American Data Privacy and Protection Act (H.R. 8152): Summary & Initial Analysis of Nonprofit Impact

Major Elements of the ADPPA

The American Data Privacy and Protection Act (ADPPA) is a bipartisan, bicameral national comprehensive data privacy and security proposal. The Act establishes a national standard to protect consumer data privacy, imposes obligations on covered entities, and allows for federal, state, and individual enforcement. The Federal Trade Commission (FTC) is designated as the regulator to enforce the bill at the federal level. Reps. Pallone (D-NJ), Rodgers (R-WA), Schakowsky (D-IL), and Bilirakis (R-FL) introduced H.R. 8152 on June 21, 2022. On July 20, 2022 the bill passed the House Energy and Commerce Committee by a vote of 53-2.

Who is covered: The bill would apply to most entities, including nonprofits and common carriers. "Large data holders" that meet certain thresholds and service providers that use data on behalf of other entities, would face different or additional requirements. "Large data holders" would be defined as organizations (1) with more than $250 million in gross annual revenue in the prior calendar year, and (2) which processed covered data of more than 5 million individuals or the sensitive covered data of more than 100,000 individuals.

As mentioned above, small- and medium-size businesses that meet certain size and data-collection thresholds would be exempt from several requirements, such as being allowed to respond to a consumer's request to correct their data by simply deleting the data rather than correcting it. They are also exempt from most of the bill's data security requirements.

What sorts of data are covered: The bill applies to information that "identifies or is linked or reasonably linkable" to an individual, including derived data and unique identifiers. That definition covers a wider universe of data than the privacy laws of Connecticut, Colorado, Utah, Connecticut, and (arguably) California, *Reuters* has reported.

Restrictions and duties: The bill would prohibit covered entities from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual, unless the collection, use, or disclosure is one of 17 permissible purposes specified by the bill. Service providers may only collect or process covered data for the purposes directed by the covered entity, and must assist covered entities in fulfilling requests by individuals to exercise their data rights.

1602 L Street NW, Suite 900
Washington, DC 20036
Phone: 202-467-6100
Email: info@independentsector.org

The ADPPA also would create special protections for 16 categories of "sensitive covered data." Among other requirements, covered entities would have to get a consumer's affirmative, express consent before transferring their sensitive covered data to a third party, unless a specific exception applies. "Sensitive covered data" includes information such as government identifiers, social security numbers and drivers' license numbers; any information about an individual under the age of 17; sensitive categories such as health, geolocation, financial, log-in, racial, and sexual information; and private communications, personal digital media such as photos and videos, and web-browsing activity over time and across websites. Conversely, de-identified data, employee data and publicly available information are specifically excluded.

The bill also requires large data holders to conduct a privacy impact assessment biannually, like the European Union's influential General Data Protection Regulation (GDPR), but with a wider scope. The bill would also prohibit entities from collecting, processing, or transferring covered data in a manner that discriminates based on race, color, religion, national origin, gender, sexual orientation or disability.

Covered entities would have to adopt *data security practices* and procedures (as promulgated by the FTC) that are reasonable in light of the entity's size and activities, including a requirement to protect covered data against unauthorized use or acquisition, including implementing practices to identify vulnerabilities, test systems and provide employee training.

Within one year of the ADPPA becoming law, the CEO or highest-ranking officer, along with each privacy officer and data security officer at a large data holder must certify with the FTC by showing that "reasonable" controls are in place to comply with the ADPPA and that reporting structures are in place so certified officers are involved in decisions regarding compliance with the law.

Transparency: The bill would require covered entities to disclose, among other things, the type of data they collect, what they use it for, how long they retain it, and whether they make the data accessible to the People's Republic of China, Russia, Iran, or North Korea.

Right of control and consent: Consumers would have various rights over covered data, including the right to access, correct, and delete their data held by a particular covered entity. Covered entities would also have to give consumers an opportunity to object before the entity transfers their data to a third party or targets advertising toward them. Entities would be responsible for informing third parties to make changes to the data of users who have chosen to correct or delete it. Significantly, the ADPPA may require the consent of a user to use their internet search or browsing history for purposes of targeted advertising.

1602 L Street NW, Suite 900
Washington, DC 20036
Phone: 202-467-6100
Email: info@independentsector.org

Children under 17: The bill would create additional data protections for individuals under age 17, including a prohibition on targeted advertising, which would only apply when the covered entity knows the individual in question is under age 17. Certain social media companies or large data holders would be deemed to "know" an individual's age in more circumstances. Furthermore, any data about an individual under age 17 is considered "sensitive covered data", and cannot be shared with a third party unless the organization receives affirmative consent from the minor or their guardian, or unless it is being used to prevent imminent injury.

Data brokers: The bill would create specific obligations for third-party collecting entities whose main source of revenue comes from processing or transferring data that they do not directly collect from consumers (e.g., data brokers). These entities would have to comply with FTC auditing regulations and, if they collect data above the threshold amount of individuals or devices, would have to register with the FTC. The FTC would establish a searchable public registry of third-party collecting entities and a "Do Not Collect" opt-out mechanism by which individuals could request that all registered entities refrain from collecting covered data relating to them.

