CLIENT ALERTS & INSIGHTS

Proposed Federal Data Protection Law Would Impose Duty of Loyalty and Allow Limited Private Right of Action

JULY 5, 2022

Authors: Megan C. Parker

The proposed law-which is broadly applicable to most entities doing business in the United States-is the first real indication of bipartisan movement on data protection at the federal-level.

The House Committee on Energy & Commerce recently began the formally legislative process for the American Data Privacy and Protection Act ("**ADPPA**"), which-if passed-would represent the United States' first omnibus federal privacy law. The ADPPA will receive a full House Committee vote sometime in July, representing the first test of its viability.

This is yet the latest indication that the federal government is moving to regulate data protection more broadly in a possible shift away from the sectoral approach and patch work system of data protection laws that has dominated the federal government approach for decades.

The shift is both a reaction to the exponential growth of data technology and businesses over the past 20 years, but also the pace at which individual states are enacting data protection laws. For example, California, Colorado, Connecticut, Utah, and Virginia have passed different data protection laws in the past two years. California, Colorado, and Virginia's new laws come into effect in January 2023. The ADPPA, as currently drafted, would preempt all of the foregoing laws except for small portions of the California Privacy Rights Act ("**CPRA**").

While the legislative process is underway, the road to passage for the ADPPA is murky with midterm elections fast approaching in November and a lack of support from Senate Democrats.

However, analyzing the proposed ADPPA gives valuable insight into (1) the areas of data protection the federal government will focus on (i.e., data minimization and consumer rights), (2) how broad of a scope any such law may have, (3) how such a federal law would deal with inconsistent state law (i.e., preemption), and (4) how the federal government would enforce such a law (i.e., through the FTC, state attorney generals, and a limited private right of action).

Scope and Applicability

An entity falls within the scope of the ADPPA if it is a "covered entity" that collects and/or uses "covered data."

A "covered entity" includes any entity or person that collects, process, or transferred covered data, and that meets one of the following: (1) is subject to the Federal Trade Commission Act; (2) is a common carrier under the Communications Act; or (3) is a non-profit. The covered entity status flows through to any affiliated or related (i.e., using common branding) entities of a covered entity.

This definition casts a wide net and includes any businesses partaking in "commerce" within the U.S. by making reference to the FTC, specifically calls out those businesses that transport goods of people, and also goes further than state data protection laws by including non-profits in the scope of the ADPPA.

Accordingly, "covered data" is broadly defined to include any information that identifies or is linked or is reasonably linkable to an individual or a device that identifies or is linked or is reasonably linkable to one or more persons; including any data derived from any such information and any unique identifiers created from such information. This last category of covered data-"unique identifiers"-is broad enough to include IP addresses, cookies, targeted advertising identifiers, and other sorts of tracking technologies that some third party service providers might insist are "non-identifying" but that are otherwise considered identifying under the ADPPA, and also already considered personal data under existing state and international laws.

This broad definition largely tracks with the broad definitions of "personal data" and "personal information" that businesses have grown accustomed to under the GDPR and U.S. state laws.

Covered data *does not* include de-identified data, publicly available information, or employee data (which generally includes any information derived out of the employment context). The exclusion of employee data aligns with more recent state data protection laws and goes further than the CPRA. The CPRA's employee data exemptions sunset on January 1, 2023.

Taken together, the ADPPA would have a broad impact across all sectors of the economy, regulating any for-profit, or non-profit, engaged in commerce that handles any data that does, or is reasonably capable, of identifying an individual.

Large Data Holder

The ADPPA, similar to the EU's proposed Digital Services Act, sets forth an enhanced category of entity that is subject to further regulation: large data holders.

A large data holder means any covered entity that (in the previous calendar year): (1) had an annual gross revenue of $250 million or more; (2) and collected, processed, or transferred (a) the covered data of more than 5 million individuals or devices or (b) the sensitive covered data of more than 100,000 individuals or devices.

If passed, the ADPPA will require the FTC to set forth regulations on a type of short form notice that large data holders must submit to the FTC to describe their any covered data practices (i.e., collection and processing of covered data). Additionally, if the large data holder uses algorithms will be required to conduct annual assessments of those algorithms and submit such assessments to the FTC.

