The federal government has been trying to reach a consensus on data privacy and thus far has failed to pass legislation. On June 3, 2022, a bipartisan draft bill, titled the American Data Privacy and Protection Act was released by the Committee on
Energy and Commerce. The bill intends to provide comprehensive data privacy legislation, including the development of a uniform, national data privacy framework and robust set of consumer privacy rights.

A covered entity for purposes of the draft bill is defined as “any entity or person that collects, processes, or transfers covered data” and is subject to the Federal Trade Commission Act, is a common carrier under the Communications Act of 1934, or is an organization not organized to carry on business for their own profit or that of their members.

Per the draft, the new act would be carried out by a new bureau within the Federal Trade Commission (FTC). Interestingly, the proposed legislation would preempt similar state laws, though excludes the CCPA/CPRA in California and the BIPA and the GIPA in Illinois from that preemption.

The draft bill covers a wide swath of data consumer privacy issues from data collection to civil rights and algorithms. The following are some highlights of note:

**Data Collection Requirements**

The draft legislation imposes a duty on all covered entities not to unnecessarily collect or use covered data with covered data being defined broadly as “information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals, including derived data and unique identifiers”. The FTC would be charged with issuing additional guidance regarding what is reasonably necessary, proportionate, and limited for purposes of collecting data.

Covered entities would have a duty to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data. Further, covered entities would be required to provide individuals with privacy policies detailing data processing, transfer, and security activities in a readily available and understandable manner. The policies would need to include contact information, the affiliates of the covered entity that it transfers covered data to, and the purposes of each category of covered data the entitled collects, processes, and transfers.

Covered entities would be prohibited from conditioning or effectively conditioning the provision or termination of services or products to individuals by having individuals waive any privacy rights established under the law.

There would be additional executive responsibility for large data holders, including requiring CEOs and privacy officers to annually certify that their company maintains reasonable internal controls and reporting structures for compliance with the statute.

**Individual Rights Created**

Individuals would be granted the right to access, correct, delete, and portability of, covered data that pertains to them. These are similar to many of the rights California residents have under the CCPA/CPRA. The right of access would include obtaining covered data in a human-readable and downloadable format that
individuals can understand without expertise, the names of any other entities the data was transferred to, the categories of sources used to collect any covered data and the purposes for transferring the data.

Sensitive covered data, which includes items such as an individual’s health diagnosis, financial account information, biometric information, and government identifiers such as social security information, among other items, is prohibited from data collection without the individual’s affirmative consent.

Civil Rights and Algorithms

Unsurprisingly, algorithms, which were recently addressed by the EEOC and DOJ in guidance are also addressed in this draft legislation. Under the proposed legislation, covered entities may not collect, process, or transfer data in a manner that discriminates based on race, color, religion, national origin, gender, sexual orientation, or disability. This section of the law would require those large data holders that use algorithms to assess their algorithms annually and submit annual impact assessments to the FTC.

Jackson Lewis P.C. © 2022