Federal Privacy Bill: Will the United States Enact Comprehensive Privacy Legislation?

Jul 18, 2022

Categories:

Blogs
Technology Blog

Authors:

Jean Paul Yugo Nagashima
Michael E. Nitardy

On June 21, the U.S. House of Representatives introduced a draft federal privacy bill named the American Data Privacy and Protection Act (ADPPA). This bill, if enacted, would bring more transparency and base-line data privacy protections to U.S. residents. Although the ADPPA is already facing challenges from industry groups and members of Congress, its introduction demonstrates the bipartisan interest to enact a federal data privacy law.

This article provides a brief overview of what businesses are covered by the ADPPA, their obligations under the law, certain exceptions to the law, the proposed enforcement mechanisms, and what rights are provided to individuals.

Who Must Comply with the ADPPA?

The ADPPA would apply to all persons engaged in commerce,[1] non-profit organizations,[2] and telecommunications carriers[3] that collect, process, or transfer certain data classified as "covered data." The law would also apply to their subsidiaries or affiliates.[4] Together, these organizations and persons would become the "covered entities." Covered entities may be a person running a business, a corporation or a non-profit if they collect, process, or transfer "covered data." This leads to the next question: what is covered data?

Covered data is information that identifies or is reasonably linkable to an individual.[5] It also covers "derived data" and "unique identifiers."[6] Derived data may be assumptions and conclusions reached about an individual from other sources of information, and unique data may be technical identifiers like Internet Protocol (IP) addresses and cookies.[7] Covered data, however, would not include employee data[8] (regardless of whether the employee is paid), de-identified data,[9] or publicly available information.[10]

What Are the Obligations of a Covered Entity?

ADPPA would obligate covered entities to establish certain data security practices and organizational measures. Covered entities would be required to establish, implement, and maintain reasonable administrative, technical and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.[11] As a related requirement, covered entities would have to exercise due diligence in selecting its service providers and deciding to transfer covered data to a third party.[12]

For organizational measures, covered entities would be required to designate one or more qualified employees as privacy officers and data security officers.[13] These officers would then implement a data privacy program and data security program and facilitate the covered entity's ongoing compliance with the ADPPA.[14] If enacted, this federal privacy law would require appointing a data privacy officer similar to the European Union's current General Data Protection Regulation (GDPR) requirements.

As part of its transparency obligation, covered entities would be required to provide a privacy policy describing their data collection, processing, and transfer activities. Similar to GDPR, the ADPPA requires covered entities to identify the data that is collected and the purpose of the collection.[15]

What Are Large Data Holders?

The ADPPA establishes a new category of covered entities called large data holders that would have to comply with additional requirements. Of course, not all covered entities would be classified as large data holders. The ADPPA adopts a framework similar to the California Consumer Privacy Act's "business" definition to define the scope of a large data holder. A large data holder is a covered entity that:

- had annual gross revenue of $250,000,000 or more; and
- collected, processed or transferred—

- the covered data of more than 5,000,000 individuals' devices that identify or are linked or reasonably linkable to 1 or more individuals; or
- the sensitive covered data of more than 100,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding any instance where the covered entity would qualify as a large data holder solely on account of processing—
    - personal email addresses;
    - personal telephone numbers;
    - log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity.[16]

The large data holder requirement contemplates the collection, processing, and transfer of "sensitive covered data" which is a special category of personal data defined in the ADPPA. In contrast to the GDPR, sensitive personal data covers:

- government issued identifiers such as social security number
- any information that reveals the health information of an individual
- financial information and security access information to such account
- biometric information
- genetic information
- precise geolocation that is reasonably linkable to an individual
- individual's private communications
- account or device log-in information
- information revealing an individual's race, ethnicity, national origin, religion, or union membership or non-union status
- information identifying sexual orientation or sexual behavior of an individual
- information identifying online activities over time across websites

- information stored on individuals' devices for private use
- visual media that shows the naked or undergarment-clad private area of an individual
- information identifying or revealing the extent or content of any individual's access or viewing or other use of television service, cable service, or streaming service
- information of an individual under the age of 17
- any other covered data collected, processed, or transferred for the purpose of identifying the data types from (1)-(16)[17]

The large data holder definition exempts covered entities that use email addresses or cell phone numbers as part of the account login information from becoming a large data holder.

