ITI Promoting Innovation Worldwide

# Written Testimony of


## John S. Miller
## Senior Vice President of Policy and General Counsel
## Information Technology Industry Council (ITI)


## Before the

## Committee on Energy & Commerce
## Subcommittee on Consumer Protection & Commerce

## United States House of Representatives

# *PROTECTING AMERICA'S CONSUMERS: BIPARTISAN LEGISLATION TO STRENGTHEN DATA PRIVACY AND SECURITY*

## June 14, 2022


*Global Headquarters*
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

*Europe Office*
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

ITI Promoting Innovation Worldwide

**Written Testimony of**

**John S. Miller**
**Senior Vice President of Policy and General Counsel**
**Information Technology Industry Council (ITI)**

**Before the**
**Committee on Energy & Commerce United States House of Representatives**
**Subcommittee on Consumer Protection & Commerce**

***PROTECTING AMERICA'S CONSUMERS: BIPARTISAN LEGISLATION TO STRENGTHEN DATA PRIVACY AND SECURITY***

**June 14, 2022**

Chairwoman Schakowsky, Ranking Member Bilirakis, Chairman Pallone, Ranking Member McMorris Rodgers, and Distinguished Members of the subcommittee, thank you for the opportunity to testify today. I am John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1] I lead ITI's Trust, Data and Technology Policy team, driving ITI's strategy and advocacy on privacy and data protection, cybersecurity and supply chain resiliency, government access to data, digital platforms, artificial intelligence, data policy, Internet of Things, cloud computing, and other technology and digital policy issues. I have developed deep expertise on privacy, data protection, and data security policy and legal issues over the past sixteen years, including advising governments and policymakers on these issues, both domestically and globally, at a large multinational technology company as well as at ITI.

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry. We represent leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, Internet companies, and other organizations using data and technology to evolve their businesses.[2] Privacy is a longstanding ITI policy priority, as protecting privacy is integral to establishing and maintaining the consumer trust that is integral to our members' businesses. Consumer trust is a key pillar of innovation, and the industry I represent today recognizes it must do everything it

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

[2] See ITI membership list at: https://www.itic.org/about/membership/iti-members

can to deepen that trust and make sure we meet our customers' expectations when it comes to protecting their privacy and personal data.

ITI commends Chairman Pallone, Ranking Member McMorris Rodgers, and Senator Wicker for your work on the American Data Protection and Privacy Act (ADPPA), the discussion draft that is the subject of today's hearing. The technology sector has for several years shared your goal of enacting comprehensive federal privacy legislation, and the ADPPA represents welcome and tangible progress toward that goal. In terms of both its scope and potential impact, the draft bill represents not only a significant contribution to the evolving domestic and global conversation on privacy legislation, but arguably an inflection point on par with Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), due not only to robust protections it aspires to achieve for the American people but also for its wide-ranging and potentially disruptive impact on businesses across every sector of the U.S. economy and data innovation, including longstanding business models that have helped fuel the internet's development and corresponding economic growth. The ADPPA deserves to be taken seriously and thoughtfully considered by all stakeholders as the most credible bipartisan and bicameral effort yet to advance comprehensive federal privacy legislation in the United States, but we also need to acknowledge the bill needs substantial improvement, and we look forward to continuing to constructively engage with you and your staff as the bill moves forward.

ITI has long called for federal privacy legislation and shares many of the committee's concerns and priorities regarding individuals' personal data use and protection. In 2019, we released our *Framework to Advance Interoperable Rules (FAIR) on Privacy*.[3] Our FAIR Privacy framework seeks to move the conversation forward on federal privacy legislation by offering a flexible model that enhances transparency, increases consumer control, establishes company accountability, promotes data security, and calls for meaningful enforcement, oversight, and redress mechanisms. It is also important to note that we drafted the FAIR Privacy framework against the backdrop of Europe's GDPR having recently come on line, the CCPA's passage into law, and while many other comprehensive privacy bills were being considered in major global markets and several U.S. states. ITI's FAIR Privacy framework aspires not only to serve as a roadmap for a federal law in the United States but to create alignment with the privacy protections of other privacy regimes across the globe, enable interoperability with these global approaches, and avoid a fragmented approach to privacy at the U.S. state level.

