State Data Privacy and Protection Act

Background

The State Data Privacy and Protection Act is based on a bipartisan bill proposed in Congress in 2022, the American Data Privacy and Protection Act (“ADPPA”). The bill went through extensive negotiations between members of Congress of both parties, industry, civil rights groups, and consumer protection and privacy groups. The ADPPA received overwhelming bipartisan support in the House Energy & Commerce Committee, where it was favorably approved on a 53-2 vote. Unfortunately, Congress failed to enact ADPPA, but state legislators can now take advantage of the outcome of those negotiations by modeling a state bill on the bipartisan consensus language in ADPPA. The State Data Privacy and Protection Act provides that opportunity.

Key Provisions

- **Data minimization:** Establishes limits on the unfettered processing of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual (or pursuant to certain enumerated purposes.)
- **Strict restrictions on sensitive data collection and use:** Sets heightened protections for collection and use of sensitive data (i.e., biometrics, geolocation, health data), which is only permitted when strictly necessary and not permitted for advertising purposes.
- **Civil Rights:** Extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, or disability.
- **Cross-context behavioral advertising prohibited:** The collection, use, and transfer of information identifying an individual’s online activities over time and across third party websites and services is strictly limited and cannot be used for advertising.
- **Protections for children and teens:** Prohibits targeted advertising to minors under age 17. Covered entities may not transfer the personal data of a minor without the express affirmative consent of the minor or the minor’s parent. Personal data of minors is considered “sensitive data.” These additional protections would only apply when the covered entity *knows* the individual in question is under age 17, though the standard for certain high-impact social media companies is “known or should have known,” and for large data holders is “knew or acted in willful disregard of the fact that the individual was a minor.”

State Data Privacy and Protection Act

- **Algorithmic fairness and transparency:** Requires covered entities (who are not small businesses) to conduct algorithmic impact assessments, which include mitigation measures to avoid potential harms from the algorithms. Entities must also conduct algorithm design evaluations prior to deployment in some instances. The assessments and evaluations must be submitted to the Attorney General. A summary must be posted publicly.
- **Data security:** Requires entities to adopt reasonable data security practices and procedures that correspond with an entity's size and activities, as well as the sensitivity of the data involved.
- **Manipulative design restrictions:** Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns). Prohibits deceptive advertising.
- **Individual Rights:** Gives consumers the rights to access, correct, and delete personal information about them. Consumers also have the right to opt out of both data transfers to third parties and targeted advertising. Also requires the Attorney General to recognize, and entities to honor, global opt-out mechanisms.
- **Service Providers:** Establishes requirements for service providers handling personal data, including a prohibition on commingling data from multiple covered entities. Service providers can only collect, process, and transfer data to the extent necessary and proportionate to provide service requested by covered entity.
- **Data Brokers:** Data Brokers must register with the Attorney General. The AG will create a public registry of data brokers.
- **Small business protections:** Small businesses (as defined) are exempt from compliance with many provisions of the Act.
- **Executive responsibility:** An executive must personally certify each entity’s compliance with the Act.
- **Enforcement:** A State Attorney General, District Attorney, or City Corporation Counsel may bring cases in court for injunctive relief, to obtain damages, penalties, restitution, or other compensation, and to obtain reasonable attorney’s fees and other litigation costs.
- **Private Right of Action:** Individuals may enforce their rights under the Act by bringing a case against a covered entity seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney’s fees and litigation costs. This right applies to only certain provisions of the Act. Small businesses are exempt from this provision.
- **Rulemaking:** The Attorney General is empowered to issue regulations for purposes of carrying out the Act.

State Data Privacy and Protection Act Differences from ADPPA

Background

The State Data Privacy and Protection Act is based on a bipartisan bill proposed in Congress in 2022, the American Data Privacy and Protection Act ("ADPPA"). This one-pager describes any changes that were made from ADPPA and the rationale for those changes.

Changes from ADPPA

- **First party and third party definitions:** The definition of first party advertising and marketing was changed to clarify the difference between first and third parties, and the third party definition was also changed for clarity.
- **Biometric information definition:** Makes a clarification to the biometric information definition to ensure that the use of face printing to identify demographics such as race and gender falls under the sensitive data protections, even if it is not used to identify a particular individual.
- **Closes loopholes in permissible purposes for data collection and use:** Clarifying language was added to the permissible purpose that allows covered entities to use covered data to prevent, detect, protect against, or respond to fraud or illegal activity – the change makes clear that that collection for this purpose only applies if the fraud or illegal activity is targeted at the covered entity itself.
- **Removes unclear government service provider exception**: Removes a confusing exemption from the data minimization rule for government service providers. Other provisions in the Act already govern processing by service providers, including government service providers.
- **Data collection to promote civic engagement allowed:** Permits groups promoting civic engagement to collect data necessary for that purpose by adding a permitted purpose to the data minimization provisions.
- **Strengthens the non-retaliation and loyalty program language**: The provisions permitting covered entities to operate bona fide loyalty programs was updated to ensure that such programs are not used to transfer vast personal data to data brokers. The language added is substantively equivalent to language negotiated between business groups in Washington State and consumer advocates in 2022. Language from the California Consumer Protection Act protecting individuals from differential pricing that is unjust, unreasonable, coercive, or usurious in nature was also added.

State Data Privacy and Protection Act Differences from ADPPA

- **"Do Not Collect" system requirements removed**: To reduce the burden on state Attorneys General, the provisions requiring the creation of a "Do Not Collect" system where individuals can send a request to data brokers to opt-out of collection by such entities was removed.
- **Expands the requirement to conduct algorithmic impact assessments to all covered entities except small businesses:** The original provisions limiting the requirement to conduct algorithmic impact assessments to large data holders would have allowed startups creating potentially harmful algorithms to build their algorithms without doing critical assessments. The amended language still exempts small businesses from these requirements.
- **Gives the Attorney General rulemaking authority re: algorithmic assessments:** In order to allow the law to keep pace with future technology, rulemaking authority was added to allow the AG to require additional information in algorithmic impact assessments and algorithmic design evaluations. The AG may also require covered entities to establish a process to ensure audits are thorough and independent, and may exempt algorithms that present low or minimal risk of harm.
- **Places contract requirements between covered entities and third parties:** New provisions were added requiring a contract between covered entities and third parties prior to any transfers of covered data between the parties.
- **Compliance programs that would be difficult to administer at state level removed:** Provisions from ADPPA that would have required federal regulators to establish technical compliance programs and compliance guidelines, as well as to report on digital content forgeries were removed to alleviate regulatory burdens on state regulators.
- **Private Right of Action updated to exempt small businesses**: Individuals may not bring suit against small businesses.
- **Preemption language cut since not relevant at the state level**: ADPPA would have preempted certain types of state laws covered by the provisions of the Act, but that is not relevant in a state bill and therefore those provisions were cut.
- **Grants rulemaking authority to the Attorney General**: State Attorneys General have been granted rulemaking authority to address issues that would have been addressed by the Federal Trade Commission under the ADPPA, whether via rules or guidance. This will allow the law to adapt to changes in future technology.