Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 4 >>> APRIL 2015

The Draft U.S. Consumer Privacy Bill of Rights Act: Proposing Changes Large and Small

By Catherine Meyer, of Pillsbury Winthrop Shaw Pittman LLP, Los Angeles.

On February 27, 2015, the Obama Administration released its discussion draft of the Consumer Privacy Bill of Rights Act ("Draft")[1] (*see WDPR, March 2015, page 30*). Its stated purpose is to "establish baseline protections for individual privacy" and to implement and enforce those protections.

The Draft proposes to provide a single national standard replacing the patchwork of state laws now in place addressing consumer data protection. The proposal would expand some coverage currently offered by the states, mirror some current requirements and follow some current global trends in data protection. It would offer a "safe harbor" allowing companies to obtain Federal Trade Commission ("FTC") approval of their privacy codes of conduct. Enforcement would be limited to the FTC and state attorneys general, with a substantial grace period before enforcement actions commenced.

Background

Data protection on the federal level has historically focused on industry sectors rather than individual consumers. For example, financial institutions are required to adhere to standards established in the Safeguards Rule under the Gramm-Leach-Bliley Act, and health care service providers must comply with the privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act ("HIPAA"). Protection of individual information has been the purview of state law, with each state enacting legislation protecting its own residents. Some states, like California, have extensive protections, while others have few. Massachusetts has adopted regulations that specify minimum standards, while other states that address the issue use a generalized "reasonable" standard.

Compliance with privacy laws has been a challenge for companies that operate nationwide within the U.S., even ignoring the greater challenge of privacy compliance globally. First, each state is entitled to protect the legitimate health, safety and interests of its own residents while in their home state, provided the legislation does not regulate wholly out-of-state activity in violation of the Commerce Clause of the U.S. Constitution.[2] In the exercise of this right, states can (and do) enforce their own laws against out-of-state businesses that interact with state residents. Second, each state approaches privacy legislation differently, as discussed in more detail below. Third, states have been able to enact or amend their legislation relatively quickly as technology advances. As a result, a company with customers in multiple states will have to comply with the privacy laws of each of those states, to be aware of nuances

in each individual state and to constantly keep up to date on legislative developments.

Examining the Draft against this background puts its advantages and disadvantages into context.

Enactment of the Consumer Privacy Bill of Rights Act would bring greater certainty to privacy compliance by businesses operating nationwide in the U.S. Compliance with a single statute and the potential for safe harbor status should be attractive to businesses that currently struggle to maintain compliance with multiple diverse statutes across the 50 states.

Mirroring, But Also Broadening, Protections Afforded by Existing State Laws

The Draft proposes to build on existing state law. In some areas, it would mirror existing state laws. In other areas, it would broaden state law protections to cover additional data or additional data collectors and to require additional disclosures or more particular security.

What Data Would Be Protected?

The classes of personal data that are protected under state laws vary somewhat from state to state, depending on the circumstances under which data is being protected.

The Draft would expand the definition of personal data that was protected under its terms.

To provide some context for the variety of state privacy laws, nine states require some measure of protection of personal information held in a database, 24 states require secure destruction of personal information, two states affirmatively require encryption of data, and fewer than six states impose obligations of oversight of vendors with access to personal information. Additionally, three states require written policies addressing data security and three require written policies only regarding Social Security numbers.

California provides a good example of the variation in the definition of personal information. For purposes of determining what data should be protected under the California Online Privacy Protection Act,[3] the only statute requiring disclosures through an online privacy policy, "personally identifiable information" is broadly defined. It encompasses name, physical or email address, telephone number, Social Security number, or "any other identifier that permits the physical or online contacting of a specific individual," as well as any information that is maintained in combination with such attributes. However, for purposes of determining what data should be secured from unauthorized access, destruction, use, modification, or disclosure or should be protected by contract when accessible by third parties, California uses a narrower definition. In these cases, "personal information" is defined as an individual's unencrypted first name/initial and last name together with his or her Social Security, driver's license or state identification number; a financial account number and security or access code; and medical information.[4] For purposes of determining what data should be securely destroyed, California expands the definition of "personal information" to mean any information that "identifies, relates to, describes or is capable of being associated with, a particular individual" and provides examples that include, without limitation, signature, physical characteristics or description, passport number, education, employment and employment history along with the data identified in the two previously mentioned statutes.[5]

The Draft would expand the definition of personal data that was protected under its terms.

