Information Accountability Foundation

Cleanup In Aisle ADPPA

Marc Groman
March 2023

This page was intentionally left blank.

CLEANUP IN AISLE ADPPA

THE PUNCHLINE

A tremendous amount of work went into drafting the American Data Privacy and Protection Act (ADPPA). It's an impressive bipartisan effort on an important issue. A federal privacy law is long overdue in the United States. That said, the current version is difficult to interpret and if enacted into law would be challenging to implement and enforce. This comment is not a criticism of substantive decisions or policy compromises but rather a non-partisan observation that the language in the draft ADPPA deviates from the basic principles of sound and effective legislative drafting, producing an incoherent framework. Vague and ambiguous definitions, undefined terms, inconsistent and imprecise use of different words to mean the same or similar ideas, and the almost compulsive use of modifiers (e.g., reasonable, significant, substantial, material, consequential) make compliance a guessing game and enforcement unduly challenging. Without significant revisions to the text, the enacted ADPPA will be bogged down in courts for years as judges attempt to divine the intent of Congress.

The good news is that there's plenty of time if Members of Congress and stakeholders roll up their sleeves and take out their pens. Drafting federal legislation is an arduous task, more difficult than most people appreciate. Guidelines, best practices, and conventions for legislative drafting help achieve consistency from statute to statute, making federal laws, at least in theory, easier to read, understand, and follow. One such handbook, which I used when I worked on the Hill, recommends that federal laws be "written in plain English for real people." Although the draft ADPPA primarily will be read by lawyers and lobbyists, not real people, it still needs significant work if the ADPPA is going to work. As the draft ADPPA winds its way through the legislative process, staff and stakeholders should complete a line-by-line, word-by-word review of each provision so that the legislative language—the black and white text on the pages—is as clear as possible and does what people believe it was drafted to do.

RECAP - ADPPA HAS MOMENTUM

With so much legislative activity in the states, it's easy to forget about the draft ADPPA. Please don't. Congress hasn't. On March 1, the House Subcommittee on Innovation, Data, and Commerce held a hearing, "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." The Energy and Commerce Committee Majority Staff Memo set the stage and provided Members with relevant background.

> Due to the ubiquitous, insidious, and pervasive nature of data collection and Americans' increasing awareness of these practices, data privacy and security has become a major concern…. To ensure all Americans receive strong privacy and data security protections, and all businesses have clear rules of the road to operate within, the U.S. *must* enact a comprehensive and preemptive privacy and data security law so that it can maintain its leadership on the world stage.

The Staff Memo summarized the draft ADPPA's short but remarkable history. In the 117th Congress Reps. Pallone (D-NJ), Rodgers (R-WA), Schakowsky (D-IL), and Bilirakis (R-FL) introduced H.R. 8152, the "American Data Privacy and Protection Act" on June 21, 2022. The draft ADPPA subsequently passed out of the House Energy and Commerce Committee by a 53-2 vote. That is extraordinary. A more complete summary of the draft ADPPA's history is documented in the Committee Report.

In the last Congress, House Speaker Nancy Pelosi declined to bring the draft ADPPA to the House floor, based on concerns that it would preempt California's stronger privacy laws. Both Rogers and Pallone (Commerce Committee Leadership) disagreed, issuing a strong bi-partisan statement in support of the draft ADPPA.

> The [ADPPA] puts people back in control of their online data and includes the strongest privacy protections to date for children online. We remain 100 percent committed to passing ADPPA this Congress.

In the current Congress, Rogers and Pallone continue to lead the Commerce Committee, although Rogers is now Chair, and Pallone is Ranking Member. Rogers remains committed to moving the draft ADPPA through the Committee to the full House.

> We…. [should pass] comprehensive privacy and data security protections with one national standard. We made history last year when we passed the bipartisan, bicameral [ADDPA] 53-2…. This is a top priority for Americans and needs to be achieved through Congress.

On the other hand, Kevin McCarthy is now Speaker, and he does not share Pelosi's concern about California privacy law, removing a significant obstacle from future consideration of the draft ADPPA. Off the Hill, diverse stakeholders vocally support the draft ADPPA. Notably, 48 civil rights, privacy, and consumer organizations sent a letter to Speaker Pelosi last year urging her to move the draft ADPPA to a vote by the full House of Representatives.

