Testimony and Statement for the Record of Bertram Lee Jr., Senior Policy Counsel for Data, Decision Making, and Artificial Intelligence, Future of Privacy Forum

Hearing on “Protecting America’s Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security”

Before the House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce

The Future of Privacy Forum
1350 I St. NW Ste. 350
Washington, DC 20005
www.fpf.org

June 13, 2022
Chairwoman Schakowsky, Ranking Member Bilirakis, Chairman Pallone, and Ranking Member McMorris-Rodgers, on behalf of the Future of Privacy Forum, thank you for inviting me to testify today in front of the House Energy and Commerce Subcommittee on Consumer Protection and Commerce. My name is Bertram Lee and I am Senior Policy Counsel for Data, Decision Making, and Artificial Intelligence at the Future of Privacy Forum (FPF). FPF commends the House Energy and Commerce Subcommittee on Consumer Protection and Commerce for holding this hearing and introducing bipartisan and bicameral privacy legislation.

The four main points we would like to leave you with this hearing are:
1. now is the time for Congress to pass comprehensive privacy legislation;
2. compared to each of the five state privacy laws passed since 2018, the American Data Privacy and Protection Act (ADPPA) is more comprehensive in scope, more inclusive of civil rights protections, and provides individuals with more varied enforcement mechanisms;
3. the ADPPA compares favorably to global frameworks, including Europe’s General Data Protection Regulation (GDPR); and
4. work remains to be done on specific provisions to ensure individuals are protected, the bill is workable for business, and there are not unexpected or undesired consequences. We urge that work to move forward thoughtfully and expeditiously.

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship and advancing principled data practices in support of emerging technologies. We are supported by leading foundations, as well as by more than 200 companies and law firms, with an advisory board representing academics, industry, and civil society. We bring together privacy officers, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

FPF applauds Congress for advancing comprehensive privacy legislation. FPF has long recognized the need for the enactment of a baseline, comprehensive federal privacy law that gives individuals meaningful privacy rights and places clear, workable obligations on businesses and other organizations that collect, use, and share personal data. A comprehensive federal law could address the gaps in the current U.S. sectoral approach to consumer privacy, which has resulted in incomplete legal protections. Currently, personal information collected within certain sectors, such as credit reporting, finance, and healthcare, are subject to longstanding federal safeguards, while commercial data outside of these sectors remains largely unregulated even when the data may be equally sensitive or high-risk.

The ADPPA would be comprehensive, filling the gaps between existing sectoral privacy regimes with baseline protections. The legislation would require entities that handle personal data to adopt baseline privacy and security safeguards - including individual rights to access, delete, port, and correct personal data, as well as rights to opt-out of targeted advertising and data transfers. The bill would apply to most organizations that handle personal data - commercial entities, common carriers, and non-profits. The ADPPA also includes additional requirements intended to address the unique challenges algorithmic technologies pose to civil rights, while promoting the use of technology to identify and mitigate discrimination in appropriate circumstances.
Contemporary data protection is complicated. And any attempt to regulate privacy across diverse sectors of the economy must be approached with care. Bi-partisan legislation is an excellent opportunity to capture the sense of urgency felt by Congress, individuals, companies, and data protection experts to establish a practical, protective, comprehensive federal privacy regime in the United States. I urge you to move forward quickly and thoughtfully to address stakeholder concerns, reduce the likelihood that legislation impacts individuals and organizations in unexpected and unintended ways, and provide for mechanisms to address those unexpected outcomes if they occur. Many of the contentious issues regarding data protection legislation can be addressed through careful drafting and consideration of the available legal, technical, and policy tools. Congress has an opportunity to meet the challenges posed by contemporary information-driven business practices with legislation that protects consumers and provides much needed clarity to businesses about their obligations.

I. Now is the Time for Congress to Pass Federal Privacy Legislation

Congress should advance a baseline, comprehensive federal privacy law because the impact of data-intensive technologies on individuals and marginalized communities is increasing every day as the pace of innovation accelerates. Each day's news brings reports of a new intrusion, new risk, new harm, another boundary crossed. Sometimes it's a company doing something that consumers or critics regard as “creepy;” sometimes it's a practice that raises serious risks to our human rights, or civil liberties, or our sense of autonomy. There is a growing public awareness of how data-driven systems can reflect or reinforce discrimination and bias, even inadvertently.