The Draft proposes an expanded definition of "personal data" and would not vary that definition for different purposes. First, the definition of personal data would include not only information not generally available to the public that is linked to a specific individual, but also information linked to a device that is associated or routinely used by an individual. Second, in addition to the attributes typically identified in state law, the Draft would include, as examples of personal data (without limitation), passport or other government-issued identification numbers, biometric identifiers, device identifiers, any commercial account numbers, vehicle identification or license plate numbers, and access codes or passwords needed to access an account.

An entity collecting or holding "personal data" would have to make certain disclosures, protect that data and securely dispose of it.

In this way the Draft would unify the state laws and make the protections available to all U.S. residents, even those living in states that previously did not provide statutory privacy protections.

Who Must Comply?

The Draft would require compliance by any covered entity, which includes any "person that collects, creates, processes, retains, uses or discloses personal data in or affecting interstate commerce." Exceptions would be limited to government entities, natural persons (unless acting in a non-*de minimis* commercial capacity), and entities with 25 or fewer employees or that have nominal data collection activities. The Draft would extend to online and offline activity, and would reach profit and nonprofit entities as well as non-commercial organizations.

In contrast, California requires privacy policy disclosures only by commercial entities collecting data online without regard to size or amount of data collected. Nonprofits and governmental entities are not covered. California exempts financial institutions and HIPAA covered

   ISSN 1473-3579

entities from its requirements for maintaining security procedures or overseeing third party vendors. Massachusetts, whose data security regulation is the most specific nationwide, requires compliance by any natural person, corporation, association, partnership or any other non-governmental legal entity that owns or licenses personal information about a state resident, without regard to whether the data is collected online or offline.[6]

What Practices Must Be Disclosed?

The Draft would require certain disclosures to be provided to individuals in an effort to ensure transparency.

On the state law front, one state, California, requires entities that operate a commercial website or other online service to post a privacy policy disclosing the entity's practices. The California Online Privacy Protection Act[7] requires the following six disclosures:

- the categories of personally identifiable information collected online and the categories of third parties with whom that information is shared;
- the process (if offered) for an individual to review and request changes to his or her information;
- the process the operator uses to notify consumers of material changes to the privacy policy;
- the effective date of the policy;
- how the operator responds to Web browser "do not track" signals or similar technologies through which consumers can exercise choice regarding the collection of information about their online activities over time and across websites; and
- whether third parties may collect personally identifiable information about a consumer's online activities over time and across websites when the consumer uses the operator's site or services.

The Draft would track and expand on the concept of an online privacy policy, requiring every "covered entity" to adopt a privacy statement or notice. The notice would have to be made available to all individuals, not just online. The required notice would have to include the following seven disclosures:

- the personal data processed, including the sources of data collection (if not received directly from the individual);
- the purpose for collecting, using and retaining such data;
- the categories of persons with whom the data is shared;
- when the data will be destroyed, deleted or de-identified (or if it will not be destroyed, deleted or de-identified);
- the mechanisms to grant a "meaningful opportunity" to access data and grant, refuse or revoke consent for processing that data;
- a point of contact for inquiries or complaints; and
- the measures taken to secure the data.

In addition, the Draft would require that covered entities provide clear and conspicuous descriptions of material changes to their policies. Thus the Draft's coverage would include many of the disclosures required in existing state law, and then would add requirements for disclosing the purpose for collecting personal data and when the data is destroyed. The key difference is that the Draft would require disclosure for its expanded definition of personal data, whether collected online or offline, and whether the entity collecting it was for profit or non-profit.

Security Obligations

Most of the states that require that personal information be secured rely on a general description of the obligation, such as to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect it against unauthorized access, destruction, use, modification or disclosure.[8]

Massachusetts takes a different approach, and provides specific baselines for the comprehensive data security plan it requires of those holding personal information about a resident. Each plan, while scalable depending on the nature and scope of data maintained, must at least address 12 designated activities:

- designate a responsible employee;
- identify/assess risks to the security, confidentiality and integrity of personal information;
- develop an employee security policy;
- provide enforcement or discipline for violations;
- provide procedures for terminated employees;
- oversight of vendors, including written certification of compliance;
- limitations on the amount of information collected, how long it is retained and who can access it;
- identify all records and media holding personal information;
- monitor compliance;
- perform annual review;
- develop an incident response plan; and
- maintain specified security protocols.