Unfortunately, in the ensuing three years we have observed several more U.S. states and markets passing their own privacy laws including Colorado, Virginia, Utah, and Connecticut, as well as the passage of an additional law in California, the California Privacy Rights Act (CPRA), which amends CCPA and will come into force in 2023. Additionally, Brazil, China and over 140 other countries have passed privacy legislation, while the United States has continued to lag on making appreciable progress on a privacy law at the federal level. The technology sector recognizes maintaining the status quo and this current path is unsustainable. First, it leads to uneven and confusing protections for individuals in the United States that vary from state to state, and which are not on par with the protections of their peers globally. Second, the feared increasingly fragmented regulatory landscape is fast becoming a reality that exhausts resources and disproportionately impacts U.S. businesses. And finally, with every day that goes

[3] Framework to advance Interoperable Rules on Privacy
https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules(FAIR)onPrivacyFinal_NoWatermark.pdf

by without a federal law, the stature of the United States as a leader on the global privacy stage is diminished. We are hopeful the ADPPA can provide the much-needed impetus to change this trajectory.

I will focus the balance of my written testimony on three areas: (1) briefly reviewing the core elements of ITI's FAIR Privacy and noting where ADPPA positively aligns, while also flagging important divergences; (2) assessing some of the most significant areas where we believe ADPPA must be strengthened, including clarifying several key definitions and improving and refining other portions the discussion draft; and (3) evaluating the polarizing provisions on preemption and a private right of action.

## I. ITI's FAIR Privacy Framework and the ADPPA

ITI's FAIR Privacy framework sets forth specific ideas to advance the privacy rights of individuals and makes explicit the responsibilities of tech companies in using personal data while acknowledging the many different contexts in which individuals and companies interact with data. It proposes establishing context-based individual control rights for consumers to ensure meaningful transparency and a clear understanding of their choices relative to the use of their personal data.

Our FAIR Privacy framework also clearly defines an entity's responsibilities around handling personal data to hold them accountable, thereby ensuring companies use personal data responsibly and transparently. However, it also allows for variance in those obligations based on the extent to which an entity determines the purposes for and manner of use of personal data and makes certain that accountability obligations travel with data transferred to other entities' (such as service providers) for their own use. Finally, and importantly, ITI's FAIR Privacy framework seeks to protect individuals' privacy while avoiding the onerous process requirements that can degrade the user experience, inject unnecessary costs into the ecosystem, or otherwise deter continued innovation and the participation of small- and medium-sized enterprises in the digital economy.

The ADPPA shares many similarities to ITI's FAIR Privacy framework, although there are also important differences. Like ITI's framework, the discussion draft establishes robust individual control rights, putting consumers in the driver's seat when it comes to their personal information and giving them the right to expressly and affirmatively consent to the use of their sensitive personal data. However, the definition of sensitive data in the ADPPA is not only broader but in important respects less clear than that which we contemplated (or exists in other comprehensive privacy laws).

Like ITI's FAIR Privacy framework, the ADPPA requires companies to maintain robust data security programs and employ data minimization practices. ITI's framework seeks to ensure that such security programs and minimization practices are calibrated to not only the size of companies but a series of factors and considerations appropriate to the manner, purposes and context by which companies use personal data, and while the ADPPA acknowledges many of these same context-specific considerations, it additionally layers several prescriptive security requirements on all companies, which they may be inadvertently barred from implementing due to other provisions in the bill, and includes a minimization requirement that can be read expansively to prohibit all forms of processing not falling under a permitted purpose.

