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.

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.[1] 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.

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 states that have passed privacy laws 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. 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, not for profits and researchers, and there are not unexpected or undesired consequences. We urge that work to move forward thoughtfully and expeditiously.

FPF applauds Congress for advancing comprehensive privacy legislation. FPF has long recognized the need to enact 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. Personal information collected within specific sectors, such as credit reporting, finance, and healthcare, is subject to longstanding federal safeguards. In contrast, commercial data outside of these sectors remains largely unregulated even when the data may be equally sensitive or high-risk.

The ADPPA would achieve this. The legislation would require entities that handle personal data

[1] The views herein do not necessarily reflect those of our supporters or our Advisory Board. See Future of Privacy Forum, Advisory Board, https://fpf.org/about/advisory-board/; Supporters, https://fpf.org/about/supporters/.

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. Any attempt to regulate privacy across diverse sectors of the economy must be approached with care. Bipartisan 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. We 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 mechanisms to address those unexpected outcomes should 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. This was true when Future of Privacy Forum CEO Jules Polonetsky testified to it in the Senate in 2019, and it is even more true today. As he indicated, the impact of data-intensive technologies on individuals, and marginalized communities in particular, is increasing every day as the pace of innovation accelerates. Each day's news brings reports of a new intrusion, new risk, further harm, or another boundary crossed. Sometimes it's a company doing something that consumers or critics regard as "creepy;" sometimes, it is a practice that raises serious risks to our human rights, 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 powerless. 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.

Now more than ever before, Congress has the opportunity to pass a law that will shape these developments to mitigate the risks of data for society. 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. This creates real economic costs that will only increase the longer we go without a statutory standard.

Current business practices and new technologies are being shaped by laws worldwide, 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, is under stress. This may put U.S. companies, from financial institutions to cloud providers, at a disadvantage. 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 Federal Trade Commission's (FTC) 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.[2] 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.[3] 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[4] and the Asia-Pacific Economic Cooperation (APEC) framework and Cross-Border Privacy Rules (CBPRs).[5]

---

[2] Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services (1973), https://aspe.hhs.gov/report/records- computers-and-rights-citizens.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[4] Organization for Economic Co-operation and Development, Privacy Guidelines, https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[5] APEC has 21 members comprising nearly all of the Asian-Pacific economies, including the United States. The CBPR system—endorsed by APEC member economies in 2011 and updated in 2015 attempts to create a regional solution

The U.S. has a shrinking window of opportunity to regain momentum at both the national and international levels. If we wait too long, more countries and states will act, which will have an immediate impact on new technologies and business initiatives and ultimately reduce the impactof any federal law.

II. Compared to Recent StatePrivacy Laws, 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, these laws have been 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 of 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 websites 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 and the Virginia Attorney General is poised to do the same under Virginia's privacy law in six months.[6] 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

---

across 21 member economies, whose governments are at different stages of compliance with the APEC Privacy Framework. In the United States, the Federal Trade Commission has agreed to enforce the CBPRs. Eight APEC countries have formally joined the CBPR system—United States, Canada, Mexico, Japan, Singapore, Taiwan, Australia and the Republic of Korea. In the recent United States-Mexico-Canada Agreement (USMCA), which Congress is reviewing as it considers ratification, the three countries promote cross-border data flows by recognizing the CBPR system as a valid data privacy compliance mechanism for data-transfers between the countries. See Cross-Border Privacy Rules System, http://cbprs.org/. Also relevant for the Committee's reference is Convention 108 of the Council of Europe, an international data protection treaty that has been signed by 54 countries to date, not including the United States.

[6] https://oag.ca.gov/privacy/ccpa/enforcement

Colorado laws, there are also important differences between the Virginia, Colorado, Utah, and Connecticut regimes. And many pending state bills are different still. The 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 comparison of key ADPPA provisions to different state laws. Our analysis demonstrates that the 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 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.
3. 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.
4. ADPPA provides pathways for individual redress of privacy violations in some circumstances, whereas state laws have left enforcement almost exclusively to government agencies.
5. 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.
6. ADPPA requires that businesses incorporate privacy-by-design principles in the development of their data processing activities to an extent not found in existing state laws.

