Published on *The National Law Review* https://natlawreview.com

A Recently-Released "Discussion Draft" of the "American Data Privacy and Protection Act" Provides Insight into Recent Bipartisan Efforts to Pass Nationwide Privacy Law

Article By:

Brian G. Cesaratto

Patricia M. Wagner

Alaap B. Shah

Alexander J. Franchilli

As reported in a June 3, 2022 press release from the House Committee on Energy and Commerce, U.S. Representatives Frank Pallone, Cathy McMorris Rodgers, and Senator Roger Wicker released a "discussion draft" of a federal data privacy bill entitled the "American Data Privacy and Protection Act" (the "Draft Bill"), which would impact the data privacy and cybersecurity practices of virtually every business and not-for-profit organization in the United States.

As further described below, the Draft Bill's highlights include: (i) a comprehensive nationwide data privacy framework; (ii) preemption of state data privacy laws, with some exceptions; (iii) a private right of action after four (4) years, subject to the individual's prior notice to the Federal Trade Commission ("FTC") and applicable state attorney general before commencement of lawsuit; (iv) exemptions for covered entities that are in compliance with other federal privacy regimes such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Gramm-Leach Bliley Act ("GLBA") solely with respect to data covered by those statutes; (v) exclusions from Act's requirements for certain "employee data"; and (vi) a requirement for implementation of reasonable administrative, technical and physical safeguards to protect covered data. The Draft Bill would be enforced by the FTC, and violations treated as unfair or deceptive trade practices under the Federal Trade Commission Act, as well as by state attorneys general.

The press release and Draft Bill were released just days after rumors of a bipartisan consensus emerging in support of a federal comprehensive privacy bill. However, as reported by the Washington Post, the Draft Bill may stall without the support of Sen. Maria Cantwell, the chair of the Senate Commerce Committee, who supports more liberal priorities for online user rights. Nevertheless, the Draft Bill provides an informative glimpse into what a nationwide comprehensive federal privacy law may look like if it gains the needed support. The Draft Bill defines "Covered Entity" broadly, to include every entity or person subject to regulation of consumer protection laws under the FTC Act,

common carriers, and “an organization not organized to carry on business for their own profit or that of their members.”

In general, the Draft Bill outlines a comprehensive nationwide framework for data privacy of information that identifies or is linked or reasonably linkable to an individual or an individual’s device. It provides for, among other things, Covered Entities to minimize data collection and implement, and make available privacy policies; it permits individuals the right of access, correction, deletion, and portability of covered data; and it provides individuals with the right to opt out or object to the transfer of covered data. The framework would require affirmative consent for covered entities to collect or process “sensitive covered data,” such as, among other things, health-related information, biometric information, genetic information, precise geolocation information, or information relating to an individual’s race, ethnicity, national origin, or sexual orientation, subject to certain exceptions. Furthermore, certain data practices would be prohibited, including, among other things, the collection, processing, or transferring of social security numbers or nonconsensual intimate images, subject to exceptions.

The Draft Bill excludes certain employment-related data, or “employee data,” defined as (i) applicant information; (ii) business contact information; (iii) emergency contact information; and (iv) benefits related information. The bill suggests that employee personal information that falls outside the definition of excluded “employee data” is within the protections and individual rights provisions. The Draft Bill also contains carve outs for entities covered by and compliant with HIPAA and GLBA “solely and exclusively with respect to data subject to the requirements of such regulations, part, title or Act.”

Several provisions of the Draft Bill are particularly noteworthy, such as a prohibition on collecting or processing data in a manner than would discriminate on the base of race, color, national origin, gender, sexual orientation or disability. Additionally, the Draft Bill provides a private right of action for consumers alleging violations, with remedies such as injunctive relief, compensatory damages and reasonable attorneys’ fees. However, the private right of action would not be available until 4 years after the effective date, and would also be subject to procedural requirements, including notice to the FTC. Actions for injunctive relief would be subject to notice to the entity and a right to cure.

In addition, the Draft Bill provides that Covered Entities that develop an algorithm to collect, process or transfer covered data must evaluate the design of the algorithm to reduce the risk of disparate impact based on face, color, religion, national origin, gender, sexual orientation or disability. So called “Large Data Holders” with annual gross revenues in excess of $250 million or that collect covered data of more than 5 million individuals or devices or the sensitive data of more than 100,000 individuals or devices, would be required to conduct an annual impact assessment, including how it may mitigate potential harms to an individual.

The Draft Bill requires Covered Entities to implement cybersecurity practices including, at a minimum, assessment of vulnerabilities, preventative and corrective actions to mitigate any foreseeable risk or vulnerability (including changing business arrangements or operations, and cybersecurity training of employees), and disposal of covered data when it is no longer necessary for the purposes for which the data was collected, processed or transferred, absent individual affirmative express consent to retention. A Covered Entity that is in compliance with GLBA or HIPAA would be deemed compliant with respect to “any data covered by such information security requirements.”

The Draft Bill also contains broad preemption of any state law covered by its provisions, with exceptions including Illinois’ Biometric Information Protection Act (“BIPA”); “laws that govern the

privacy rights or other protections of employees, employee information, students, or student information”; generally applicable consumer protection laws; and laws addressing banking or financial records. State laws or regulations that address health information, medical information, medical records, HIV status or HIV testing would also not be preempted. The Draft Bill expressly preempts the California Consumer Privacy Act (“CCPA”) and California’s soon-to-be-effective California Privacy Rights Act (“CPRA”), with the exception of Section 1798.150 of the California Civil Code, which provides a private right of action for certain data breaches.

We will continue to monitor the developments as it relates to this Draft Bill and the ongoing efforts by lawmakers to pass a federal nationwide comprehensive privacy law.

National Law Review, Volume XII, Number 160