Changes Made in the AINS to the American Data Privacy and Protection Act (HR 8152)

July 19, 2022

Below is a list of the most significant changes in the American Data Privacy and Protection Act (ADPPA):

- The requirements for affirmative express consent have been clarified to ensure covered entities offering products or services through nontraditional devices such as cars may effectively and practically obtain individuals consent and to require separate consent for each processing purpose that covered data is used for.
- Required information and other functionalities, such as opt-out mechanisms, are now required throughout the bill to be readily accessible to those with disabilities.
- The definition of "employee data"–which is not regulated as covered data under the Act–now includes information used solely for professional activities on behalf of the business.
- Important technical changes to the definitions of "covered entity" and "service provider" close an unintended exception and make clear that entities acting on behalf of government entities to provide services using covered data remain subject to the Act.
- The ADPPA still bans targeted ads to and treats all information relating to individuals under 17 as sensitive covered data, but it now has a tiered approach to what constitutes "knowledge" that an individual is under 17:
    - Constructive Knowledge (knew or should have known) applies to "Covered High-Impact Social Media Companies" with platforms primarily used by individuals for user-generated content, at least $3 billion in annual revenue, and 300 million monthly active users for 3 of the prior 12 months.
    - Knew or Acted in "Willful Disregard" of an individual's age applies to all Large Data Holders, including service providers.
    - Actual Knowledge applies to the remaining smaller covered entities and service providers.
- The scope of video data considered sensitive covered data is clarified to include information showing the video content requested or selected by users of consumer-generated media.
- The categories of sensitive covered data are expanded to include race, color, ethnicity, religion, union membership, and internet browsing history over time and across third party websites or online service.
- The California Privacy Protection Agency is expressly included as a State Privacy Authority with the power to enforce the Act with respect to the State of California.
- The definition of "third party" now clearly establishes that affiliated companies are considered a single covered entity if consumers reasonably expect them to share information with one another.
- The list of permissible purposes for reasonably necessary and proportionate covered data use in section 101(b) now includes a few new purposes to more closely reflect what is required in certain contexts

- Section 104 has been overhauled to make clear that covered entities may not retaliate against anyone for exercising their rights under the Act by denying goods or services, charging different prices, or otherwise making people "pay for privacy" while still allowing businesses to offer bona fide loyalty programs like rewards, premium features, discount or club cards.
- A new exception to individual rights requests ensures that private schools do not have to delete student records that would unreasonably interfere with their ability to operate and provide education services.
- Section 203 establishes new timelines for when different types of covered entities must respond to a verifiable request from an individual exercising their rights under the section.
- All large data holders must annually compile and publicly disclose metrics of requests and responses from individuals exercising their rights to access, delete, and opt-out of data transfers and targeted advertising.
- The algorithmic impact assessments and evaluations required by large data holders now apply when such algorithms pose a consequential risk to an individual or individuals.
- The FTC may now establish or recognize unified opt-out mechanisms, including tools offered by businesses, to allow individuals to exercise their opt-out rights from targeted ads, transferring covered data to third parties, and deleting data held by and preventing future collection by data brokers. Additional requirements on these mechanisms also ensure consumers and businesses can effectively use and comply with the requirements.
- All entities that do not meet the small and mid-size criteria rather than just large data holders must now conduct annual privacy impact assessments.
- The federal and state enforcement provisions have been updated so that:
    - If the FTC brings an enforcement action, state enforcement authorities follow existing and well-established law as specified in the Federal Rules of Civil Procedure regarding their right to intervene.
    - State enforcement agencies may only intervene with regard to the interests of residents of their particular state.
    - State enforcement agencies, including the California Privacy Protection Agency, have the right to bring regulatory or administrative enforcement actions for ADPPA violations as well as of non-preempted state laws.
- The private right of action provisions have been updated so that:
    - Private enforcement begins 2 years after the effective date, not 4 years.
    - New provisions add clarity that private suits do not limit the ability of the FTC or state enforcement agencies from later commencing an action or intervening in an action.
    - Prohibitions on pre-dispute arbitration have been expanded to include any dispute involving claims related to gender or partner-based violence or physical harm and Pre-dispute joint action waivers are no longer referenced .
    - The limited right to cure has been clarified to apply to individual claims rather than entire suits and to require the entity being sued show a court it has cured the alleged violation.

    - The demand letter requirement no longer risks individuals losing their rights over a technicality while still ensuring federal and state regulators have 60 days to address a claim.
    - Very small businesses – those who have an annual revenue of less than $25 million, engage with the covered data of less than 50,000 individuals, and earn less than half their revenue from transferring covered data – are no longer subject to private enforcement.
- The preemption provisions have been updated so that:
    - The California Privacy Protection Agency has express authority to enforce the ADPPA in the same manner as it would otherwise enforce the California Consumer Privacy Act.
    - FCC and FTC privacy authorities are harmonized to establish regulatory parity for FCC-regulated entities and ensure consumer privacy rights are not lessened by the ADPPA while ensuring the FTC has sole federal authority in taking any actions to enforce the Act.
    - The list of existing federal laws where compliance with related requirements would establish compliance with the related ADPPA provisions has been expanded and clarified, including limiting the application of FERPA to schools defined under that law and related regulations.
    - State laws regarding the use of encryption as a means of providing data security are specifically protecting.
    - State laws pertaining to public health activities, reporting, data, or services are specifically protected.