> ADPPA is comprehensive federal privacy and civil rights legislation that will…create real and lasting protections for the personal data of …consumers in America…. The bill…is the product of input from a variety of stakeholders across the political spectrum… [and] is a meaningful compromise that has bipartisan support.

More recently, at the March 1 hearing, Alexandra Reeve Givens, President and CEO of the Center for Democracy & Technology, testified that "ADPPA represents a reasonable middle ground for protecting privacy and civil rights online, and we encourage this Committee to take it up again without delay." Graham Mudd, Founder & Chief Product Officer of Anonym, Inc, similarly praised the draft ADPPA, "We at Anonym share your belief that the ADPPA has the potential to mark a historical watershed in privacy law and policy."

ADPPA has momentum, and that's a good thing. We need a comprehensive federal privacy law. I'm concerned, however, that stakeholders have turned their attention elsewhere. That's a mistake. Some version of the bipartisan bill may well become law in the future. At a minimum, the draft ADPPA is now the baseline starting point for discussions about privacy legislation in Congress. Moreover, the draft ADPPA has become a template for a statehouse-by-statehouse campaign to enact new consumer privacy laws.

CLARITY, CONSISTENCY, AND CERTAINTY

A comprehensive, preemptive, federal privacy law that creates a single set of rules for the United States is a once in a generation effort that will impact our country and our economy for decades. The drafters should not force companies and courts down the road to guess what the text means. Given the very limited and narrow rulemaking authority granted to the Federal Trade Commission in the draft ADPPA, it's even more incumbent on Congress to get the text right so that, on a mechanical level at least, the draft ADPPA's directives can be followed and enforced.

My goal is not to slam the draft ADPPA, fuel opposition, or derail the effort. A federal privacy law is long overdue, and the draft ADPPA reflects an extraordinary bipartisan and collaborative process. Nor do I underestimate the challenge of translating vague concepts into legislative text, particularly as parties negotiate substantive compromises under tight deadlines. My sole objective is to motivate stakeholders to improve the text.

It is impossible to address in this article every line of text that could benefit from clarification or revision.. Hopefully, a handful of examples will illustrate my concern.

Defined Terms

The term "**Covered Algorithm**" could use refinement. The word "algorithm" strikes me as unrelated to the definition. It's like defining "covered vegetables" to mean apples, oranges, pears, and grapes. Congress can do that, but it's confusing. Second, the phrase "similar or greater complexity" arguably excludes actual algorithms and analytics that may cause the very harm the draft ADPPA seems intended to address. Finally, the term "Covered Data" in the definition of "Covered Algorithm" likely should be replaced with "an Individual." I believe we want to prevent or mitigate potentially problematic or harmful decisions made *about people*, not data.

The definition of "**Derived Data**" is circular. Derived Data is data that is "created by the derivation of …." Courts likely will need to refer to the dictionary definition of "derive" and "derivation" to understand the meaning, which defeats the point of defining a term. Even with Webster's help, there are multiple ways to interpret the definition, thereby narrowing or expanding the scope of the term. Flexible standards that evolve over time are needed, but ideally, the draft ADPPA should start with a clear definition.

After "asking around," I do not understand why the draft ADPPA defines "**Material**." "Material" is a well-established legal principle. There is extensive FTC law and guidance explaining the term. What is achieved by adding this definition? The confusion is exacerbated by the fact that "material" modifies different words in different provisions. Examples include material change, material facts, the material effect of each material change, materially different, and materially misleading. Does the definition apply in every context? Should it?

