered entity to provide individuals "in concise and easily understandable language, accurate, clear, timely, and conspicuous notice about the covered entity's privacy and security practices."

At a minimum, the notice would need to contain: (1) the personal data processed and the sources of data collection (if not coming from the individual); (2) the purposes for which the data is collected, used, and retained; (3) the persons, or categories of persons, to whom the information is disclosed and the reason for the disclosure; (4) when the personal data will be destroyed, deleted or identified (if it will not, the notice must say so); (5) mechanisms for individuals to have a meaningful opportunity to access their personal data and grant, revoke, or consent to the processing; (6) whom individuals may contact with inquiries or complaints; and (7) the measures taken to protect personal data.

Title I, Section 102. Individual Control.

The CPBR also would give individuals some level of control regarding data collection and use. It would require a covered entity to "provide individuals with reasonable means to control the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context." The control mechanisms provided must be reasonably accessible, understandable, and usable and available at times and in manners that are reasonable.

Moreover, individuals must be given an opportunity to withdraw consent. If an individual withdraws consent, the entity must delete the data within a reasonable period of time not less than 45 days or provide the individual with the means to request that their data be de-identified.

If an entity materially changes its data collection, use, dissemination, or maintenance procedures, it must provide advance clear and conspicuous descriptions of the changes and controls to mitigate against privacy risks associated with previously collected personal data.

Title I, Section 103. Respect for Context.

This section of the CPBR would only apply if the entity processes personal data in a manner that is *not* "reasonable in light of context." Personal data processing that fulfills an individual's request is presumed to be reasonable in light of context.

If a covered entity processes personal data in a manner that is *not* "reasonable in light of context," it must conduct a privacy risk analysis and take reasonable steps to mitigate identified privacy risks, including providing "heightened transparency and individual control." Individuals should be given notice regarding privacy practices that are not reasonable in light of context at times and in a manner reasonably designed to enable individuals to decide whether to reduce their exposure to the associated privacy risk and provide a mechanism for control allowing the individual to reduce the privacy risk.

However, an entity would not have to provide heightened transparency and individual controls if its analysis of the data is supervised by a Privacy Review Board approved by the FTC and the Privacy Review Board determines it: (1) is impractical to provide heightened transparency and individual controls; (2) the goals of the entity's analysis are likely to provide substantial benefits that do not exclusively accrue to the entity; (3) the entity has taken

reasonable steps to mitigate privacy risks; and (4) the likely benefits of the analysis outweigh the likely privacy risks.

Title I, Section 104. Focused Collection and Responsible Use.

A covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context . An entity would be required to consider ways to minimize privacy risk and delete, destroy, or de-identify personal data within a reasonable time after it has fulfilled the purposes for which the personal data was collected.

Title I, Section 105 Security.

A covered entity is required to: (1) identify reasonably foreseeable internal and external risks to the privacy and security of personal data; (2) establish, implement, and maintain safeguards designed to ensure security of personal data; (3) regularly assess the sufficiency of any safeguards in place; and (4) evaluate and adjust the safeguards as needed.

Title I, Section 106. Access and Accuracy.

A covered entity would be required, upon request, to provide an individual with reasonable access to personal data. A covered entity would only be allowed to deny access if the individual cannot verify his or her identity, access to the personal data is limited by applicable law or privilege, or the request is "frivolous or vexatious."

Covered entities would be required to maintain procedures to ensure that the personal data is accurate, unless the personal data was obtained from government records or from the individual.

A covered entity would be required to provide individuals with a means to dispute and resolve the accuracy or completeness of personal data. If a covered entity uses or discloses personal data for purposes that could not reasonably result in an adverse action against the individual, the entity may decline to correct the personal data. If the entity declines to correct the personal data, the entity would be required, upon request, to destroy or delete the personal data that the covered entity maintains within a reasonable time that need not be less than 45 days.

Title I, Section 106. Accountability.

A covered entity must take measures appropriate to the privacy risks associated with its personal data practices, including, but not limited to: (1) training employees working with personal data; (2) conducting internal or independent evaluations of their privacy and data protections; (3) building appropriate consideration for privacy and data protections into the design of its systems and practices; and (4) binding any person to whom the covered entity discloses personal data to use such data consistently with the covered entity's commitments to personal data.

Title II-Enforcement

Title II, Section 201. Enforcement by the Federal Trade Commission

This section provides that a violation of Title I is to be treated as an unfair or deceptive act or practice in violation of section 5 of the Federal Trade Commission Act.

The FTC cannot bring an enforcement action for violations of Title I seeking civil penalties against a covered entity based upon the entity's conduct undertaken within the first eighteen months after the date the covered entity first created or processed personal data.

Title II, Section 202. Enforcement by State Attorneys General.

If a state attorney general believes that a covered entity in violation of Title I has caused or is causing harm to a substantial number of the state's residents, the attorney general may bring a civil action on behalf of those residents exclusively in an appropriate district court of the United States. Unless the FTC brings an action or intervenes, the only remedy that may be awarded is injunctive relief.

Title II, Section 203. Civil Penalties.

In an action brought by or prosecuted by the FTC, the covered entity is liable for a civil penalty if it, with actual knowledge or knowledge fairly implied on the basis of objective circumstances, violates the Act. The amount of the civil penalty should be based upon the degree of culpability, any history of prior conduct, ability to pay, effect on ability to continue to do business, and other matters as justice requires.

The penalty is calculated by multiplying the number of days the covered entity is in violation of the Act by an amount not to exceed $35,000; or, if the FTC provided notice with particularity of a violation, the penalty shall be calculated by multiplying the number of directly affected consumers by an amount not to exceed $5,000, unless, within 45 days of receiving the notice, the covered entity files an objection meeting certain requirements

The total civil penalty cannot exceed $25,000,000.

Title III. Codes of Conduct to Implement the Consumer Privacy Bill of Rights

Title III-Section 301. Safe Harbor Through Enforceable Codes of Conduct.

Any person may apply to the FTC for approval of codes of conduct governing the processing of personal data by a covered entity. The codes of conduct provide a "safe harbor" meaning that a complete defense exists to any action brought under Title II of the ACT if the defendant entity demonstrates that it has maintained a public commitment to adhere to an FTC-approved code of conduct that coves the practices underlying the suit or action and is in compliance with the code of conduct.

Title IV. Miscellaneous.

The CPBR would preempt any State or local government statutes, rules, or regulations to the extent that the provision imposes requirements on covered entities with respect to personal data processing. It would not, however, preempt any attorney general or official enforcement action of any State consumer protection law of general application not specific to personal data processing. Nor would it preempt any State or local laws addressing the processing of health or financial information, notification requirements in the event of a data breach, trespass, contract, or tort law, privacy of minors, or other laws relating to fraud and public safety.

No private right of action exists under the CPBR.