What Are the Additional Obligations of Large Data Holders?

The ADPPA places a number of requirements on covered entities classified as large data holders. These additional requirements range from disclosure and reporting obligations to performing privacy impact assessments.

For their disclosure obligations, large data holders would be required to provide a short notice of their covered data practices that are readily accessible to an individual.[18] Large data holders would also be required to annually certify that they have reasonable internal controls to comply with the ADPPA and reporting structures in place to ensure that privacy and security officers would be involved in the decision making to comply with the ADPPA.[19]

Large data holders would also be required to provide additional authority to their privacy officers and/or data security officers. Large data holders would be required to provide one of these officers with the authority to report directly to the highest official of the large data holder as a privacy protection officer.[20] The privacy protection officer would be tasked to perform periodic reviews of privacy policies, regular and comprehensive audits, develop training programs, maintain clear compliance records, and serve as a contact point between the large data holder and enforcement authorities.[21]

Under the ADPPA, large data holders would also be required to conduct a privacy impact assessment biannually.[22] This assessment would weigh the benefits of the large data holder's covered data collecting practices against the potential adverse consequences to individual privacy.[23] Furthermore, any large data holder that uses an algorithm to collect or transfer covered data must conduct an algorithm impact assessment.[24] As required, the algorithm assessment would describe steps the large data holder has taken or plans to take to mitigate potential harms to an individual, especially in areas of race, religion, national origin, gender, sexual orientation, or disability.[25]

Are there Exceptions for Certain Industries to Comply with ADPPA?

The ADPPA provides exceptions to entities in an industry that must already comply with the privacy rules of certain laws. For example, a covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (GLBA), the Health Information Technology for Economic and Clinical Health Act (HITECH), part C of title XI of the Social Security Act (SSA), the Fair Credit Reporting Act (FRA), the Family Educational Rights and Privacy Act (FERPA), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) would be deemed to be in compliance with the ADPPA's related privacy requirements.[26] Similarly, covered entities that comply with the GLBA, HITECH, SSA, and HIPAA are deemed to be in compliance with the ADPPA's data security practices requirements for data already subject to those regulations.[27]

Enforcement of the ADPPA

The ADPPA would provide the Federal Trade Commission (FTC) and the State Attorney Generals the authority to enforce compliance against covered entities.[28]

The ADPPA also would provide a private right of action to individuals.[29] However, the ADPPA would require specific procedures for individuals to follow before filing suit, making it a

difficult option to pursue. For example, individuals must first notify the state attorney general of their intent to file suit, and the state attorney general will then have 60 days to determine whether to independently seek action.[30] In addition, any communication for monetary payment that is sent to the covered entity is deemed to have been made in bad faith if (a) the communication is sent before the 60-day determination period by the state attorney general or (b) the attorney general made the determination to independently seek action.[31] Even if the attorney general does not seek action, an individual must notify the covered entity, at which point the covered entity is provided 45 days to cure its violation under the ADPPA.[32]

What Rights Are Provided to Individuals?

The ADPPA would also afford certain access rights to individuals. Similar to state data privacy laws, these include the right to: (1) access the covered data collected on the individual's behalf, (2) correct any inaccuracies of the individual's personal data, (3) delete covered data obtained about the individual, (4) notify any third party or covered entity to which the covered entity transferred such covered data of the individual's deletion request, (5) opt-out of covered data transfers and targeted advertising, (6) express consent is needed to collect, process, transfer an individual's sensitive covered data.[33]

Covered entities would be required to respond to individuals' requests within 60 days of verification.[34] Large data holders have a shorter deadline. They must respond to these requests within 30 days of the request being verified.[35]

Conclusion

The long-awaited, bipartisan federal privacy bill has received mixed reception from different industries and from certain members of Congress. For example, the U.S. Chamber of Commerce has opposed the bill for the inclusion of an individual's private right of action. In Congress, Senator Maria Cantwell (D-WA) also expressed her opposition to the bill, noting "major enforcement loopholes."[36]

We will continue to follow any developments concerning this bill.