And like ITI's FAIR Privacy framework, the ADPPA calls for strong accountability and oversight. However, while our framework similarly called for an oversight body such as the Federal Trade Commission (FTC) to be appropriately resourced including with the technical capacity needed to regulate effectively to protect individuals, for companies to maintain records pertaining to their use of data, risk assessments, and security programs so that they are auditable in the event incidents do occur, and for individuals to have the right to redress mechanisms that ensure their rights are adequately protected, the ADPPA goes significantly further, imposing unnecessary and unprecedented prescriptive requirements on companies to perform algorithmic impact assessments and design evaluations, and elevating a broad private right of action in a manner that may make it the preferred form of redress.

I will discuss the principal issues touched on in this section in more depth below.

## II. Recommendations to Strengthen the ADPPA

One of the most critical parts of any bill is the "definitions" section, and the ADPPA is no exception. The scope of the protections bestowed to individuals, obligations imposed on companies and the potential impact of the enforcement provisions all flows from these key provisions. In our view, there are several key definitions in the discussion draft that must be clarified and tightened up to ensure that the bill achieves what should be its primary purpose of protecting individuals' privacy and personal data without unnecessarily undermining data innovation.[4] I highlight a few of the most problematic definitions below as well as a couple of other important provisions in the discussion draft that we believe must be recalibrated (please do not consider this an exhaustive list).

### *a. "Sensitive Covered Data"*

The definition of "sensitive covered data" under Section 2(22) is overly broad in numerous respects and out of step with sensitive data definitions in similar laws at the U.S. states and globally, render many critical internet functions difficult if not possible to perform, and is in some ways inconsistent with other provisions in the discussion draft.

Perhaps the most problematic section is 2(22)(A)(xi), which includes "information identifying an individual's online activities over time or across third party websites or online services," thus seemingly subjecting all online activity relating to individuals to opt-in consent. This broad definition, would, for instance, render routine browsing activities performed by users difficult, arguably requiring them to provide opt-in consent every time they logged into a search engine. Perhaps more concerningly, this provision would effectively eliminate the ability of companies to perform the cybersecurity analyses necessary to prevent cyber-attacks (including those required by the data security provisions in the bill), or act as content delivery networks, or do many other things requiring the processing of unique identifiers such as IP addresses (i.e., information identifying an individual's online activities) necessary for these functions.

[4] While I will offer constructive feedback aimed at improving a few specific provisions in the discussion draft, I want to make it clear that this is not an exhaustive list, and that we will offer additional written feedback to staff including technical edits as we continue to receive and consolidate feedback from ITI members.

One recommended improvement to section 2(22)(A)(xi) would be to replace the "or" in the language cited above with an "and" so that this subpart of the definition would read: "information identifying an individual's online activities over time **and** across third party websites or online services."

Beyond "online activities," what qualifies as "sensitive covered data" is in numerous other respects very broadly defined and would include any telephone number, text, email, voicemail, or phone or text logs, amongst other things. The discussion draft thus greatly expands the definition of what is considered sensitive data in existing prominent global privacy laws and U.S. state laws. The implications of this expansion are at least twofold: first, it elevates several seemingly "ordinary" categories of personal data (such as telephone numbers which are publicly available in phone books) to be on par with obviously sensitive data such as social security numbers, health or biometric data; second, requiring affirmative express consent to collect, process, or transfer all sensitive covered data would extensively impact many companies who may simply be unable to comply with these provisions. For instance, given many service providers are business-to-business (B2B) companies that may not have direct relationships with or access to consumers so as to be able to obtain the required consent, the result of the overbroad sensitive data definition is to create an unworkable situation where a service provider could be held liable for a covered entity's failure to appropriately gain consent, including in instances where a consumer decides to do something as ordinary as changing their phone number.

We recommend recalibrating the definition of sensitive covered data in the discussion draft to better align it with the definitions of "sensitive data" in other privacy laws.