1. Civil Rights Protections and Algorithmic Discrimination

ADPPA, unlike any 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, protections against price discrimination in digital marketplaces and content monetization based on an individual's race, gender, or similar trait. 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 uses an algorithm in whole or in part to collect, process, or transfer covered data.

2. Corporate Accountability Requirements

The ADPPA requirement for privacy and data security officers at companies is a major step toward formalizing data protection accountability mechanisms in the U.S. Leading organizations have appointed compliance experts to these roles and dedicate substantial resources to building effective privacy programs. Global privacy regimes encourage or require this sort of institutional commitment to data protection. But these roles and programs are not universal, and recent state privacy laws do not incentivize or require organizations to appoint privacy and data security officers to the extent of ADPPA. The ADPPA requirements are consistent with emerging trends in FTC enforcement actions and settlement agreements, which routinely require companies to adopt "comprehensive privacy and/or security programs."

For years, many have asked that privacy and data security be a part of the corporate governance structure for companies.[7] By mandating that corporate governance structures take 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.[8] 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.

3. Short Form Privacy Notices

Large entities' provision of simple, understandable short-form privacy notices in addition to full privacy policies is a major help to consumers. Experts have long understood that consumers are unable to meaningfully review and understand all the privacy policies governing personal data on

---

7 https://www.ftc.gov/business-guidance/blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security-oversight; https://hbr.org/2000/11/chief-privacy-officer; https://www.avertium.com/blog/chief-privacy-officer-enterprises-c-level-leadership-personal-data-privacy

8 https://www.forbes.com/sites/blakemorgan/2020/06/22/50-stats-showing-why-companies-need-to-prioritize-consumer-privacy/?sh=46c2bd037f61

all the digital services they use.[9] And the terms of most policies likely create additional challenges. In many cases, even privacy professionals struggle to understand the jargon and legalese associated with current privacy policies. Short form privacy notices put consumers 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.

4. 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, particularly for individuals from traditionally marginalized communities. 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 service to individuals who choose to opt out of certain data sharing or decline to waive their privacy rights, while preserving loyalty programs that provide free or discounted products and services in exchange for an individual's continued business.

5. Data Protection for Children and Restrictions Against Harmful Data Uses

The ADPPA would create additional federal data protections for minors, prohibiting collection of personal information from those under age 17 without affirmative express consent, barring targeted advertising to individuals under 17, and conditioning data transfers regarding individuals between 13 and 17 years old on express consent. ADPPA would also create a new Youth and Privacy Marketing Division at the FTC that would be responsible for enforcement.

The bill takes an approach to child privacy that FPF has long recommended - it grants important protections to young people aged 13-17 while declining to extend parental access provisions to

[9] In 2012, Prof. Lorrie Faith Cranor and Aleecia McDonald, privacy experts and researchers at Carnegie Mellon, estimated that reading every privacy policy that the average American encounters in a year would take 76 work days. Given the increased integration of technology into everyday life, it is likely that number has increased greatly in the decade since the study.
https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

teens. These protections are increasingly important as more teens use digital services, but the parental access provisions COPPA provides to children can raise privacy and safety issues when applied to teenagers.

Overall, these ADPPA's protections are more comprehensive than those set forth in recent state laws, either in terms of the ADPPA's substantive provisions, coverage ages, or the investigative and enforcement resources provided.

The ADPPA would also provide heightened protections for other types of sensitive consumer data, including government-issued identifiers, genetic information, biometric data, and intimate photos and videos. The sensitivity of data is often contextual, and state law approaches to regulating it have met with varying degrees of success. Some laws regulating sensitive data have failed to account for evolving technologies, leaving novel data sets under regulated. Other state laws concerning sensitive data have been critiqued for inadvertently imposing burdensome requirements on emerging technologies that pose few privacy risks. The ADPPA provides a regulatory mechanism for recognizing new categories of sensitive data under the law; it would also be helpful to include a mechanism to provide additional clarifying guidance regarding the scope of the definitions for sensitive data categories.