For more information, please contact the authors or any other member of Frost Brown Todd's Privacy & Data Security practice group.

**Summer Associate Grace Kuntz contributed to this article.*

---

[1] The ADPPA states that it is a person subject to the Federal Trade Commission Act. *See* H.R. 8152. Sec. 2(9)(A)(i).
[2] An organization not organized to carry on business for their own profit or that of their members. H.R. 8152. Sec. 2(9)(A)(iii).
[3] A common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended. H.R. 8152. Sec. 2(9)(A)(ii).
[4] H.R. 8152. Sec. 2(9)(B).
[5] H.R. 8152. Sec. 2(8)(A).
[6] *Id.*
[7] H.R. 8152. Sec. 2(11); H.R. 8152. Sec. 2(31).
[8] Employee data covers (1) information relating to a perspective employee collected by a covered entity, (2) the business contact information of an employee, (3) an emergency contact information collected by an employer that relates to an employee, and (4) information relating to an employee that is necessary for the employer to collect. *See* H.R. 8152. Sec. 2(8)(C).
[9] Under the ADPPA, de-identified data requires more than the information just to be unlinked or reasonably unlinked to an individual or device. It also requires the covered entity to take the following action to ensure that the information is de-linked:

- Take reasonable measures to ensure that the information cannot, at any point, be used to re-identify any individual or device;
- Publicly commit in a clear and conspicuous manner to:
  - to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and
  - to not attempt to re-identify the information with any individual or device; and

- Contractually obligate any person or entity that receives information from the covered entity to comply with taking reasonable measures publicly committing to transfer the information in de-identified form and not attempt re-identification. R. 8152. Sec. 2(10).

[10] The ADPPA defines publicly available information relatively broadly. Publicly available information is any information that a covered entity has a reasonable basis to believe it has been lawfully made available to the general public from (a) government records, (b) widely distributed media, (c) a website or online service made available to all members of the public for free, (d) disclosures made to the public as required by law. H.R. 8152. Sec. 2(21).
[11] H.R. 8152. Sec. 208(a)(1).
[12] H.R. 8152. Sec. 302(c)(1).
[13] H.R. 8152. Sec. 301(c)(1).
[14] H.R. 8152. Sec. 301(c)(2).
[15] H.R. 8152. Sec.202(b)(1)(3).
[16] H.R. 8152. Sec. 2(17).
[17] H.R. 8152. Sec. 2(22).
[18] H.R. 8152. Sec. 202(e).
[19] H.R. 8152. Sec. 301(a)(1)-(2).
[20] H.R. 8152. Sec. 301(a)(3).
[21] H.R. 8152. Sec. 301(a)(3)(A)-(E).
[22] H.R. 8152. Sec. 301(d)(1).
[23] *Id.*
[24] H.R. 8152. Sec. 207(c)(1).
[25] H.R. 8152. Sec. 207(c)(1)(B)(i)-(iv).
[26] H.R. 8152. Sec. 404(a)(2).
[27] H.R. 8152. Sec. 404(a)(3).
[28] H.R. 8152. Sec. 401(c)(2)(A); H.R. 8152. Sec. 402(a).
[29] H.R. 8152. Sec. 404(a)(1).
[30] H.R. 8152. Sec. 404(a)(3)(A).
[31] H.R. 8152. Sec. 404(a)(3)(B).
[32] H.R. 8152. Sec. 404(c)(1)-(2).
[33] H.R. 8152. Sec. 203(a)(1)-(4).
[34] H.R. 8152. Sec. 203(b)(1)-(3).
[35] H.R. 8152. Sec. 203(b)(1)-(3).

[36] Cristiano Lima, *Top Senate Democrat Casts Doubt On Prospect of Major Data Privacy Bill* https://www.washingtonpost.com/technology/2022/06/22/privacy-bill-maria-cantwell-congress/ (Jun. 22, 2022).

FBT Gibbons