*b. "Covered Entity" and "Service Provider"*

One of the reasons ITI built context into our FAIR Privacy framework was because while each one of our eighty companies uses data every day, they each use data differently, both in their internal operations in how they interact with their different types of customers, and in how they use data to innovate and continue to drive their businesses forward. Each one of those eighty companies also have a unique business model and will experience the impacts of the ADPPA differently should it become law. The same is true of every other U.S. business, because data is important to all of them, and the multiplicity of ways that companies use data is matched by the potential impacts the ADPPA would have on their businesses, their technology products and services, their employees, and their customers.

While the bill makes an effort to distinguish the responsibilities of entities based on their size (e.g., by creating separate obligations for "large data holders" and an exception for "small data" entities), it does not carefully distinguish the obligations of the different types of entities that use data. In particular, it does not clearly differentiate the responsibilities of "covered entities" (or what are commonly referred to as "data controllers" under the GDPR, or entities that determine the purposes for which and the means by which data is processed) and "service providers" ("data processors" under the GDPR, or entities that processes personal data only on behalf of a controller). The so-called data controller/data processor distinction is made clear not only in the GDPR but in other comprehensive privacy legislation globally and in the United States (indeed, the distinction is clear in all five U.S. state bills).

Given the complex and variable relationships between entities in the data ecosystem, it is essential to clearly delineate between the roles and responsibilities of covered entities/controllers and service providers/processors for a privacy law to function effectively. For example, there are times when a company will act as a covered entity/controller that is deciding the means or purposes of managing and

processing data, while at other times, that same company will act as a service provider that is processing data on behalf of a covered entity/controller solely at their direction and under a contract. Covered entities and service providers should both be regulated under the ADPPA (or any federal privacy law), but it is imperative for the law to assign the appropriate role-based obligations to controllers and service providers so as to apportion their responsibilities and potential liabilities clearly.

Unfortunately, the discussion draft does not clearly delineate between "covered entities" in sec. 2(9) and "service providers" in sec. 2(23), and in fact the definitions could be read as imposing greater obligations on the service providers, flipping the typical controller/processor paradigm, even though the processors often lack access to data they do not control. We recommend the discussion draft be modified to define these terms more crisply in line with other major privacy legislation or at least try to distinguish the obligations of "covered entities who are not acting as service providers" rather than lumping these different entities together.

*c. "Covered Data"*

Amongst other things, several aspects of the definition of "employee data" as defined under "Covered Data" under Section 2(8)(C)) should be clarified. First, the definition should be further strengthened to include information that laws require employers to collect about employees, such as diversity data. Second, employees should not be able to demand deletion of such data if employers collect it pursuant to legal obligations. Third, subpart (ii) of the definition of Employee Data assumes that the business contact details of an employee will be provided to the employer. In practice, it is often the other way around with employers providing business contact details to the employee.

*d. "Targeted Advertising"*

As stated above we believe the ADPPA or any comprehensive privacy law should have a dual objective - protecting the privacy of Americans while also preserving data innovation, including the business models that have helped the internet thrive and powered the growth of the global internet economy.

We have concerns that as presently drafted, the definition of "targeted advertising" in sec. 2(26) would simply preclude the ad-supported internet business model to continue, as publishers would not be able to use their knowledge of the preferences and interests of their users to show ads. We would suggest changes that would bring the definition more in line with the definition of "targeted advertising" that was included in recent privacy laws passed by Virginia, Colorado, Utah, and Connecticut. The definitions in those states struck the right balance to enable internet companies to reasonably advertise to their users on their sites while protecting their privacy interests.

We recommend limiting the definition of "targeted advertising" in sec. 26(A) to the use of data collected over time ***and*** across third party websites or online services. This edit would be consistent with the approach taken in the state bills and also consistent with a similar edit we suggested making to the "sensitive data" definition as related to "online activity." We additionally recommend revisiting the exceptions in the definition under sec. 26(B)(ii) for first party advertising and sec. 26(B)(iii) for contextual advertising as they seem unnecessarily limiting given the trust relationship companies typically have established with users of their own sites or apps.

