



June 22, 2022

The Honorable Frank Pallone
Chair
House Committee on Energy and Commerce
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rogers
Ranking Member
House Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Subcommittee Chair
Subcommittee, Consumer Protection and
Commerce
House Committee on Energy and Commerce
2107 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Gus M. Bilirakis
Subcommittee Ranking Member
Subcommittee, Consumer Protection and
Commerce
House Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone,
Ranking Member McMorris Rogers,
Chair Schakowsky and
Ranking Member Bilirakis:

AAJ strongly supports the Committee's focus on enacting privacy and data security legislation and is encouraged by the significant progress achieved thus far with the introduction of H.R. 8152 the "American Data Privacy and Protection Act". However, continued work on this legislation is critical to ensuring that any new privacy law fulfills the promise of achieving data privacy for the protection and empowerment of the American public. We look forward to working with the committee to achieve this goal.

Currently, Americans' private and most personal information is ubiquitously being used and sold by the world's largest tech corporations. It takes seconds for an individual's HIV status to be revealed, personal health information to be shared with companies for profit, or someone's financial information to be compromised and stolen, and Americans are repeatedly and unnecessarily suffering the consequences of such actions without having the right to seek accountability from the tech companies that are responsible. The tech industry has been wildly successful in profiting off the private financial, healthcare, and personal data gained from tracking Americans online leading to some of the most powerful and profitable companies in all of human history. Americans and leaders in Congress have agreed that the American public has a right to privacy, security, and autonomy regarding how their personal information is used and shared.

AAJ has reviewed H.R. 8152 introduced and amended by Chairman Pallone, and Ranking Members McMorris Rodgers and Wicker. Based on this review, the following issues must be addressed:

1. Section 403(b)(2): Joint Action Waivers & Forced Arbitration: Section 403(b)(2) seeks to ban the use of joint action waivers, which is a mechanism used by corporations to stop Americans from joining together with other Americans to seek accountability as a class. Addressing this issue is critical to ensuring that the protections in the bill have any meaningful impact on most of the American public. This is because for many Americans it is not feasible to take on big tech alone – individuals must be able to join together to have any chance at seeking justice and enforcement of the new law from some of the largest corporations in the world.

- This language needs to be clarified so that individuals have the continued right under current rules to bring or join a collective action to enforce the provisions of the law, regardless of whether individuals are subject to forced arbitration or have full rights to file a case in court. Any efforts to erode the ability of victims to seek justice together would be of the utmost concern.
- The bill also does not address forced arbitration in any respect for Americans over the age of 18, while being debated in a world in which forced arbitration is the default mechanism with which corporations strip Americans of their rights to seek accountability for everything from discrimination and death to massive data breaches and privacy violations. The bill can and should at a minimum ban forced arbitration for claims created by the Act related to civil rights, disability rights, gender-based violence and health information. Forced arbitration guts public accountability, deprives Americans of their rights, and hides evidence of systemic abuses. Continuing to allow businesses to use forced arbitration knowing that this will be the default significantly undercuts the bill's protections.

2. Section 403(a)(3): Private Right of Action: The Federal Trade Commission (FTC) and state attorneys general (AG) enforcement provisions are also in need of critical clarifications. FTC and state AG enforcement are necessary tools to ensure the right to privacy is maintained; however, because the bill is unclear on whether an individual pursuing her case under the private right of action can continue to do so if the FTC or any AG is also taking action, the bill's text should be clarified to protect private citizens seeking to enforce their rights for harm caused.