Finally, the term "**Substantial Privacy Risk**" also needs refinement. This term also suffers from the "covered vegetables" problem. This term requires a careful read. What does "in a manner" mean and why is it necessary? What does "reasonably foreseeable substantial" modify? What does substantial mean here? How does a Covered Entity determine when processing Covered Data creates a risk of a "highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances?" I'd think an "offensive intrusion" would suffice here and that "under the circumstances" isn't necessary if the standard is "a reasonable individual." That's shorter, but not necessarily better. The problem I am highlighting goes beyond this one definition. The absence of definitions in the draft ADPPA for fundamental terms such as “privacy,” “privacy risk,” “privacy expectations,” “harm,” “injury”, and “adverse consequences” is problematic. If Congress is going to define “Substantial Privacy Risk,” shouldn’t it first define “Privacy” and “Privacy Risk.” Without such guidance, how will a Covered Entity identify, assess, mitigate, and prevent harm, injury, or adverse consequences from processing Covered Data? More importantly, how does an agency enforce the provision? Congress hasn’t sufficiently defined the problems the draft ADPPA is seeking to solve or the harms the draft ADPPA is intended to prevent.

Undefined Terms

The absence of definitions for key concepts may lead to absurd results and unintended consequences. The drafters should make every effort to minimize the chances that a company, court or consumer will need to look outside the four corners of the document to comply with the law, much less understand it. Additional explanation will help elucidate the intent of Congress and promote consistency in interpretation and implementation, which will benefit all stakeholders.

A good example is the term “sensitivity” which, at least in the text as drafted, is not the same as “Sensitive Covered Data.” Is determining the “sensitivity” of Covered Data, as required in several provisions, different than determining whether Covered Data includes Sensitive Covered Data, a defined term in the draft ADPPA? If yes, how does a Covered Entity assess the “sensitivity” of Covered Data? If no, then the text should be revised.

Other undefined concepts include:

- Category of Sources of Covered Data
- Categories of Third Parties
- Categories of Service Providers
- Categories of Covered Data
- Demonstrably Impracticable
- Legitimate Request to Opt-Out

Even terms like “online” may benefit from additional clarification. The draft ADPPA appears to apply to all Covered Data regardless of source; online, offline, world-wide web, dark web, mobile, internet-of-things, brick-and-mortar stores, social media, anti-social media, virtual reality, paper records, etc. But some provisions apply to a subset of Covered Data and data sources, such as “online.” The intended scope of such provisions is not sufficiently clear.

Undefined Terms and the Undefined Problem. Mitigate the Risk of What?

The draft ADPPA is intended to prevent or mitigate negative outcomes (or an equivalent term) to Individuals arising from collecting, processing, or transferring Covered Data. The draft ADPPA, however, fails to identify and define those negative outcomes. The terms “harm,” “injury,” and “adverse consequences” are used in different provisions, but they’re never defined or explained, and it’s not clear why one word or term isn’t used consistently throughout the draft ADPPA.

The Committee Report offers some context, referencing sources such as the recent law review article Privacy Harm:

> Online privacy harms are well-documented, including unwanted observation from excessive data collection and secondary use, discrimination, harms to children and teens from manipulation and targeting, thwarted consumer expectations, and more.
>
> As more data is collected by Big Tech on individuals by more products and services necessary for everyday life, Americans are subject to more risks.

This discussion doesn't get us very far. First, it's not in the legislative text. Second, it offers an illustrative, incomplete list of "online privacy harms." Third, the "risks" that Americans increasingly face from data collection (the subject of the draft ADPAA) are not defined. None of these terms are straightforward or self-executing, which is one of the reasons why a clear national standard is so important. Privacy Harm, the article cited in the Committee Report, highlights the drafting problem and inevitable confusion.

- "Privacy harms have been a challenge to conceptualize because they are so varied. Privacy is an umbrella concept that encompasses different yet related things."
- "Privacy harms are highly contextual."
- "The law's treatment of privacy harms is a jumbled, incoherent mess."
- "Privacy harm is a conceptual mess that significantly impedes U.S. privacy law from being effectively enforced."

Given that there's no generally accepted definition of "privacy harms," Congress should clarify what it means to identify, evaluate, and mitigate the risk of privacy harm to individuals. What harms or consumer injury does the draft ADPPA assess? How will a Covered Entity determine if processing or the use of a Covered Algorithm "poses consequential risk of harm" or "may reasonably contribute to the risk of potential harms." What is a "Covered Algorithm that presents low or minimal consequential risk?" What is a "consequential risk?" Absent definitions and enforceable standards the privacy risk assessments required in the draft ADPPA become meaningless tasks that burden companies but provide limited, if any, benefit to consumers, the marketplace, or innovation.