Such assessments must, at a minimum: (1) describe steps taken to mitigate potential harms related to education, employment, healthcare, insurance, credit, and other potentially significant subjects in a person's life; and (2) analyzing potential harms that may impact those individuals under the age of 17. The algorithm assessments must be conducted during the design of any new algorithm as well.

If passed, the large data holder algorithm requirements would align with the FTC's recent push to look at regulating and penalizing discriminatory algorithmic practices.

Beyond algorithms, large data holders would also be required to designate a data privacy officer (something akin to a Data Protection Officer, or Chief Privacy Officer) that reports directly to the covered entity's highest ranking officer, conduct biennial privacy impact assessments analyzing the pros and cons of the covered entities covered data practices, and annually certify that reasonable security measures are in place.

Sensitive Covered Data

It has become the standard that omnibus data protection laws and regulations impose stricter standards on the collection and processing of "sensitive covered data." The ADPPA is no different and would actually impose a broader definition than other data protection laws like the CPRA or the GDPR.

Under the ADPPA, "sensitive covered data" includes any covered data that falls within one of the following categories: (1) government-issued identifiers (social security numbers, passport or license numbers, etc.) that ***are not*** required to be publicly posted; (2) health data (including related to mental health, disability, diagnosis, or treatment); (3) financial account numbers, debit card numbers, credit card numbers or access credentials for any such financial account; (4) biometric information; (5) genetic information; (6) precise geolocation data; (7) private communications; (8) account or device log-in credentials; (9) race and ethnicity; (10) sexual orientation or sex life; (11) any information identifying an individual's online activities over time or across third party websites or online services; (12) calendar entries, address book information, photos, audio, texts, or videos maintained for private use on an individual's device; (13) information related to an individual's access or viewing of any TV, cable, or streaming service; and (14) information related to an individual who is under the age of 17.

Additionally, the ADPPA requires any covered entity to obtain an individual's express, affirmative consent prior to collecting or processing sensitive covered data.

While most of the above definition aligns with the CRPA and the GDPR's definitions of sensitive data, the ADPPA goes further in that information like text messages, contact information, and calendar entries on devices would also fall into the sensitive covered data bucket. Meaning, any covered entity operating a mobile application that connects to an individual's device contact list or calendar, will require express, prior consent from that individual before making such a connection.

Currently, there is no US law or regulation that requires opt-in consent for cookies, similar to the GDPR's and EU law's requirements. However, third party cookies fall within the definition of sensitive covered data; meaning if the ADPPA is passed, opt-in consent will be required before a covered entity loads third party cookies onto an individual's device or browser.

Duty of Loyalty

The ADPPA places a heavy focus on data minimization, privacy by design, and consumer data rights; under what the ADPPA coins the duty of loyalty.

The ADPPA's duty of loyalty's focus is data minimization. This duty requires a covered entity to only collect and process the covered data that is reasonably necessary and proportionate to the product or service being provided. Additionally, the ADPPA prohibits or restricts specific covered data

practices such as the transfer or sharing of specific covered data like passwords, social security numbers, genetic information, or biometric information.

In line with the GDPR, the duty of loyalty also requires privacy by design. Under the ADPPA, privacy by design requires a covered entity to establish policies and procedures mitigating privacy risk to those under the age of 17, mitigating privacy risks related to the design and development of products or services, and implementing reasonable training to promote legal compliance and risk mitigation.

How strict or onerous the ADPPA's duty of loyalty is on a covered entity depends on many factors, including (1) its size and complexity; (2) sensitivity of the covered data at issue; (3) volume of covered data at issue; (4) number of individuals that the covered entity collects covered data from and (5) the costs of implementing security and risk mitigation measures.

Consumer Data Rights

Consumer data rights have become a main stay in data protection laws; including under new state data protection laws. The ADPPA is no different and would set forth a number of consumer data rights in line with those existing state data protection laws and as set forth in the GDPR.

