MEMORANDUM

To: GuidePost Clients
From: GuidePost Strategies
RE: Federal and State Privacy Landscape
Date: **UPDATED:** July 4, 2022

On June 23, the *American Data Privacy and Protection Act* was passed by voice vote in a House Energy and Commerce Subcommittee markup, and next moves to a full Committee markup. Senator Maria Cantwell (D-WA) remains adamantly (and vocally) opposed to the bill, although House members have expressed some hope that they can bring her onboard with some work and negotiations over the July 4 recess. Cantwell remains concerned that the bill does not have strong enough enforcement mechanisms, particularly in light of the Supreme Court decision in *Dobbs v. Jackson Women's Health Organization.* More on those implications below.

Prior to Subcommittee consideration, the ADPPA was modified slightly to address feedback received from stakeholders in last week's hearing, among others. These modifications were largely to provide additional clarification, but did not significantly change the private right of action provision, which has caused much of the concern among interested parties. The bill is expected to be further modified over the next few weeks ahead of a full committee markup, and, as mentioned above, there is hope that modifications can be made to bring Senator Catnwell onboard the legislation.

Cantwell is not the only Senate Democrat who has expressed concerns about the bill however; Senator Ron Wyden (D-OR), who is a leading voice on privacy policy, has expressed concerns, and Senate Majority Leader Chuck Schumer (D-NY) has shown support for Cantwell's position. Without Cantwell's support, the bill faces an almost insurmountable hurdle in the Senate.

What does *Dobbs* mean for privacy prospects?

The Supreme Court recently ruled in Dobbs v. Jackson Women's Health Organization to overturn both *Roe v. Wade* and *Planned Parenthood v. Casey*. In addition to eliminating the constitutional protection for abortion, the case also comes with a number of privacy issues. The decision in *Roe* found that the U.S. Constitution, through the Fourteenth Amendment, provides a right to privacy that also protects a right to an abortion. Justice Clarence Thomas has also indicated that he believes the decision in Dobbs also warrants a reconsideration of other cases, such as those creating a right to contraception and same-sex marriage.

The Court's decision will likely politicize what has been, up until this point, a bipartisan process. Coupled with Senator Cantwell's concerns expressed even before the final ruling, the bill is likely to become mired in partisan politics. There have already been concerns expressed that tech companies will be forced to divulge data in an effort to prosecute individuals who seek an abortion, and lawmakers have already penned a letter to Google expressing those concerns and asking them to stop collecting location data that could be used against those seeking abortions. On Friday, July 1, Google appeared to respond to these concerns, announcing in a blog post that the company will delete location data after people visit abortion clinics, domestic violence shelters, and other sensitive locations.

It seems unlikely at this point that Democratic members of Congress will choose to (or politically, be able to) move forward legislation addressing data privacy without some acknowledgement or provision addressing the abortion issue, which would be a poison pill for nearly all Republicans, and even potentially some Democrats. As such, it would seem that the privacy efforts that briefly had life are likely to face an insurmountable hurdle once again. *We will continue to monitor any movement on the House legislation.*

This memo serves to provide an overview of the key provisions of the *American Data Privacy and Protection Act* ("ADPPA" or "draft bill") and the interplay between the key actors in Congress who could move privacy measures forward.

At the outset, the ADPPA appears broad in scope - from its definition of "covered entity" and accompanying covered entity obligations to its consumer rights and private right of action - but does little to help stakeholders understand its implications and what it would mean in practice. This is in part due to the draft bill's heavy reliance on guidance that the Federal Trade Commission (FTC) would be required to issue in accordance with the bill's provisions. As such, the ADPPA leaves many questions unanswered. However, the House Energy and Commerce Committee will hold a hearing on the bill scheduled for Tuesday, June 14, which will offer the opportunity to begin a pathway to clarity. What's more, in an interview following the release of the ADPPA draft, FTC Chair Lina Khan - while declining to comment on the specific provisions of the bill - expressed optimism regarding the federal privacy developments and added that the Commission will "assess" its priorities and resources if Congress passes a federal privacy law.

EXECUTIVE SUMMARY

On Friday, June 3, Congressional leaders released the ADPPA, a bipartisan draft bill which seeks to establish a comprehensive federal data privacy framework. The bill was led by authors House Energy and Commerce Committee Chair Frank Pallone (D-NJ), House Energy and Commerce Ranking Member Cathy McMorris Rodgers (R-WA), and Senate Commerce Committee Ranking Member Roger Wicker (R-MS).