For many people, personal privacy is a deeply emotional issue, and a real or perceived absence of privacy may leave them feeling vulnerable, exposed, or deprived of control. For others, concrete financial or other harm may occur; a loss of autonomy, a stifling of creativity due to feeling surveilled, or the public disclosure of highly sensitive information like individuals' financial data or disability status are just some potential consequences of technology misuse, poor data security policies, or insufficient privacy controls.

Congress has the opportunity now to pass a law that will shape these developments to maximize the benefits of data for society while mitigating risks. Delaying Congressional action means that businesses will inevitably continue to develop new models, build infrastructure, and deploy technologies, without the guidance and clear limits that only Congress can set forth.

Current business practices along with new technologies are being shaped by laws around the world, while the U.S. approach to data protection remains outdated and insufficient. The continuation of cross-border data flows, which are crucial to the United States' leadership role in the global digital economy, are under stress. This may put U.S. companies, from financial institutions to cloud providers, at a disadvantage due to the perception that our laws are inadequate. Congress must ensure that the U.S. is not left behind as the rest of the world establishes trade and privacy frameworks that will de facto define the terms of international information and technology transfers for decades to come.
The United States currently does not have a baseline set of legal protections that apply to all commercial data about individuals regardless of the particular industry, technology, or user base. For the past decades, we have taken a sectoral approach to privacy that has led to the creation of federal laws that provide strong protections only in certain sectors such as surveillance, healthcare, video rentals, education records, and children’s privacy. As a result, U.S. federal laws currently provide strong privacy and security protection for information that is often particularly sensitive about individuals but it leaves other – sometimes similar – data largely unregulated aside from the FTC’s Section 5 authority to enforce against deceptive or unfair business practices.

The U.S. has not always lagged behind its major trade partners in privacy and data protection policymaking. In fact, the central universal tenets of data protection have U.S. roots. In 1972, the Department of Health, Education, and Welfare formed an Advisory Committee on Automated Data Systems, which released a report setting forth a code of Fair Information Practices. These principles, widely known as the Fair Information Practice Principles (FIPPs), are the foundation of not only existing U.S. laws but also many international frameworks and laws, including GDPR. And while GDPR is the most recent influential international data privacy and protection framework, the U.S. should look for interoperability with and insights from the OECD Privacy Guidelines and the Asia-Pacific Economic Cooperation (APEC) framework and Cross-Border Privacy Rules (CBPRs).

II. Compared to Recent State Privacy Laws, the ADPPA is More Comprehensive

Five states recently established comprehensive privacy laws. Some are fairly similar, although with key distinctions. Others have striking differences - for example, California’s approach is significantly different from the other four states in both form and structure.

Although these state regimes differ, they share several similarities that are important to Congress’ pursuit of federal privacy legislation:

1. First, all of these laws were enacted since 2018, and the most recent state legislative sessions across the U.S. - whether they resulted in bill passage or not - included more activity on data protection bills than any in recent memory. There is a clear trend - states are making privacy rules whether Congress moves forward or not.
2. Second, key dates are on the horizon for several of the state laws. The California Privacy Protection Agency (CPPA) is in the midst of an important rulemaking to clarify rights and obligations under the CPRA, with additional regulatory and enforcement activity expected over the next twelve months. The Colorado Attorney General is crafting rules to implement the Colorado Privacy Act, with a regulations deadline set for July 1, 2023.
3. Third, individuals and businesses are acting now in response to the states laws. Individuals in California are clicking CPRA-required “do not sell” links on web sites and filing “data subject access requests” which the CPRA requires companies to honor in many cases. The California Attorney General has initiated enforcement actions against
entities the AG alleges do not comply with the law.¹ And companies are dedicating substantial resources to build compliance programs in light of these new regimes.

4. Fourth, state bills are not coalescing around a single de facto national standard. The first-enacted law - California - did not result in a string of states adopting identical or nearly identical laws. While there are real similarities between, e.g. the Virginia and Colorado laws, there are also important differences between the Virginia, Colorado, Utah, and Connecticut regimes. And many pending state bills are different still. Lack of state to state uniformity is resulting in different rights for individuals and different obligations for businesses.

Taken together, these four factors should encourage Congress to move quickly toward a common, workable national standard. By analyzing the approaches taken by state lawmakers, including what protections they provide, how they are structured, and where compromises were achieved, many lessons can be learned to inform Congress’ work on a comprehensive federal bill.