Inconsistent And Imprecise Use of Terms

A fundamental principal of legislative drafting is "express like ideas in like ways." It also may be expressed as "use the same word over and over" and "do not use the same word in two different ways in the same text." This feels like nitpicking now, but it becomes pivotal later. When interpreting statutory language, Courts follow a presumption of consistent usage. A word or phrase is presumed to bear the same meaning throughout a text. When reading the draft ADPPA, I encountered several words or phrases that were used inconsistently. In some cases, different words seemed to be used to address the same idea, but I'm not sure. Thus, it would be worthwhile to review terms in the draft ADPPA to confirm that they have distinct and intentional meanings. Consider the following different words in the draft ADPPA that are used to express the same idea:

- Person v. consumer v. Individual v. user
- Injury v. harm v. adverse consequences v. privacy risk v. privacy impact

- risks v. privacy risks v. privacy impact
- nature of covered data v. sensitivity of covered data v. Sensitive Covered Data
- significant v. substantial v. material v. consequential

Unreasonable Use of Modifiers

Finally, best practices for drafting clear legislation counsel against the excessive use of modifiers. The draft ADPPA, however, has a dizzying number of modifiers to limit or restrict the meaning of simple nouns and verbs. There are even modifiers for modifiers. This drafting technique creates tremendous ambiguity and uncertainty. Every modifier inserted in the text of will, upon enactment, call for some sort of administrative judgment. When used sparingly, modifiers play an important role in legislation. We're all familiar with bedrock legal concepts such as substantial injury, material misrepresentation, and reasonable consumer. However, modifiers should be used judiciously and with precision otherwise they just muck everything up, even when they are inserted as part of a compromise.

Any one paragraph or provision when read in isolation may not be problematic, but when the draft ADPPA is considered in its entirety, implementation and enforcement challenges become apparent. As noted above, modifiers such as substantial, significant, material, consequential, strictly, and highly are used throughout the draft ADPPA. I suspect that different words were inserted at different times, and by different stakeholders or authors, leading to a confusing and potentially inconsistent set of standards. To the extent, for example, different levels of risk or injury are described, one clear, consistent set of modifiers (low, moderate, high, or significant etc.) should be used uniformly throughout the draft ADPPA. Ideally the different levels of harm or injury should be defined or explained with more than a vague adjective or adverb, or the Federal Trade Commission should be delegated the authority to more precisely define the terms through rulemaking.

And although statutes use the modifier "reasonable" in many contexts, at some point even the use of "reasonable" becomes unreasonable. In the case of the draft ADPPA, "reasonable" is everywhere and it's unclear if every use is necessary, intentional, or modifies the correct noun or verb. Some examples include:

- Reasonably necessary and proportionate
- Reasonable expectation of privacy
- A reasonable consumer's reasonable expectation
- Privacy expectations of a reasonable individual
- Reasonably necessary and proportionate residual risk to covered minors
- Highly offensive intrusion into the privacy expectations of a reasonable individual
- Reasonable time before a merger or acquisition
- Reasonable policies, practices, and procedures
- Sufficient for a reasonable individual to understand
- Reasonably anticipated within the context of the relationship
- Reasonable basis to believe
- Reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person …
- Reasonable efforts to notify
- Reasonably foreseeable substantial

- After a reasonable investigation, reasonable grounds to

Conclusion

I want a comprehensive, federal privacy law too. I'm concerned, however, that several Sections in the draft ADPPA are vague and ambiguous at best, impossible to interpret, implement, or enforce at worst. Such provisions incentivize data practices that are not in line with the stated objectives of the draft ADPPA, could leave consumers with less protections and fewer rights, may open companies up to enforcement for conduct that was not clearly unlawful, and stifle American innovation. It's a fundamental tenant of good writing of any kind, "Say what you mean." In some cases, I'm concerned that Congress has instead opted for, "say what can pass," punting a huge mess down the road.