Use of algorithms: The bill would prohibit most covered entities from using covered data in a way that discriminates based on protected characteristics such as race, gender, or sexual orientation. Large data holders would have to conduct "algorithm impact assessments" describing their steps to mitigate potential harms resulting from such algorithms, and would have to submit the assessments to the FTC and make them available to Congress on request. This feature is a new obligation that is not included in the major state data privacy laws.

Enforcement: The bill would be enforceable by the FTC, under the agency's existing enforcement authorities, and by state attorneys general and state privacy authorities in civil actions. The FTC would have to establish a new Bureau of Privacy.

Private right of action: Before bringing a suit for injunctive relief or a suit against a small- or medium-size business, individuals would be required to give the violator an opportunity to address the violation. The bill also would render pre-dispute arbitration agreements or joint-action waivers with individuals under the age of 18 unenforceable in disputes arising under the ADPPA.

Minimal "Duty of Loyalty". While the ADPPA has various requirements that are classified under a "Duty of Loyalty" in Title I, its version of such a duty would impose a data minimization requirement and define several specific prohibited data practices. It does not broadly prohibit providers from acting in ways that could harm individuals, as called for by some Democrats.

1602 L Street NW, Suite 900
Washington, DC 20036
Phone: 202-467-6100
Email: info@independentsector.org

Preemption of state laws: The bill would generally preempt any state laws that are "covered by the provisions" of the ADPPA or its regulations, although it would expressly preserve state laws that fall into 16 categories, including consumer protection laws of general applicability, data breach notification laws, and laws on civil rights, student and employee privacy and financial and health records.

However, the ADPPA also would preserve several specific state laws, such as Illinois' Biometric Information Privacy Act and Genetic Information Privacy Act and California's private right of action for victims of data breaches. Specific statutes on civil rights, student and employee privacy, criminal codes, and financial and health records would also be excluded from federal pre-emption. States would retain the ability to pass future laws limiting the collection and use of facial recognition data, and to regulate other activities and sectors, such as wiretapping, health care and banking.

Considerations for Nonprofits

1) Nonprofits are explicitly covered by the legislative text. The bill's definition of a "covered entity" reads:

> (A) IN GENERAL.—The term ''covered entity''—
> (i) means any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and—
> (I) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.);
> (II) is a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; or
> (III) is an organization not organized to carry on business for its own profit or that of its members; and
> (ii) includes any entity or person that controls, is controlled by, or is under common control with the covered entity.

2) Impact may vary based on size. Many individual nonprofits would likely not be in the category of "large data holders" established by the bill that would face the most stringent duties and restrictions. Some nonprofits would fall within the bill's "small business exemption" defined in Section 209:

- Have annual gross revenue below a certain threshold (the bill proposes $41 million) for each of the prior 3 years;
- Not process the data of more than 200,000 individuals; and
- Not derive more than 50% of its revenue from transferring covered data.

1602 L Street NW, Suite 900
Washington, DC 20036
Phone: 202-467-6100
Email: info@independentsector.org

These data holders would be exempt from the requirement to make data corrections at the individual's request. Those organizations would be allowed to simply delete the data. Small data holders would also be exempt from most of the bill's data security practice requirements, except for the requirement to delete data that is no longer necessary.

3) Concerning barriers to information sharing between nonprofits, including federated networks. Because separate organizations within the same national network are considered "third parties", the current text would limit the ways that these organizations can share data between national and local organizations. This is especially true for youth-serving organizations, as any data about individuals under age 17 is considered "sensitive covered data" and cannot be shared within a network without affirmative consent. Data sharing is critical because many of these national organizations centralize program or fundraising data collection under one system, to increase efficiency and ease of local affiliates.

These limitations could impact nonprofits beyond federated networks as well. For example, organizations that share information because they serve the same mission area, region, or client population may also be constrained.

4) The ADPPA would be a shift from existing comprehensive data privacy laws because it explicitly includes nonprofit organizations. The International Association of Privacy Professionals has said that because the Federal Trade Commission's primary jurisdiction applies to matters "in or affecting commerce," most nonprofit organizations have previously been considered exempt from FTC consumer protection enforcement. Although some state-level "mini-FTC" acts apply to nonprofits, many comprehensive state-level data privacy laws specifically exempt nonprofits from their requirements.

Outlook for the Legislation

While the ADPPA has advanced farther than any previous legislative attempt to regulate data privacy on the federal level, including a strong bipartisan vote in the House E&C Committee, *serious hurdles remain in front of the legislation in the short term*, including the opposition of Speaker Pelosi to the bill in its present form and the opposition of Senate Commerce Committee Chairman Maria Cantwell (D-WA). If no resolution is reached after the election, the bill will expire at the end of the year. The bill's prospects next year would be affected by the make-up in Congress as well as the likely departure of key supporter Sen. Roger Wicker (R-MS) from the top spot on the Senate Commerce to serve as top Republican on the Armed Services Committee. Even if the legislation does not advance this year, its significant bipartisan support makes it a potential starting point for future attempts, and the nonprofit sector would be wise to engage thoughtfully with it now.

1602 L Street NW, Suite 900
Washington, DC 20036
Phone: 202-467-6100
Email: info@independentsector.org