This bipartisan and bicameral effort has been years in the making. It is one of the most notable developments at the federal level since federal data privacy discussions began in earnest several years ago. Senate Commerce Committee Chair Maria Cantwell (D-WA), a key player in privacy talks who is also in charge of the Senate committee of jurisdiction, is notably absent on this list of sponsors, and has said there is no chance of the Senate taking up the House bill.

While Congress has struggled to pass, or even move, a data privacy bill at the national level, states have not been inactive themselves. There are other recent developments in privacy legislation and regulation at the state level, which this memo will also cover.

Of particular note in the ADPPA are its controversial preemption and private right of action provisions. In short, the ADPPA would preempt state privacy laws - with exceptions for the *Illinois Biometrics Information Privacy Act* and for certain provisions of the C*alifornia Privacy Rights Act*, among other exclusions - and would create a limited private right of action starting four years after the ADPPA would go into effect. We highlight these provisions later in this memo in greater detail.

THE AMERICAN DATA PRIVACY AND PROTECTION ACT: LEGISLATIVE SUMMARY

Covered Entities and Covered Data

The ADPPA as written is broad in scope and would impose obligations on a vast spectrum of entities, particularly on "large data holders." While certain data-level exemptions are authorized under the draft bill for entities subject to certain other federal laws, the ADPPA appears to rely on the FTC to further define what these limited exemptions would mean in practice.

Covered Entities. The ADPPA defines covered entity as "any entity or person that collects, processes, or transfers covered data" and is: (1) subject to the *Federal Trade Commission Act*; (2) a common carrier subject to title II of the *Communications Act of 1934*; or (3) an organization not organized to carry on business for their own profit or that of their members.

The draft bill also clarifies that the term covered entity includes "any entity or person that controls, is controlled by, is under common control with, or shares common branding with another covered entity."

Service providers are also considered covered entities in this legislation. Service providers qualify as such "only to the extent that such collection, processing, or transfer relates to the performance of such service or function or is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims."

Note that under the umbrella of covered entities are "large data holders", covered entities that, in addition to meeting the general requirements described above, also in the most recent calendar year:

- Met a certain gross revenue threshold of $250 million or more; and collected, processed, or transferred -
    - The covered data of more than 5 million individuals or devices "that identify or are linked reasonably linkable to 1 or more individuals" or
    - "The sensitive covered data of more than 100,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals."

This could include companies, such as auto companies, that would not traditionally be impacted by data privacy laws - but in this case, would be.

- Note further that this excludes any instance where the covered entity would qualify as a large data holder *solely on account of processing*:
    - Personal email addresses,
    - Personal telephone numbers, or
    - Log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity.

Large data holders, as discussed later in this memo, would be subject to additional requirements under the ADPPA, including certification responsibilities, the designation of data privacy and data security officers, and conducting privacy impact assessments.

The current text of the ADPPA also includes a small data exception from compliance with certain requirements outlined in the bill for any covered entity that can establish it meets the following requirements for three years (or for the period during which the covered entity has been in existence, if less than three years).

The requirements for qualifying for this small data exception are:

- The covered entity's average annual gross revenues during the period did not exceed $41 million.

- The covered entity did not annually collect or process the covered data of more than 100,000 individuals beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted within 90 days.

- The covered entity did not derive more than 50 percent of its revenue from transferring covered data during any year (or part of a year if the covered entity has been in existence for less than 1 year) that occurs during the period.

While it appears that there are data-level exemptions for entities subject to the *Gramm-Leach-Bliley Act* (GLBA), the *Health Insurance Portability and Accountability Act* (HIPAA), the *Family Educational Rights and Privacy Act* (FERPA), among other federal statutes, the extent of these exemptions would need to be further defined by FTC guidance. Such guidance would be issued no later than 1 year after enactment of the ADPPA.

Covered Data. The ADPPA generally defines covered data as "information that identifies or is linked to or reasonably linkable to an individual or a device that identifies or is linked to 1 or more individuals, including derived data and unique identifiers." The term excludes de-identified data, employee data, and publicly available information.

Duty of Loyalty and Consumer Data Rights

While many of the entity obligations and consumer rights detailed below call for further clarity (which per the ADPPA would be provided through FTC guidance), the running theme of the obligations and rights provided for in the draft bill is transparency. Moreover, beyond standard administrative and business operations as described below, the ADPPA would require covered entities to ensure that their data collection, processing, and transferring practices are narrowly tailored.

Duty of Loyalty. The ADPPA would prohibit covered entities from collecting, processing, or transferring covered data "beyond what is reasonably necessary, proportionate, and limited to" provide or maintain: (1) a specific product or service requested by an individual; or (2) a communication by the covered entity to the individual reasonably anticipated within the context of the relationship.