In the addendum to our testimony, we offer a comprehensive comparison of ADPPA to different state laws. As our analysis demonstrates, ADPPA is more comprehensive in scope, more inclusive of civil rights protections, and provides individuals with more varied enforcement mechanisms than recent state laws:

1. ADPPA expands civil rights protections against algorithmic discrimination, whereas state laws have sought to codify existing civil rights protections.
2. ADPPA includes requirements that businesses incorporate privacy-by-design principles in the development of their data processing activities to an extent not found in existing state laws.
3. ADPPA includes corporate accountability mechanisms not found in the state laws, such as the requirement of designating privacy and data security officers and executive certifications of compliance.
4. In addition to requiring traditional privacy policies, ADPPA requires certain large data holders to provide 'short form' privacy notices to better inform individuals of how their data will be used and their rights, a provision not found in any state law.
5. ADPPA provides pathways for individual redress of privacy violations, whereas state laws have left enforcement exclusively to government agencies.
6. ADPPA creates new protections for youth data, including a prohibition on targeted advertising to minors under the age of 17, as well as including broader prohibitions against harmful uses of data.

1. Civil Rights Protections and Algorithmic Discrimination

ADPPA, unlike any other state privacy law, extends longstanding civil rights protections that prohibit discrimination in the enjoyment of public accommodations by protected class (race, gender, sexual orientation, etc.) to the provision of online products and services. This includes, for example, price discrimination in digital marketplaces, content monetization, and all digital

¹ https://oag.ca.gov/privacy/ccpa/enforcement
services. The ADPPA would prohibit both direct, intentional discrimination and disparate impact (neutral practices that have a disparate discriminatory impact on a protected class).

ADPPA would also require large data holders who collect, process or transfer covered data to conduct yearly algorithmic impact assessments. Additionally, a covered entity, as defined by the bill, must conduct an algorithm design evaluation, including any training data used to develop an algorithm, if it is a covered entity or uses an algorithm in whole or in part to collect, process, or transfer covered data.

2. Privacy by Design

The current privacy by design requirement of ADPPA would require covered entities to “establish and implement reasonable policies, practices, and procedures” regarding data processing. Covered entities would be required to mitigate risks, including to individuals under 17, in their design, development, and implementation of products and services. This would include implementing meaningful safeguards and training to facilitate compliance with all privacy laws, in alignment with guidance from the Federal Trade Commission over time.

Privacy by Design is a key feature of many global data protection regimes, including the GDPR, and provides an important safeguard that goes beyond notice and choice. Among its core principles are user-centric design, visibility, transparency, and privacy as a default setting. Supporters of Privacy by Design also argue that it encourages state-of-the-art privacy engineering, and the development and use of privacy-enhancing technologies (PETs).

This requirement is similar to the Data Protection by Design and by Default requirement of the GDPR. However, the latter was criticized for not covering “processors” or “service providers”, who are usually the entities building technology solutions and processing systems which are then offered as a service to “controllers” or covered entities under the GDPR. ADPPA could clarify that Privacy by Design applies to covered entities, including “service providers”, in order to render this obligation more effective.

3. Corporate Governance Requirements

The requirement for privacy and data security officers at companies is a major step in the right direction. For years, many have asked that privacy and data security be a part of the corporate governance structure for companies. By mandating that corporate governance structures take

2 Article 15
3 Ann Cavoukian; https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
into account privacy and data security concerns, privacy, and data security professionals are better able to help ensure not only compliance with ADPPA but also build public trust in consumer privacy.\(^5\) We have already seen great strides in privacy and data security becoming an integral part of the corporate governance infrastructure. However, placing legal obligations on companies to do so ensures better privacy and data security practices globally.

4. Short Form Privacy Notices

Large entities requiring simple, understandable short-form privacy notices in addition to full privacy policies are a major help to consumers. In many cases, even privacy professionals struggle to understand the jargon and legalese associated with current privacy policies. Consumers will be in a better position to understand how their data is being used, where it goes, and what policies companies have in place in order to better protect their data.

Addressing the widespread problems of targeted advertising is also critically important. Digital ads can play a key role in supporting media and services, but from publishers to advertisers to consumers, everyone agrees the current ecosystem is unsustainable. A path that ensures competition, prevents discrimination, and supports individual rights without requiring complicated choices by consumers is needed.

