American Data Privacy and Protection Act

Background

The United States faces a data privacy crisis. For more than two decades, without any meaningful restrictions on their business practices, powerful technology companies have built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit. Through a vast, opaque system of databases and algorithms, we are profiled and sorted into winners and losers based on data about our health, finances, location, gender, race, and other personal characteristics and habits. The impacts of these commercial surveillance systems are especially harmful for marginalized communities, fostering discrimination and inequities in our society.

The **American Data Privacy and Protection Act** would force changes to the abusive data practices driving commercial surveillance and online discrimination.

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 sensitive data collection and use (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." Establishes a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC).

American Data Privacy and Protection Act

- **Algorithmic fairness and transparency:** Requires large data holders to conduct algorithmic impact assessments, which must describe steps they have taken or will take to mitigate potential harms from their algorithms. All entities that develop an algorithm designed to make consequential decisions must conduct an algorithm design evaluation prior to deployment. The assessments and evaluations must be submitted to the FTC, and, upon request, to Congress. 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 FTC to establish, 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 (“Third Party Collecting Entities”) must register with the FTC. The FTC will create a national registry of data brokers so that individuals can find them and exercise their rights, and a "Do Not Collect" mechanism by which individuals can request that all registered entities refrain from collecting their personal data.
- **Executive responsibility:** An executive must personally certify each entity’s compliance with the Act.
- **Enforcement:** The law provides for three-tier enforcement by a new Bureau of Privacy at the FTC, by state attorneys general and privacy authorities, and (for some provisions of the Act) by individuals via a private right of action.
- **Preemption:** No state would be permitted to enforce provisions of law covering the provisions in the Act, and existing provisions of law that cover those issues would be superseded. But state laws that are not “substantially subsumed” by the Act would still be in force. And there are many significant exceptions to preemption, including for general consumer protection laws, civil rights laws, and provisions concerning facial recognition, criminal law, or electronic surveillance. The Act establishes a consistent standard for comprehensive consumer privacy regulations in the United States, but does not preempt all state laws in the “field” of privacy. States would retain power to enforce current laws and enact new laws that address issues not “substantially subsumed” by the Act or within one of the savings provision categories.