The "reasonably necessary, proportionate, and limited" standard would be defined by FTC guidance on such "data minimization" standards, but the exact timing of this guidance is not clear based on the text of the bill. Ultimately, sensitive data collection, processing, and transfer would only be authorized for certain activities and purposes under the ADPPA.

Activities that would be prohibited under the draft bill's "duty of loyalty" include (but are not limited to):

- The collection, processing, or transferring of social security numbers, except when necessary to facilitate extension of credit, authentication, or the payment and collection of taxes.

- The transfer of an individual's precise geolocation to a third party without affirmative express consent of the individual through a notice (the requirements of which are described in the bill).

- The collection, processing, or transferring of biometric information, except for data security, authentication, to comply with a legal obligation, to establish, exercise, or defend a legal claim, or for law enforcement purposes. Note that, beyond the enumerated exceptions, these activities would also be authorized where the covered entity obtains affirmative express consent of the individual through a notice.

Conditioning service or pricing on an individual's decision to waive or not waive his or her privacy rights would also be prohibited under the ADPPA.

In contrast, authorized activities that involve the collection, processing, or transferring of covered data - provided that such activities are reasonably necessary, proportionate, and limited to such activities - include (but are not limited to):

- Initiating or completing a transaction or fulfilling an order or service specifically requested by an individual, including any associated routine administrative activity (e.g., billing, shipping, and accounting).

- Activities including, generally, system maintenance, diagnostics, or maintaining a product or service for which such covered data was previously collected.

- Detecting or responding to a security incident or fulfilling product or service warranty.

The bill further establishes an explicit authorization for journalism - the draft bill clarifies that "nothing in this Act shall be construed to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution."

Expectedly, the bill would require covered entities to "establish and implement reasonable policies, practices, and procedures, regarding the collection, processing, and transfer of covered data." Data processing statements would also need to provide "whether or not any covered data collected by the covered entity is transferred to, processed in, or otherwise made available" to China, Russia, Iran, or North Korea. FTC guidance on such policies and practices would be issued no later than one year after enactment of the ADPPA.

Consumer Data Rights. In the interest of promoting transparency, covered entities would be required to ensure that their privacy policies, among other things, include a description of how an individual can exercise the consumer data rights provided for in the ADPPA. In general, under the draft bill an individual that makes a verified request to a covered entity would be able to exercise the right to access, correct, delete, and export covered data. The exercise of these rights would be subject to certain exceptions as described in the bill. The rights would also be further defined by the FTC, as the draft bill provides a 90-day window for the FTC's publication of a webpage that would elaborate on consumer rights and covered entity obligations.

The ADPPA would further establish an individual's right to opt out of covered data transfers and the right to opt out of targeted advertising. Covered entities would be prohibited from engaging in these activities particularly as they apply to children and minors, and the bill would establish a Youth Privacy and Marketing Division ("Division") within the FTC. The Division would address the privacy of children and minors as well as marketing directed at children and minors. The establishment of the Division underscores an urgency that has long been expressed by Congress to address children's online privacy.

Under the draft bill, covered entities also acting as third-party collecting entities (by meeting a certain threshold of data that they process while acting as such) would be required to register with the FTC.

The failure of such entities to register as third-party collecting entities will result in liability in the form of a civil penalty.

The ADPPA also contains non-discrimination provisions in connection with the collection, processing, and transferring of covered data, and would give the FTC the authority to initiate proceedings against covered entities that violate those provisions. Additionally, large data holders would be required under the draft bill to conduct impact assessments of their algorithms that are used to collect, process, or transfer covered data and submit annual algorithmic impact assessments to the FTC.

Corporate Accountability and Enforcement

Corporate Accountability. The ADPPA would impose certain requirements on large data holders' CEOs, privacy officers, and data security officers to annually certify to the FTC their "reasonable internal controls" in compliance with the bill and "reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance" with the bill.

Service providers would generally be prohibited from collecting or processing service provider data "for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider." They would also be prohibited from transferring service provider data to a third party, other covered entity, or another service provider "without the affirmative express consent, obtained by the covered entity with the direct relationship" to the individual to whom the data is "linked or reasonably linkable."

The draft bill further provides that the FTC will establish regulations and processes of approval for covered entities' technical compliance programs. Covered entities not in compliance with the guidelines to be established by the FTC would be subject to enforcement.

Enforcement. The ADPPA would direct the FTC to establish a new bureau related to consumer protection and competition to assist the FTC in exercising its authority under the bill and related authorities. The bill further provides that an Office of Business Mentorship would be established to provide guidance and consultation to covered entities regarding compliance with the provisions of the bill. Additionally, covered entities would be authorized to petition the FTC for tailored guidance on compliance.