6. Privacy by Design and Data Minimization

The ADPPA's privacy by design provision 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 ("Data Protection by Design and by Default"),[10] 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.[11] 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).

III. Comparing 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

[10] Article 25
[11] Ann Cavoukian; https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

and organizations' 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 individuals from outside the US covered by comprehensive data privacy frameworks like the GDPR.

Any new privacy law creates risks - risks of uncertainty and unintended consequences for individuals and organizations, risks of inconsistent legal obligations to businesses, and more. New privacy frameworks generate 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 organizations subject to other global regimes - including Europe's GDPR - can utilize or build on years of previous compliance work.

Similarities to GDPR

ADPPA compares favorably to GDPR in a number of respects. For example, ADPPA matches GDPR in defining a 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 ADPPA and GDPR, commercial entities and not for profits 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 personal 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 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, which 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.

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.[12] The ADPPA also does not cover publicly available personal information and employee data, as 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**. The 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 GDPR and ADPPA prohibit the processing of specific categories of sensitive data, with exceptions based on consent and other limited grounds. However, 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 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 ADPPA, similar to how it manifests as an overarching principle in the GDPR.

5. **The identical standard for valid consent under GDPR and 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. At the same time, it 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 ADPPA appropriately protects individuals, is workable for businesses, and there are not unexpected or undesired consequences. Below are four recommendations that would improve ADPPA:

[12] The 1974 Privacy Act applies to federal agencies, and states have passed comparable laws.

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 the 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 the 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 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 authorize 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 and the recognition that certain types of privacy-enhancing technologies may change.

3. **Intersection with Other Federal Laws**

The ADPPA takes a practical approach to preserving longstanding federal privacy laws (COPPA, FERPA, HIPAA, etc.). Individuals and companies have established understandings of rights and responsibilities under these laws, and the ADPPA largely preserves these frameworks. However, any comprehensive privacy bill can generate unexpected outcomes when it intersects with decades-old statutes, regulations, agency guidance, and interpretive jurisprudence. We

recommend that Congress analyze the intersection of these laws from a compliance standpoint and create more clarity when appropriate so that consumers and businesses can better understand how the ADPPA intersects with specific provisions of the existing federal privacy regimes.

For example, the ADPPA preserves the COPPA statute and rule, but the ADPPA includes a limited private right of action that COPPA lacks. Under one interpretation, this could produce a counterintuitive result, with teens granted an enforcement mechanism against unlawful data processing that would be unavailable to children.

Another potential anomaly could arise from the inclusion of childrens' data in the ADPPA's "sensitive covered data" category. The provisions for processing "sensitive covered data" do not include a knowledge standard. This is unsurprising, because nearly all of the sensitive data categories can be identified by examining the data. For example, few compliance experts are likely to mistake a list of account login credentials or genetic data for other, less sensitive data. However, the fact that data was collected from a child may not be obvious on its face or easily distinguishable from data collected from adults. And the ADPPA places substantively different obligations on entities that serve targeted advertising or engage in onward data transfers involving adults' versus childrens' data. Those who process data from minors or from "general audience" products and services will likely benefit from 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 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 the legislative history, subsequent rulemaking, or informal guidance from the FTC. There would be a particular benefit in identifying circumstances in which ADPPA terms align with existing federal sector laws or with the GDPR; both could be 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, *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 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." Data driven research is the lifeblood of public health, clinical research, and

has been proposed as one part of a practical approach to platform accountability. An expanded research exception, aligned with research best practices and subject to common sense ethical review and privacy safeguards, would be welcome.

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 most other global frameworks, including the GDPR, as well as in some of the state laws in the US, the relationship between controllers and processors is governed by a Data Processing Agreement - a contract where the obligations of each are laid out, confidentiality obligations are established, as well as rules about what happens to personal information once the relationship between controllers and processors ends. In contrast, the current Draft applies obligations broadly to all "covered entities," with only limited exceptions for service providers. It also does not include the obligation for covered entities and service providers to enter an agreement. The definitions are likely to create conflict when obligations of the service providers are in conflict with restrictions of certain controllers.