5. Individual Redress and Expanded Consumer Rights

ADPPA’s inclusion of individual redress mechanisms, on top of regulatory enforcement, goes beyond what existing state privacy laws provide, and thus provides greater protections for consumers. The history of civil rights enforcement shows that individual redress can ensure accountability. At the same time, ADPPA seeks to prevent bad faith litigation and provide small businesses the right to cure.

Similar to most U.S. laws and proposals (including the CCPA), ADPPA would prohibit retaliation against individuals who exercise their privacy rights, meaning a covered entity could not deny, charge different prices or rates, or condition or effectively condition the provision of a service or product to an individual on the individual’s agreement to waive any privacy rights . . .” while preserving loyalty programs that provide free or discounted products or services in exchange for an individual’s continued business.

Generally, the Draft would preempt comprehensive state privacy laws insofar as they relate to the same “covered” areas (exception for the CPRA’s private right of action for data breaches). The Draft text would, however, expressly preserve more than a dozen categories of state laws, including law regarding health and financial data that are integral companions to those sectoral federal regimes, civil rights laws, employee and student privacy laws, laws regarding library record confidentiality, and a range of state laws that are either generally applicable to common

law actions under contract and tort principles, or intended to cover very specific sorts of data, like HIV status.

6. Data Protections for Children and Protections Against Harmful Data Uses

The ADPPA would extend federal data protection to minors. As written it would appear to prohibit the collection of information for those under 17 without affirmative express consent, targeted advertising to individuals under 17, and transfers of data on individuals between 13 and 17 years old without express consent from the minor or the parent. The ADPPA also creates a Youth and Privacy Marketing Division at the FTC that would be responsible for enforcement.

Additionally, restrictions on presumptively harmful uses of data help ensure that sensitive consumer data, such as biometric data, is not being overly collected. The ADPPA protects an individual's biometric information, including traditional biometric markers like facial recognition and iris scans, as well as emerging biometric identifiers like gait, personally identifying physical movements, and other behavioral biometrics.

Of note ADPPA does not exclude photographs or videos from its definition, nor does it permit “biometric information” to be considered public information. This would likely mean that companies like Clearview AI cannot argue that collecting social media photos for generating facial recognition systems is outside the scope of the law. The biometric provisions in the ADPPA would also apply to Virginia and Utah comprehensive laws which contain carveouts for biometric information.

In contrast, other recently adopted comprehensive state privacy laws either do not require consent for facial recognition (California), do not define biometric data (Colorado), or contain ambiguous language (Virginia).

III. Comparing the ADPPA to GDPR and Global Data Privacy and Protection Frameworks:

Commerce, data flows, business practices, and privacy compliance regimes are increasingly global. As Congress crafts federal privacy legislation, it should consider how individuals’ rights and companies’ obligations would interact with global privacy regimes. These intersections have implications for how individuals understand and avail themselves of rights to access and control personal data, how privacy safeguards are implemented by organizations, and how enforcement actions proceed against those who misuse personal information. A successful federal regime would ensure that user rights are robust, understandable and consistent, while companies are governed by clear rules that do not subject them to conflicting legal obligations across borders. It would also ensure that Americans enjoy the same or greater level of protection for their data privacy rights as do users and consumers from outside the US covered by comprehensive data privacy frameworks like the GDPR.
New privacy frameworks also generate opportunities. Opportunities to align obligations with existing regimes so that individuals understand their rights and companies have clear, consistent responsibilities. Congress also has the opportunity to help ensure that companies subject to other global regimes - including Europe’s GDPR - can utilize or build on years of previous compliance work.

**Similarities to GDPR**

In this respect, the ADPPA compares favorably to the GDPR, for example in defining a very broad scope of covered data and in providing Americans individual data privacy rights like access, correction, deletion and portability in relation to their personal information handled across sectors.

Under both the ADPPA and the GDPR, commercial entities would have obligations to protect and restrict the processing of all personal information that can identify a person, directly or indirectly. That includes, for example, the wide range of information about our phones, computers, and other devices that may not be attached to our name, but can nonetheless be used for targeted and micro-targeted advertising, the creation of detailed profiles of our lives and behavior, and in some cases used to discriminate against people in pricing, messaging, and opportunities. Understanding how the ADPPA fits into global frameworks helps support consistent protections for individuals and ensures businesses and not for profits of every size can compete in international markets.