Violations of the ADPPA or its accompanying regulations would be treated as an unfair or deceptive act or practice under the *FTC Act*. The bill would also establish a "Privacy and Security Victims Relief Fund" ("Fund") under the Treasury Department. Per the provisions of the bill, the FTC would be directed to deposit into the Fund "the amount of any civil penalty obtained against any covered entity or any other relief the Commission obtains to provide redress, payments or compensation, or other monetary relief" to individuals than cannot be located or the payment of which would otherwise not be practicable. The Attorney General (AG) as well as state AGs would be governed by similar provisions. State AGs are also authorized to bring a civil action to enjoin a covered entity's violative act or practice, enforce compliance, and obtain damages.

What is most noteworthy regarding the draft bill's enforcement provisions - in addition to its preemption of state laws by default with exemptions for California and Illinois laws [among others] - is its private right of action. Individuals would be authorized to enforce violations through a private right of action beginning 4 years after the date on which the bill is enacted. Actions against covered entities, in certain cases, may be granted the right to cure - with a 45-day cure window.

THE CONSUMER ONLINE PRIVACY RIGHTS ACT

Originally introduced in 2019, Senator Maria Cantwell's Consumer Online Privacy Rights Act offers a contrast to the ADPPA. Senator Cantwell expressed her reservations about the June 3 draft bill, asserting that "[f]or American consumers to have meaningful privacy protection, we need a strong federal law that is not riddled with enforcement loopholes. Consumers deserve the ability to protect their rights on day one, not four years later," referring to the 4-year moratorium after enactment before any private right of action can be pursued.

While Senator Cantwell's bill contains similar provisions to the ADPPA - such as requirements for covered entities to make privacy policies publicly available, establishment of the rights to delete, correct, and export data, and prohibitions on transfer of sensitive data without consent - there are some key distinctions between the competing bills. For one, Senator Cantwell's bill would prevent companies from using user-agreements to force individuals to go through arbitration to settle disputes rather than sue in court, while the Representative Pallone bill would not block companies from forcing customers to use arbitration (with an exception for cases related to children).

Additionally, in contrast with the Cantwell bill, the ADPPA would include data minimization requirements, loyalty duties, and privacy by design and price discrimination. Ultimately, it remains to be seen how these bills will progress, though as previously noted, the ADPPA is scheduled for a hearing in the House Energy and Commerce Committee on Tuesday, June 14.

PRIVACY IN THE STATES

Congress has long been eager to address the patchwork of state privacy legislation, and through the ADPPA, it has that opportunity in light of its preemption provisions. While ADPPA would preempt laws like the *Colorado Privacy Act* and the *Virginia Consumer Data Protection Act* (both enacted back in 2021), this preemption isn't absolute - for example, Illinois's Biometric Privacy Act (as a targeted state statute) will not be preempted by ADPPA.

While ADPPA has the potential to shift the state patchwork landscape of privacy laws, we have outlined significant recent state developments below.

California

In late May, California's new privacy agency, the California Privacy Protection Agency, released its first batch of draft rules for companies required to adopt the state's data privacy laws. California has been a pioneer in state privacy legislation since the enactment of the *California Consumer Privacy Act* (CCPA) in 2018--though note that CCPA will be replaced by the stricter *California Privacy Rights Act* (CPRA) early next year.

As previously discussed, ADPPA would generally preempt state laws, but it appears that not every provision of CPRA would be preempted by the federal measure. Still, laws such as those of California are "the target of preemption" given their contribution to "the emerging 'patchwork' of state consumer privacy laws."

Connecticut

In early May, Governor Ned Lamont signed Senate Bill 6 into law, which takes effect on July 1, 2023. SB 6 applies to entities that conduct business in Connecticut or produce products or services targeted to Connecticut residents that, during the previous calendar year, met certain thresholds related to personal data control and processing. Under SB 6, unlike California's CCPA, an entity is not subject to the law due to its annual revenues. With that said, Connecticut's new law would be one among the state patchwork that ADPPA would preempt.

Utah

In late March, Governor Spencer Cox signed the *Utah Consumer Privacy Act* (UCPA) into law, which becomes effective on December 31, 2023. The International Association of Privacy Professionals (IAPP) describes the substance of Utah's law as "a lighter, more business-friendly approach to consumer privacy" than its predecessors (California, Virginia, and Colorado). And while its sponsor Senator Kirk Cullimore stated that UCPA's current form is intended as a starting point, the ADPPA would appear to outright preempt the law.