DrinkerBiddle

Client Alert

January 26, 2015

Proposed Personal Data Notification & Protection Act

By Kenneth K. Dort and Mita K. Lakhia

Leading up to his State of the Union address last week, President Obama proposed a number of federal legislative goals intended to provide a uniform standard as to how data breaches and other related incidents would be addressed across the United States. The initiatives included, among others: (i) The Personal Data Notification & Protection Act; (ii) The Student Digital Privacy Act; (iii) a Voluntary Code of Conduct for Smart Grid Customer Data Privacy; and (iv) a Consumer Privacy Bill of Rights – all of which were generally referenced during the address to bipartisan applause. Given the influx of media attention drawn to data-related incidents over the last two years, it is not surprising that the president intends to start 2015 with a focus on the safeguarding the data of American consumers and families.

Specifically, the proposed Personal Data Notification & Protection Act (the "Act") offers a single standard for companies to adhere to in the event of a data-related incident. When applicable, this proposed legislation will supersede current state data breach notification laws, and in effect create a single checklist to follow in responding to a breach. Outlined below are the key provisions set forth in the proposal.

1. Federal Trade Commission.

A central theme to note with regard to each of the provisions of the Act is the central role envisioned for the FTC. As discussed in more detail below, a business entity must approach the FTC to request an extension of time to notify individuals or to qualify for the Act's safe harbor provision. The Act also includes several rulemaking provisions designed to give the FTC additional authority to modify the definition of Sensitive Personally Identifiable Information, revise the notice to law enforcement provisions and requirements of such notice, and address enforcement issues – all of which would supplement its current authority under Section 5 of the FTC Act to take action in the data security and privacy sector.

2. Sensitive Personally Identifiable Information.

Currently, state statutes offer a variety of definitions of what qualifies as "personally identifiable information" or "sensitive personally identifiable information." The proposed legislation, however, as drafted, considerably expands this definition by defining Sensitive Personally Identifiable Information as including any one of a number of scenarios. The most expansive being sections 1, 2, 3 and 4:

(1) An individual's first and last name or first initial and last name in combination with any two of the following data elements:

(a) Home address or telephone number;

(b) Mother's maiden name;

(c) Month, day, and year of birth;

(2) A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number;

(3) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;

(4) A unique account identifier, including financial account number or credit or debit card number, electronic identification number, user name, or routing code.

As these sections now stand, an unauthorized disclosure of a list, for example, of social security numbers or driver's license numbers with no associated names would constitute a security breach under this Act. Similarly, biometric data alone or credit card data alone would be considered a breach. This would be a major expansion of current state law in that without associated names, a disclosure of such data points would not require responsive action by any state.

3. Notice to Individuals.

The Act provides that it will apply to any business entity that "uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period." Therefore, is inapplicable to entities who have data (and use it in some way) of less than 10,000

individuals. Thus, a data incident for very small companies would still be covered by applicable state notification laws.

The Act also requires that notification about a breach must occur within a "reasonable time," which is defined as not exceeding 30 days from the "discovery" of a breach. The Act is not clear as to when this trigger occurs – is it when a business first learns of a security problem requiring additional investigation, or when a business first concludes that a breach has occurred? The Act is not clear on this point.

However, the Act also provides that it does not require notice in response to those breaches where "there is no reasonable risk of harm or fraud." Such a finding must be supported by a risk assessment submitted to the FTC within the 30-day notice period. The Act specifies what must be included in these assessments, including system logging data for the six-month period preceding the breach.

In the event that an entity requires more than the 30 days provided by the Act for notification to affected persons, that entity must seek an extension of time from the FTC. This process would likely be refined via the FTC's rulemaking authority. As currently handled by existing state laws, the method of notice would be accomplished by written notice, personal telephone calls, or an email notice if the individual has consented thereto. Additionally, the entity must issue a notice via major media outlets in those states where the number of affected persons reaches 5,000 people.

Likewise, the Act's provisions as to the content of breach notices is similar to the majority of current state statutes – a description of the type of information affected, a toll free number to contact the business and learn what type of information the business stored, and toll free contact numbers for credit reporting entities and the FTC.

4. Safe Harbor.

Generally, a business entity would be exempt from the Act's notice requirements if "a risk assessment conducted by or on behalf of the business entity concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach," and a the business entity notifies the FTC of the results of the risk assessment and that it decided to invoke the risk assessment.

This provision turns on the definition of "risk assessment." The legislation has provided guidance as to what the risk assessment must contain, but the guidance is primarily directed at entities that have a database component. It is also notable that this provision imposes a 30-day deadline on the submission of these risk assessments, unless an extension has been granted by the FTC.

5. Notice to Law Enforcement and Other Purposes.

The Act provides that the business entity must also notify the United States Secret Service, the FBI and the FTC for civil and law enforcement purposes if: (i) the number of individuals exceeds 5,000; (ii) the security breach involves a database, networked or integrated databases containing sensitive personally identifiable information of more than 500,000 people nationwide; (iii) the security breach involves databases owned by the federal government; or (iv) the security breach involves primarily sensitive personally identifiable information of individuals who are known to the business entity to be contractors to the federal government involved in national security or law enforcement.

The timing of this notice must be 72 hours before notification to any individuals or 10 days after the discovery of the events requiring notice, whichever comes first.

Notably, it appears that the role of reporting to individual state attorneys general (as now required by many states) will only be required if such entities register with the FTC.

6. Excluded Entities.

This proposed legislation does not apply to (i) business entities to the extent they are covered entities or business associates covered by the HITECH Act, and (ii) those business entities to the extent they act as vendors of personal health records or third parties service providers subject to that Act.

7. Preemption of State Laws.

Finally, the Act would supersede or preempt any provision of the law of any state or locality relating to the notification by any business engaged in interstate commerce of a security breach of computerized data.

We will continue to monitor the status of the Act as it proceeds before the various House and/or Senate committees for evaluation and amendment (as well as any other bills relating to breach notification), and will update this report as developments occur. Please feel free to contact us with any questions you may have.