Given the importance of the United States data protection framework to the global economy, we encourage policymakers to consider the interoperability of this legislation with the GDPR. As drafted, the legislation has a more streamlined overall approach compared to the GDPR, that is stronger in some aspects and more limited in others. There are also several ways in which this legislation could be better aligned with the GDPR to enable easier compliance for entities that may be subject to both. We will expand on those in Section IV.

Below, we highlight seven key areas in which the ADPPA aligns with the GDPR, as well as three recommendations for improvements to bring the two frameworks even closer.

The key areas where the ADPPA aligns with the GDPR are:

1. **Comprehensiveness in terms of data covered, types of processing covered and cross-sectoral applicability**, with the caveat that the ADPPA is more limited in comparison. While it largely applies across industries and to non-profits, it does not apply in the public sector. The ADPPA also does not cover publicly available personal information and employee data, like the GDPR does. Otherwise, its definition of covered data is just as broad, including the “identifiability” standard by reference to unique identifiers, just like the GDPR. Its definitions of collection, processing and transfers are also as broad as the GDPR definition of “processing”.

2. **The existence of individual rights, including access, correction, deletion and portability, as well as a limited right to object**. Rights of individuals to control their own information are an essential element of the GDPR and the rights provided by the ADPPA measure up well to it. However, the GDPR right to object is broader in scope, as it applies
to any processing of personal data conducted on the basis of the legitimate interests of
the covered entity, and is not limited only to transfers and targeted advertising.

3. The recognition of special categories of data that merit enhanced safeguards due to
their sensitive nature. Both the GDPR and the ADPPA prohibit processing of specific
categories of sensitive data, with exceptions based on consent and other limited grounds.
However, the ADPPA is more comprehensive in terms of the categories of sensitive data it
protects and is also more protective than the GDPR since it has more limited exceptions
allowing the processing of such data.

4. Requiring data minimization for all processing of covered data, including collection
and transfers. Just like in the ADPPA, the data minimization principle underpins all
processing of personal data under the GDPR. Moreover, there are instances of the
principle of purpose limitation that surface in the ADPPA, in a similar manner to how it
manifests as an overarching principle in the GDPR.

5. The identical standard for valid consent under the GDPR and the ADPPA - “freely
given, specific, informed and unambiguous” - as well as the similar requirements
against bundling of consent for different acts and practices ensure that individual
consent is meaningful and not a “tick the box”, “take it or leave it” exercise. The right to
withdraw consent also has an identical standard under the two frameworks - it must be as
easy to withdraw consent as it is to give consent. This provides a strong safeguard for
individuals in relation to how their personal information is collected and used and at the
same time streamlines compliance for those entities covered by both frameworks.

IV. Recommended Revisions and Additions

A comprehensive federal privacy law would be a monumental step towards ensuring that all
Americans have meaningful privacy rights across all business sectors that use personal data. But
it is hard to craft a privacy law that is clear, consistent, and interacts harmoniously with existing
legal frameworks and evolving technologies and business practices. More work remains to be
done to ensure that the ADPPA appropriately protects individuals, is workable for businesses,
and there are not unexpected or undesired consequences. Below are four recommendations that
we think would improve ADPPA:

1. Funding for the FTC

The FTC would need substantial additional funding to effectively enforce ADPPA, as well as to
comply with additional requirements ADPPA places on the Commission. The bill would provide
the Commission with authority to enforce privacy requirements that are more specific than the
FTC’s current general authority to combat “unfair and deceptive” business practices. With greater
specificity comes greater demand for capable technologists, lawyers, and other experts to ensure
the Commission is effectively executing Congress’ mandate. In addition to this heightened need
for general investigation and enforcement resources, ADPPA includes specific provisions that
would require the FTC to promulgate new regulations regarding certain bill provisions, and to
create a “Youth Privacy and Marketing Division,” headed by a Director. Rulemaking and
establishment of a new division should be supported by additional funding for the Commission; these activities require support beyond the general increase in authority, investigative activities, and enforcement actions contemplated by ADPPA.

Fully staffing and funding the FTC is critical for ADPPA to live up to its promise as a thoughtful and powerful privacy law that would bring critical privacy protections to all Americans. A fully functioning FTC is critical to the ADPPA's success.

2. More Iterative Processes

Portions of the bill provide for limited FTC rulemaking, but several key provisions do not include mechanisms to update the law in light of rapidly evolving technologies and business practices. The impact of technological change has long bedeviled authors of privacy laws. In 2012, Congress amended the Video Privacy Protection Act to account for the shift from physical video stores to online video delivery - a shift that was unforeseeable in 1988 when the law was passed, download speed typically topped out around 2,400 baud, and it would have taken approximately 100 hours to download a single feature film even if one were available.