- In addition, the language as drafted implies that the FTC and state AGs could appeal a decision in a private enforcement action even if the privacy victim disagrees with such decision. We believe additional clarity is critical to delineate who retains the right to be heard and whether existing rules on claim consolidation will apply. Whether a government action is taken should have no implications on whether private citizens retain rights under the bill's enforcement provisions.
- In addition, section 403(a)(3) specifies that the FTC and state AG right to appeal a decision in a private enforcement action, yet the legislation is silent about the appeal rights of an individual. This also needs to be clarified and should remain consistent with existing law.
- Lastly, the AG notice provisions must also be clarified. The bill provides that any person or class of persons must give the FTC and their state AG 60-days-notice before filing a claim under the private right of action. However, at the outset of the case, it's impossible to determine whether class certification is appropriate and to what extent – such determinations occur much later in the process. The language should be clarified to require the known persons intending to file the claim should notify their state AG and the

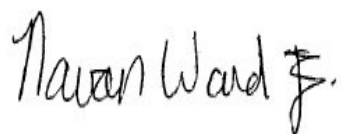
FTC. This should happen again or repeatedly when additional class members become known or are certified as a class.

3. **Section 404(b): Preemption:** The preemption of state and local law provisions uses unique terminology that could be interpreted exceptionally broadly. Section 404(b) would preempt any state or local law “covered by the provisions of the Act.” Without a definition of “covered by,” this provision could potentially preempt any state or local law that touches in some way on the same subjects as the Act. It has the potential to be the broadest preemption provision in law and could have massive unintended consequences.
4. **Section 404(c): Savings:** The preemption carve out for civil rights laws and consumer protection laws are not specific or well defined. We are concerned that using broad catchall terminology may inadvertently narrow the scope of what is intended to be saved. In short, we believe that there are numerous statutes related to employment, housing, public accommodations, contracting, etc. that are intended to be saved but without giving a court more instruction they may fall by way of the preemption language.
5. **Section 403(a)(1): Delay in Enforcement/Statute of Limitations:** This section delays enforcement for four years after the Act takes effect, which is a very long period for Americans to wait to enforce privacy harms. In addition to this long delay, it is critical that the bill delineates how claims accrue and how long an individual has to file a claim. Without this critical information, it is highly unclear how or when, if at all, any claims will ever accrue.
6. **Section 403(d): Demand Letters:** The provision mandating inclusion of specific language in demand letters regarding the FTC website should only apply to represented parties and should not impact absent class members; this needs to be clarified in the text. Consumers often write letters or reach out to businesses when they’ve suffered a privacy violation. They will have no knowledge of this provision and it should not determine whether they have any rights under the Act. Similarly, classes are not determined prior to filing a claim and thus would not be certified until well after this provision would have expired. As a result, any violation of this provision should be treated individually and not impact the larger class of claims. This must be clarified to ensure any meaningful enforcement of the new law.
7. **Section 403(c): Right to Cure:** The “Right to Cure” provision allows a “covered entity” to fix a privacy violation, no matter how serious or substantial and regardless of harm caused.
 - Under the provision, it is unclear whether an entire action would be dismissed if the covered entity demonstrates that it has “cured” the violation within 45 days, or just the claim for injunctive relief. Only a claim for injunctive relief should be dismissed - not the whole action or the claim for monetary relief because such relief is meant to compensate Americans for what has already been lost or harm that has already been suffered.
 - Second, it’s entirely unclear who would decide whether the defendant has “cured” a violation. That must be clarified.
 - Finally, clarification is needed on how the cure provision works with a potential class of persons. There could repeated requests for “cure” from similarly situated individuals that all end in dismissal rather than injunctive relief as one potential class member after another waits for a “cure” and instead ends up with a dismissal. That would just result in massive delay and wholly illusory accountability.

8. Section 404(a)(2): Carve Outs: This section exempts covered entities from the Act's data privacy requirements if the covered entities are required to comply with other federal laws. That would mean that credit reporting agencies, banks, and health care providers would not face any stiffer privacy requirements than under current federal law. More granularly, it is unclear whether or how this would impact covered entity's subsidiaries and other related businesses. The definition of covered entity seems to link together for these purposes any businesses with joint control.

AAJ deeply appreciates the committee's consideration of its views, and we look forward to working with the committee to enact comprehensive data security and privacy legislation.

Sincerely,

A handwritten signature in black ink that reads "Navan Ward Jr." with a stylized flourish at the end.

Navan Ward Jr.
President
American Association for Justice