Beyond the critical definitions reviewed above, there are other provisions in the discussion draft that the committee should consider revamping, including those relating to algorithms and cybersecurity.

*e. Algorithmic Impact Assessments and Design Evaluations*

With respect to Algorithms and Civil Rights under Section 207, ITI shares the firm belief that building trust in the era of digital transformation is essential and agrees there are important questions that should be addressed regarding the responsible development and use of algorithms. We are also aware of existing concerns regarding potential negative outcomes related to the use of algorithms and are participating in related existing efforts underway at the Department of Commerce around AI risk management, explainability and mitigation of AI bias at the National Institute of Standards and Technology (NIST) and privacy and civil rights at the National Telecommunications and Information Administration (NTIA). We encourage the Committee to consider these ongoing federal workstreams as a potential guide to future legislative efforts rather than prematurely including in the discussion draft prescriptive requirements to conduct algorithmic design evaluations and impact assessments, which are unprecedented not only in privacy laws globally but even laws more squarely focused on related topics such as artificial intelligence.

*f. Cybersecurity Exceptions*

While the legislation is appropriately focused on consumer privacy rights, including data security, the combination of vague definitions and somewhat haphazardly aggregated general exceptions in section 209 could easily implicate all sorts of enterprise focused, B2B activity that could have serious unintended consequences, particularly on cybersecurity.

For example, large swaths of internet and network telemetry used for real-time cybersecurity defense and security automation activity could be considered covered data (and potentially sensitive covered data due to the geolocation provision). Additionally, as mentioned above, given IP addresses, a foundational data point of cybersecurity vulnerability management, are considered a unique identifier despite being publicly available information and thus also categorized as sensitive covered data requiring consent, the ADPPA as drafted could create substantial headwinds for routine, enterprise-focused cybersecurity activity.

We suspect cybersecurity activity is not intended to be negatively impacted by this legislation. While section 209 does include a general exception "to detect or respond to a security incident or fulfill product or service warranty," and another “to protect against fraudulent or illegal activity,” the exceptions as written do not clearly include cyber defense activity where large swaths of network data are analyzed in real-time for the purpose of preventing security incidents.

We would encourage the Committee to explicitly include security incident *prevention* in the exception, amongst other changes. Detecting or responding to a security incident means the incident is already happening, and we want to ensure we do all we can to enable companies to protect consumers by preventing an incident in the first place.

## III. Evaluation of ADPPA’s Enforcement Provisions and Preemption

As the committee considers our recommendations for improvement, I would urge you to not lose sight of the fact that edits to specific provisions should not be considered in isolation, and that you should stay focused on how these provisions interrelate to and impact each other. In other words, a change to

one section may well have an impact on a host of other sections. That is certainly the case when it comes to some of the key definitions, but also to other sections such as the enforcement provisions.

As mentioned above, ITI is on record in our FAIR Privacy framework as supporting strong redress and enforcement as essential to protecting American citizens' privacy rights. The discussion draft contains multiple prongs providing strong redress and enforcement, including robust FTC rulemaking and enforcement authorities including the establishment of a new bureau dedicated to enforcing the ADPPA (sec. 401) and enforcement by state attorneys general (AG) (sec. 402). These authorities must be evaluated in the context of the existing FTC and AG enforcement regimes, which are substantial and, by way of comparison, do not need to be built from the ground up as has been the case with other privacy regimes that have recently come on line (such as Brazil's LGPD).