Congress and state lawmakers have turned to various mechanisms to address the legislative challenges posed by evolving technology, including targeted rulemaking authority regarding specific statutory provisions, administrative safe harbors, and other methods. California's and Colorado’s recent privacy laws provide for rulemaking as a mechanism to provide certainty on definitions, take account of newly-discovered or developed categories of sensitive data, and promote the development of novel privacy enhancing technologies. Sections that might benefit from iterative mechanisms might be the definition of sensitive data, the recognition of certain types of privacy-enhancing technologies may change.

3. Intersection with Other Federal Laws

The ADPPA is clear on a number of issues, but one where there is a significant concern is how the ADPPA intersects in compliance with other federal privacy laws (COPPA, FERPA, HIPAA, etc.). We would recommend that Congress look at the intersection of these laws from a compliance standpoint and create more clarity both for consumers and businesses as to where ADPPA compliance begins and ends.

The ADPPA would not amend or alter the federal frameworks set forth under COPPA or FERPA, and the draft's section on preemption preserves state laws that govern privacy rights for students and protections for student information. This could impact, for example, enforcement rights for parents. Because COPPA has no private right of action, this means that unlawful transfers of data collected from minors between 13 and 17 could be subject to private enforcement, while the same conduct involving data from children under 13 might not.

While covered entities are required to refrain from targeted advertising and data transfers if they have “actual knowledge” that an individual is a minor, the provisions for processing “sensitive covered data” do not currently include a knowledge standard. Unlike many other categories of sensitive data (e.g. account login credentials), the fact that data was collected from a child may not be obvious on its face or easily distinguishable from data collected from adults. Companies
that process data from minors or from “general audience” products and services will likely push for greater clarity on this point.

Additionally, in order to prevent unintentionally amending U.S. surveillance laws and to allow for both clarity for covered entities with respect to compliance and to better protect civil liberties, we would suggest that this section expressly reference compliance with due process along with state and federal law as a precondition for law enforcement data access. Such language is also necessary for other sections that reference law enforcement access (Sec. 102(a)(3), (5), and (6); Sec. 203(d)(3)(vi)). Failure to address this could also create jurisdictional friction with the judiciary committees in both houses.

4. Definitional Clarity

Several ADPPA definitions\(^6\) could benefit from clarification, either through statutory revision, regulatory explication, or judicial interpretation. When ADPPA definitions are intended to align with similar terms in other legal frameworks, those links could be made explicit in legislative history, subsequent rulemaking, or informal guidance from the FTC. There would be a particular benefit in identifying circumstances in which ADPPA terms align existing federal sector laws or with the GDPR; both could be incredibly helpful from a compliance standpoint and give much-needed clarity to the bill. For example, given the centrality of the term, we recommend aligning the definition of “covered data” with “personal information” in the GDPR, while providing clarifying, non-exhaustive subsections to ensure that the definition includes, \textit{but is not limited to}, persistent identifiers, device identifiers, pseudonyms generated through probabilistic tracking, and so forth. This is but one example of many where revised definitions could help from a compliance, enforcement, and consumer rights standpoint.

We also recommend that Congress consider expanding the research exception for the ADPPA. The current exception for IRB-approved research is much more limited than as defined under the Common Rule, which allows for “systematic, generalizable studies,” i.e. not only research that is in the “public interest.”

Additional clarity on the distinction between data controllers and processors is needed. Most data protection laws, including the GDPR, establish a clear distinction between data controllers (that determine the purposes and means of processing) and data processors (that process data solely on behalf of a controller – for example, cloud storage and other service providers). Typically, processors are not expected to comply with the majority of business obligations, but are expected to assist controllers in compliance and may not process data further for secondary uses. In contrast, the current Draft applies obligations broadly to all “covered entities,” with only limited exceptions for service providers. This is likely to raise operational questions – for example, how a service provider would obtain consent if it materially changed a privacy policy.

Conclusion

Now is the time for Congress to pass comprehensive privacy legislation. The impact of data-intensive technologies on individuals and marginalized communities is increasing every day

\(^{6}\) [Insert Sections Here]
as the pace of innovation accelerates. Congress has the opportunity now to pass a law that will shape these developments to maximize the benefits of data for society while mitigating risks. Delaying Congressional action means that businesses will inevitably continue to develop new models, build infrastructure, and deploy technologies, without the guidance and clear limits that only Congress can set forth.