Under the ADPPA, individuals have the right to (1) access the covered data collected about them, the names of third parties who the covered data was transferred to, the sources of where the covered data was collected from, and the purposes of that collection and processing; (2) correct any inaccurate or incomplete covered data; (3) delete covered data held about them and require the covered entity to notify any third parties who the covered data was transferred to that the individual requested deletion; and (4) to receive a copy of the covered data that can be downloaded from the Internet (i.e., data portability).

As mentioned above, express, opt-in consent is required prior to collecting and processing sensitive covered data. Related, individuals have the right to withdraw any such consent and covered entities are required to provide individual with a clear and conspicuous (easy-to-execute) process to withdraw that consent.

The ADPPA would also provide certain opt-out rights, including (1) to opt-out of covered data transfers to third parties; and (2) targeted advertising.

The covered data transfer opt-out would be similar to the CPRA's "DO NOT SHARE" and "DO NOT SELL" requirements and subsequent data rights. Additionally, the targeted advertising opt-out, while seemingly broad on its face, actually only applies to cross-contextual, behavioral advertising.

The targeted advertising opt-out ***would not*** impact a covered entity's ability to use first party advertising cookies, advertising based on information obtained or tracked on the covered entity's website(s), or the processing of covered data solely for analyzing or reporting advertising performance, reach, or frequency (e.g., analytics).

Security Requirements

In line with other data protection laws, the ADPPA sets up a balanced security requirement on covered entity that requires an analysis of the context of the business and nature of the data being collected and processed.

Under the ADPPA, a covered entity must establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.

The following factors determine how onerous the security requirement is: (1) the size and complexity of a covered entity; (2) the context of the collection, professing, or transfer activities; (3) the amount and context of the data collected, processed, or transferred; (4) the sensitivity of the data; (5) the currently available technologies and safeguards; and (6) the cost of improvements in such measures.

Related, covered entities must continually assess security vulnerabilities, preventative and corrective actions, record retention and disposal policies and procedures, security training, designation of information security point person(s) within the covered entity.

Covered entities are exempt from the foregoing security requirements if a covered entity is subject to, and in compliance with, the security requirements under the Gramm-Leech-Bliley Act (e.g., financial institutions) ("**GLBA**") or the Healthcare Insurance Portability and Accountability Act (e.g., covered healthcare providers) ("**HIPAA**").

Enforcement and Penalties

The FTC would have enforcement and rulemaking authority under the ADPPA, giving the FTC an explicit directive to regulate data protection more broadly. Specifically, the FTC would be tasked with establishing a new bureau to assist with compliance and enforcement efforts.

Any violation of the ADPPA would be treated as unfair or deceptive trade practice, enforceable by the FTC under Article 5 of the Federal Trade Commission Act and its applicable regulations. Individual state attorney generals are also granted to ability to bring suit against covered entities that are in violation of the ADPPA to recover damages on behalf of residents in their respective states.

The draft ADPPA does not, itself, include any set amounts of fines or damages per violation.

The ADPPA would also provide a private right of action for individual consumers; however, it is only effective four years after the ADPPA effective date. The private right of action would allow anyone who suffers injury as a result of a violation of the ADPPA to bring a civil suit against a covered entity. The private right of action would allow individuals to seek compensatory damages, injunctive or equitable relief, and reasonable attorney's fees and litigation costs.

Before making a private claim, however, the individual must notify the FTC and state attorney general in writing of their civil claim. The FTC and specific state attorney general have 60 days to respond to state whether they will seek action. If they take action, the prospective plaintiff cannot pursue their private claim.

Preemption

One of the most debated topics in the ADPPA is whether the ADPPA should preempt existing state data protection laws and how far any such preemption should go (i.e., preempting ***any*** state data protection law, or just those that set lower requirements).

In its current form, the ADPPA preempts any and all state data protection laws except for (1) Illinois' biometric information protection act ("**BIPA**") and any other state laws governing the collection or use of biometric or genetic information; (2) the security-breach provisions of the CPRA; (3) state laws governing the privacy rights or protections for students or employees; (4) other specific state laws governing the collection and use of personal data related to crimes, public safety, financial information, marketing or spam, and medical or health information.

As the federal government beings drafting laws, regulations, and guidance that continue to regulate data protection along with several U.S. state laws, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Megan C. Parker at https://www.beneschlaw.com or 216.363.4416.