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 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; ADPPA compares favorably to global frameworks, including the GDPR. This is a monumental feat that should be celebrated by all involved. Of course, 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 move forward thoughtfully and expeditiously to find common ground on these critical issues.

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

ADDENDUM

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)* [13]

	ADPPA	**California Privacy Rights Act** [14]	**Other Laws (Colorado, Connecticut, Virginia, and Utah)** [15]
Covered Entity Threshold *(the requirements for an entity to be subject to the law)*	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.	Either has: - Annual revenue >$25 million; - Annually buy, sell, or "share" personal information of 10,000+ consumers; OR - Derive 50% annual revenue from selling or sharing personal data for behavioral advertising	- 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/process personal data of 25,000 state residents
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

[13] 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.

[14] 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.

[15] 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

readable format to another entity)			
Opt-In Consent *(an individual must affirmatively consent for an entity to collect or use certain data)*	For: - Sensitive covered data - Adolescent data transfers (13–17); - Retention of data beyond its processing purpose; and - Service provider transfers of covered data to other entities.	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.	All other state laws require opt-in consent for ***sensitive data*** and inconsistent secondary uses of data (except Utah). Connecticut requires opt-in consent for sales and targeted advertising using adolescent data (13-15).
Opt-Out Rights (*the right of an individual to cease being subject to certain processing activities)*	For: - Targeted advertising - Data transfers Does not require for automated decision-making or profiling	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.	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
Global/Unified Opt-Out *(Automated exercise of opt-out rights through user-enabled signals)*	Required if found feasible by FTC within 18 months	Yes	Included in Colorado and Connecticut; excluded in Virginia and Utah
<u>Business Obligations</u>			
Privacy Notices *(information provided about an entity's actions taken with respect to personal data)*	Yes, plus **short-form notices** for 'large data holders'	Yes, but no short-form notice requirement.	All require privacy notices, but do not require short-form notices.
Data minimization *(the requirement to limit data collected and retained as necessary for the purpose)*	Yes	Yes (pending regulations)	Most state laws have <u>limited</u> minimization principles connected to privacy notices.
Privacy by Design (*requirement for entities to consider privacy risks in the design, development, and implementation of products)*	Yes	No	No
Prohibited processing activities (*prohibits the collection and use of certain data unless the purpose falls within an exception, including affirmative express*	Yes, including - SSNs - Precise geolocation information - Biometric information - Password - Non-consensual intimate	No	No

consent)	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.		
Data security provisions (*requiring entities to implement certain security measures)*	Yes, additional obligations for 'large data holders'	Yes	Yes
Civil Rights Provisions and AI (*providing that data processing cannot discriminate against protected classes)*	Yes, plus requires algorithmic impact assessments and design evaluations.	Limited to complying with existing laws. Does not require algorithmic assessments.	Most state laws have civil rights provisions limited to complying with existing laws. None require algorithmic assessments.
Privacy Impact Assessments (*technical assessment to identify and document privacy risks for systems and processes)*	Yes (applicable to 'large data holders')	Yes (assessments required for risky processing activities)	Yes (assessments required for risky processing activities). Not required in Utah.
Specific 'Data Broker' Requirements (*requirements for entities that collect data from secondary sources, aggregate, and sell the data to other entities)*	Yes, requires "third-party collecting entities" to register with the FTC and honor a **"Do Not Collect" mechanism**.	No	No
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)*	Yes	Yes	Yes (limited in Utah)
<u>Enforcement</u>			
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 & 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

(ability of regulatory bodies or executive agencies to create rules; and the scope of this authority)	the FTC for identified provisions		law contains rulemaking provisions.
Enforcement of Arbitration Agreements (*provisions relating to the validity of pre-dispute agreements requiring individuals to arbitrate any potential claims and waive judicial redress)*	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.	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.	No
Safe Harbors and Defenses (*compliance mechanisms that prevent or provide protection against enforcement actions)*	Yes - technical compliance programs and commission approved compliance guidelines.	No	No