Compared to each of the five state privacy laws passed since 2018, the American Data Privacy and Protection Act (ADPPA) is more comprehensive in scope, more inclusive of civil rights protections, and provides individuals with more varied enforcement mechanisms; the ADPPA compares favorably to global frameworks, including the Europe's General Data Protection Regulation (GDPR). This is a monumental feat that should be celebrated by all involved and passed into law. While work remains to be done on specific provisions to ensure individuals are protected, the bill is workable for business, and there are not unexpected or undesired consequences, we again ask that Congress to move forward thoughtfully and expeditiously to find common ground on these important issues.

Again thank you for the opportunity to testify and I look forward to answering your questions.
**ATTACHMENT**

Please see disclaimers contained in relevant footnotes

Table 1: Comparative Chart (between the American Data Protection and Privacy Act, California Privacy Rights Act, and other comprehensive state privacy laws)  

<table>
<thead>
<tr>
<th>Covered Entity Threshold (the requirements for an entity to be subject to the law)</th>
<th>ADPPA</th>
<th>California Privacy Rights Act 8</th>
<th>Other Laws (Colorado, Connecticut, Virginia, and Utah) 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Either: - Collects, processes or transfers covered data and is (i) subject to FTC Act; (ii) a common carrier under title II of the Communications Act of 1934; or (iii) a non-for-profit organization; OR - Any entity or person that controls, is controlled by, is under common control with, or shares common branding with an entity that meets the above requirements.</td>
<td>Either has: - Annual revenue &gt;$25 million; - Annually buy, sell, or &quot;share&quot; personal information of 10,000+ consumers; OR - Derive 50% annual revenue from selling or sharing personal data for behavioral advertising</td>
<td>- Most require controlling or processing personal data of over 100,000 state residents; OR - Derive 50% of annual revenue from the sale of personal data and control/processing personal data of 25,000 state residents</td>
<td></td>
</tr>
</tbody>
</table>

| Scope/Coverage (features affecting which entities have obligations under the law) | - Extends to non-profits and common carriers - Includes limited small business carve-outs | - Does not extend to non-profits - Includes small business carve-outs | All laws contain small business exemptions. Most do not extend to non-profits (except Colorado) |

| Consumer Rights |
| --- | --- | --- |
| **Access** (ability to request what data an entity has) | Yes | Yes | Yes |
| **Correction** (right to correct inaccurate data held by an entity) | Yes | Yes | Yes (Not Utah) |
| **Deletion** (right to request deletion of personal data held by an entity) | Yes | Yes | Yes |
| **Portability** (ability to receive a copy of data and transfer in) | Yes | Yes | Yes |

---

7 This chart focuses on high-level details of what is and is not in the proposed bill and state laws. It is not designed to reflect subtle distinctions between these proposed and codified laws.

8 The California column reflects the provisions of the CPRA, which will go into effect on January 1st, 2023, and will replace the currently enacted CCPA. Certain aspects of California law are being clarified through rulemaking.

9 Colorado, Connecticut, Virginia, and Utah are included in the same column because these states share similar structural frameworks. Despite this similarity, the laws of these states contain significant variations in consumer rights and business duties.
<table>
<thead>
<tr>
<th><strong>Opt-In Consent</strong>&lt;br&gt;(an individual must affirmatively consent for an entity to collect or use certain data)</th>
<th>For:  - Sensitive covered data  - Adolescent data (13–17);  - Retention of data beyond its processing purpose; and  - Service provider transfers of covered data to other entities.</th>
<th>For:  - Sale or sharing of adolescent data (13–15);  - Inconsistent secondary use  Does not require opt-in consent for collection or processing of sensitive data.</th>
<th>All other state laws require opt-in consent for <strong>sensitive data</strong> and inconsistent secondary uses of data. (except Utah)  Connecticut requires opt-in consent for sales and targeted advertising using adolescent data (13-15).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Opt-Out Rights</strong>&lt;br&gt;(the right of an individual to cease being subject to certain processing activities)</td>
<td>For:  - Targeted advertising  - Data transfers  Does not require for automated decision-making or profiling</td>
<td>For:  - Data sales and sharing (including cross-context behavioral advertising)  -Right to ‘limit the use and disclosure of sensitive personal data’  - Future rulemaking on automated decision-making and profiling.</td>
<td>All other states permit opt-out targeted advertising and data sales.  Utah is the only state that does not permit individuals to opt-out for profiling</td>
</tr>
<tr>
<td><strong>Global/Unified Opt-Out</strong>&lt;br&gt;(Automated exercise of opt-out rights through user-enabled signals)</td>
<td>FTC to determine feasibility</td>
<td>Yes</td>
<td>Included in Colorado and Connecticut; excluded in Virginia and Utah</td>
</tr>
</tbody>
</table>