The Draft would require that each covered entity must secure personal data. This includes the establishment and maintenance of safeguards using language similar to the general descriptions in some state laws. In addition, covered entities would be required to conduct risk assessments and re-assess their safeguards in light of changes to their business or other circumstances. The safeguards are scalable, and the reasonableness of the safeguards would be judged according to the degree of privacy risk to the data, the foreseeability of threats to

the data, widely accepted practice for protecting data and the cost of implementing and regularly reviewing the safeguards.

'Safe Harbor' through Enforceable Codes of Conduct

In Title III, the Draft contains the provisions for codes of conduct, and proposes a "safe harbor" for covered entities that adopt enforceable codes of conduct. This would allow covered entities to develop their own codes of conduct for complying with the Draft and to protect themselves against potential enforcement actions by having their codes of conduct be approved by the FTC.

The application for approval of a code of conduct would have to include a description of how it provides protections for personal data that are equal to or greater than those defined in the Draft, a description of the entities or activities the code of conduct would cover, a description of how the code was derived, a list of the covered entities planning on adopting the code of conduct and any additional information requested by the FTC. The FTC would be required to act promptly on the applications. For applications developed through a Department of Commerce multistakeholder process, the FTC must act within 90 days after receipt. It must act within 120 days on applications developed through a process that is open to and affords a voice to all interested participants and which maintains transparency by making decisional documents readily available to the public for meaningful review. For all other applications, it must act within 180 days of receipt.

Codes of conduct that are approved by the FTC would be presumed to meet the requirements of the Draft. The safe harbor would require that the FTC reassess the code of conduct between three and five years after its initial approval. If the code of conduct continued to meet the FTC's standards, it would continue to qualify as a safe harbor for a period of up to five additional years.

Preemption and Enforcement

The Draft specifies that it would not have unlimited preemptive effect. Generally, it would preempt any provision of a state or local statute or regulation to the extent that such provision imposed requirements on covered entities with respect to personal data processing. It would not preempt state or local laws addressing the processing of health or financial information; data breach notification; trespass, contract or tort laws; the privacy of kindergarten through 12th grade students or those under the age of 18; or fraud or public safety. It would not limit enforcement by a state official of any state consumer protection law of general application and not specific to personal data processing.

Enforcement of the Draft's requirements would be relegated to the FTC. A violation of the Draft would be treated as an unfair or deceptive act under the Federal Trade Commission Act. A state attorney general would have limited power to enforce violations, only after notice to the FTC and a decision by the FTC not to participate. The FTC would have the ability to intervene as a party to any proposed civil action by the state attorney general and to assume lead responsibility for the prosecution of the action. There is specifically no private right of action to enforce compliance.

There would be a transitional period during which enforcement was prohibited, as well as a "new business" exception. The FTC could not bring an enforcement action within the first two years after the date of enactment. Further, it could not bring an action based on conduct within the first 18 months after the date the covered entity first created or processed personal data.

Penalties for violating the Draft would be calculated by multiplying the number of days the violation existed by an amount not to exceed $35,000. Alternatively, if the FTC notified the covered entity of specific violations, the civil penalty would be calculated by multiplying the number of directly affected consumers by an amount not to exceed $5,000. The maximum civil penalty would be $25 million.

Comment

Enactment of the Consumer Privacy Bill of Rights Act would bring greater certainty to privacy compliance by businesses operating nationwide in the U.S. Compliance with a single statute and the potential for safe harbor status should be attractive to businesses that currently struggle to maintain compliance with multiple diverse statutes across the 50 states.

NOTES

[1] Available at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[2] *See*, for example, *Watson v. Employer Liability Corp.*, (1954) 348 U.S. 66 and *Huron Cement Co. v. Detroit,* (1960) 362 U.S. 440.

[3] CA Business & Professions Code Section 22575 *et seq.*

[4] CA Civil Code Section 1798.81.5

[5] CA Civil Code Sections 1798.80 and 1798.81.

[6] 201 CMR 17.00 Standards for the Protection of Personal Information of Residents of the Commonwealth.

[7] CA Business & Professions Code Sec. 22575 *et seq.*

[8] *See*, for example, CA Civil Code Section 1798.81.5.

The text of the discussion draft of the Consumer Privacy Bill of Rights Act is available at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

Catherine Meyer is Senior Counsel at Pillsbury Winthrop Shaw Pittman LLP, Los Angeles. She may be contacted at catherine.meyer@pillsburylaw.com.

   ISSN 1473-3579