To: Members of the House Committee on Energy and Commerce
From: Will Yepez, Policy and Government Affairs Manager, National Taxpayers Union
Date: July 19, 2022
Subject: NTU Views on the Markup of H.R. 8152, the American Data Privacy and Protection Act

---

I. Introduction and Key Taxpayer Considerations

On behalf of National Taxpayers Union (NTU), the nation's oldest taxpayer advocacy organization, we wish to share some of NTU's views and considerations on the American Data Privacy and Protection Act (ADPPA/H.R. 8152). As California, Virginia, Colorado, and other states have passed their own data privacy legislation, it is encouraging to see lawmakers in Congress act to address the emerging patchwork of state laws that imposes hefty compliance costs on American companies. The Information Technology & Innovation Foundation estimates out-of-state costs from 50 state laws would exceed $1 trillion over 10 years. This emerging patchwork threatens to create an unworkable system for small businesses and create confusion for consumers.

While this is an important topic, Congress should not rush the process. Roughly 24 hours before the markup of this bill, an amendment in the nature of a substitute (AINS) was released, giving little time for outside feedback on key changes to the bill. It is more important to get his legislation right than it is to get it done right away. Especially as more companies small and large expand their online presence and technology becomes more omnipresent, data privacy legislation can have far reaching consequences. Lawmakers should move forward deliberately with an open process that allows adequate time to discuss, change, improve, and debate a federal framework.

In considering a federal data privacy framework, NTU believes lawmakers should:

- Avoid following the heavy-handed European approach to data privacy legislation and ensure any federal framework protects consumers without unduly burdening businesses with excessive regulations or restricting economic growth;
- Avoid granting overly broad rulemaking and discretionary powers to the Federal Trade Commission (FTC) or other unelected bureaucrats, especially in areas outside of data privacy;
- Include a strong preemption of state laws; and
- Avoid a private right of action.

The European Union (EU) passage of the General Data Protection Regulation (GDPR) should provide lawmakers with a roadmap of what *not* to do. GDPR's regulations have several unfortunate unintended consequences. While large incumbent companies are more aptly able to navigate burdensome regulations, small- and mid-size companies are being harmed, leading companies to close their doors in

Europe. Meanwhile, the substantial compliance costs associated with GDPR divert resources away from pro-growth investments and can limit the availability of startup capital. At a time when the American economy is already fragile, any framework that follows the EU's GDPR would be a mistake.

II. Changes and Amendments That Could Improve the Legislation

NTU offers the following suggestions and recommendations that we believe would improve this legislation. They are:

- **Guardrails on FTC authority:** While NTU agrees with the bill authors that the FTC should play the primary role as the federal enforcement agency for a federal data privacy framework, adequate guardrails should be included in the legislation. NTU has been alarmed at the direction the FTC has taken under its current Chair, and we believe that any latitude given to the agency will be pushed to the absolute limit. As the Committee considers this legislation, it should evaluate how a potentially partisan enforcement agency could overreach and ensure proper guardrails are put into place.

- **Remove Sec. 207:** NTU believes Sec. 207, which covers algorithms, should be removed from ADPPA. This section would require large data holders that use algorithms that pose "a consequential risk of harm" to an individual or a group of individuals to submit an impact assessment to the FTC, as well as requiring covered entities and service providers to reduce the risk of potential harms in designing future algorithms. It's not clear how covered businesses should determine if algorithms may cause potential harms or what predictive powers the FTC has in determining these guidelines for entities covered by this legislation. Algorithms, which are fairly ubiquitous in technology, have been a point of contention with lawmakers. If policymakers want to address this complex topic, it would be better to do it on a standalone basis rather than including it in this federal data privacy legislation.

- **Stronger preemption of state laws:** Sec. 404 includes a preemption of state laws, but it exempts nineteen categories of state laws, rules, regulations, and requirements, including Illinois' Biometric Information Privacy Act and Genetic Information Privacy Act, as well as Section 1798.150 of the California Civil Code. It is encouraging to see a preemption of state laws in ADPPA, but this provision should be improved and strengthened.

  NTU has argued a light-touch federal standard would help businesses avoid burdensome compliance costs and create more clarity for consumers who shouldn't have different data protections based on their zip code. A lengthy list of exemptions to a federal preemption undermines that goal. Additionally, it is unclear why there are carve outs for the data privacy laws of Illinois and California, and these are by no means insignificant exemptions.

  California unfortunately has followed a similar approach to the EU with the California Consumer Privacy Act (CCPA) which went into effect in 2020. NTU Foundation has warned California's

data privacy legislation imposes onerous burdens as well as substantial fines on online businesses, even if they are not based in California. As some California Democrats call on Congress to avoid weakening CCPA with a federal preemption in ADPPA, lawmakers would be wise to reject this notion. If Congress fails to include a strong federal preemption of state laws in a federal framework it will fail to address the key issue with the status quo — a patchwork of state laws that make compliance extremely difficult and costly for small businesses.

- **Eliminate the private right of action:** Another sticking point with past negotiations on a federal data privacy framework has been a private right of action. Sec. 403 of the AINS provides for a private right of action after two years of enactment, shortened from four years in the previous version. This section would allow individuals to seek compensatory damages, injunctive relief, declaratory relief, and attorney fees. Lawmakers attempted to limit the scope of the private right of action, but it should be eliminated.

  While proponents state a private right of action would empower consumers, trial lawyers would be the ultimate beneficiaries. Even a limited private right of action leaves the door open for costly and frivolous lawsuits. A private right of action also would create market inefficiencies, as companies are forced to divert revenue towards litigation rather than other pro-growth investments in their business and employment.

III. Conclusion and Contact Information

NTU applauds the Committee for taking up this important topic and will continue to engage in the process. While much of recent technology policy has been consumed with proposals to radically overhaul antitrust laws and disadvantage American technology companies, it is encouraging to see lawmakers focus on the critical issue of data privacy. While these recommendations are not an exhaustive list of all of NTU's thoughts or reservations with the legislation, we believe these changes would meaningfully improve the legislation. Should you have any questions about the recommendations in this memo, please do not hesitate to reach out to Will Yepez at wyepez@ntu.org.