### Business Obligations

<table>
<thead>
<tr>
<th><strong>Privacy Notices</strong>&lt;br&gt;(information provided about an entity's actions taken with respect to personal data )</th>
<th>Yes, plus <strong>short-form notices</strong> for 'large data holders’</th>
<th>Yes, but no short-form notice requirement.</th>
<th>All require privacy notices, but do not require short-form notices.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data minimization</strong>&lt;br&gt;(the requirement to limit data collected and retained as necessary for the purpose)</td>
<td>Yes</td>
<td>Yes, pending regulations</td>
<td>Most state laws have limited minimization principles connected to privacy notices.</td>
</tr>
<tr>
<td><strong>Privacy by Design</strong>&lt;br&gt;(requirement for entities to consider privacy risks in the design, development, and implementation of products)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Prohibited processing activities</strong>&lt;br&gt;(prohibits the collection and use of certain data unless the purpose falls within an exception, including affirmative express)</td>
<td>Yes, including - SSNs - Precise geolocation information - Biometric information - Password - Non-consensual intimate</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>consent)</td>
<td>images - Genetic information - An individual’s aggregated internet search or browsing history - An individual’s physical activity information from a smartphone or wearable device, with exceptions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data security provisions (requiring entities to implement certain security measures)</td>
<td>Yes, additional obligations for ‘large data holders’</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Civil Rights Provisions and AI (providing that data processing cannot discriminate against protected classes)</td>
<td>Yes, plus requires algorithmic impact assessments and design evaluations.</td>
<td>Limited to complying with existing laws. Does not require algorithmic assessments.</td>
<td>Most state laws have civil rights provisions limited to complying with existing laws. None require algorithmic assessments.</td>
</tr>
<tr>
<td>Privacy Impact Assessments (technical assessment to identify and document privacy risks for systems and processes)</td>
<td>Yes (applicable to ‘large data holders’)</td>
<td>Yes (assessments required for risky processing activities)</td>
<td>Yes (assessments required for risky processing activities). Not required in Utah.</td>
</tr>
<tr>
<td>Specific ‘Data Broker’ Requirements (requirements for entities that collect data from secondary sources, aggregate, and sell the data to other entities)</td>
<td>Yes, requires “third-party collecting entities” to register with the FTC and honor a “Do Not Collect” mechanism.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Non-retaliation for exercise of consumer rights (an entity may not deny products or services, or charge different prices, based on whether individuals exercise privacy rights)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (limited in Utah)</td>
</tr>
</tbody>
</table>

### Enforcement

<p>| Private Right of Action (right of individuals to bring suits for violations) | Yes, for most provisions | Only for data breaches or business violation of security measures | No |
| Regulatory Enforcement (regulatory body or executive agency responsible for enforcing the law) | FTC &amp; State Attorneys General | Attorney General and California Privacy Protection Agency | Typically State Attorney General (and District Attorneys in Colorado). |
| Regulatory Rulemaking | Yes, fairly broad authority for | Yes for identified provisions | Except Colorado, no other state |</p>
<table>
<thead>
<tr>
<th><strong>Enforcement of Arbitration Agreements</strong> (provisions relating to the validity of pre-dispute agreements requiring individuals to arbitrate any potential claims and waive judicial redress)</th>
<th>Yes - Entities may generally have pre-dispute arbitration agreements with individuals over 18 years old. Individuals under 18 years old cannot be subject to arbitration agreements or joint action waivers.</th>
<th>Unclear - the law generally states that agreements to limit consumer rights are unenforceable, however Courts have granted motions to compel arbitration of asserted CCPA class action claims where terms and conditions contained arbitration provisions.</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safe Harbors and Defenses</strong> (compliance mechanisms that prevent or provide protection against enforcement actions)</td>
<td>Yes - technical compliance programs and commission approved compliance guidelines.</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>