Of course, the discussion draft notably includes a Private Right of Action (PRA) (sec. 403), and reasonable minds can disagree as to whether a PRA is necessary in light of the other strong enforcement provisions. While we appreciate staff's efforts to narrow the PRA provision, our members remain concerned that it is too broad and will not appreciably limit a likely wave of litigation, for at least three reasons. First, while it is true neither punitive nor statutory damages are permitted under the PRA, the availability of attorney's fees could encourage the filing of borderline meritorious cases by specialized attorneys charging exorbitant hourly rates. Second, while plaintiffs must provide 60 days' notice to the FTC and/or AGs to allow them to take over a case, the somewhat illogical result this approach may lead to may be that the *less* meritorious cases are the ones that will be pursued by private litigants in court. Third, and perhaps most importantly, the previous section summarized several key definitions in the discussion draft that are broad and/or unclear such as the key terms "sensitive data" and "covered entity"/"service provider" - the problems with these unclear terms will only be exacerbated by the availability of a PRA because lawsuits will inevitably be required to clarify which entities have what obligations under the law unless the definitions are substantially tightened.

The goal of the ADPPA or any privacy law should not just be to protect American citizens' privacy, but to do so in a way that does not unnecessarily hamstring U.S. businesses and continued data innovation. In the context of the discussion draft when considered as a whole, the PRA as currently drafted misses this mark. The committee should consider other reasonable limits on a PRA in order to allow consumers the ability to enforce their rights without subjecting industry to broad class action liability in lawsuits where there is no demonstrable harm to consumers. For instance, section 303 grants the FTC authority to issue regulations to establish a process for the proposal and approval of technical compliance programs for covered entities. The FTC, State AGs and courts must consider a covered entity's history of compliance with these programs in actions brought pursuant to sections 401-403. One idea worth considering is whether section 303 could be further strengthened, such as by considering whether submitting to a technical compliance program might be considered as a "safe harbor" to guard against the potential abuse of the PRA provision.

We stand ready to work with Committee staff to explore whether the PRA can be meaningfully cabined in this or other ways so as to reasonably maintain individuals' ability to pursue their rights without unnecessarily damaging businesses and the American economy.

With respect to preemption, ITI has long advocated for the inclusion of preemption in any federal privacy law, and we appreciate the ADPPA expresses the intent to preempt state consumer privacy laws covered by the provisions of the bill (sec. 404(b)). It appears the intent of the preemption clause is to be broadly preemptive subject to the specific exceptions in the savings clause. To clarify this intent, it would be helpful to note that the bill preempts not just laws that are specifically "covered by the provisions of this Act" but all laws "relating to the subject matter covered by this Act" minus the explicit exceptions.

Regarding the exceptions, the lengthy list of state laws that is preserved seems to include some laws that are at least in part covered by the ADPPA (e.g., Illinois' Biometric privacy law (BIPA)), but not other similar laws (e.g., Texas' biometric privacy law.) At a minimum, we would like to better understand the Committee's rationale for preempting some specific existing state privacy laws and not other similar laws.

The discussion draft explicitly preserves state consumer protection laws of general applicability in section 404(b)(2)(A), and we note the bracketed language there, which would prohibit pleading the fact of a violation of the ADPPA as an element of a violation of state consumer protection laws. These brackets should be removed because without this limitation the preemption clause would be rendered somewhat meaningless.

**Conclusion**

ITI and our member companies appreciate the committee's attention to this matter and its effort to develop a compromise solution to advance comprehensive federal privacy legislation. We share the committee's goal of enacting comprehensive federal privacy legislation, and we are committed to working with the Committee, others in Congress and the stakeholder community to find common ground. This is a highly complex bill impacting every American citizen's privacy rights and nearly every American company's ability to operate and innovate. We all agree we need to get privacy legislation done. But we should also all agree need to get privacy legislation right, because the stakes are too high.

If we take a clear-eyed view of the ADPPA, we must acknowledge that the bill is not perfect. But we must also fairly acknowledge the discussion draft represents arguably the best chance we have ever had to move the ball forward on federal privacy legislation to prove to American citizens and the world that the United States takes privacy seriously and protects it in a way that maintains American companies' continued leadership in driving innovation globally.

As ITI continues to gather feedback on the discussion draft of the ADPPA from its member companies, we look forward to sharing that feedback with the committee. Thank you again for the opportunity to testify today, and I look forward to your questions.