December 17, 2022
The Honorable Nancy Pelosi
Speaker of the House
U.S. House of Representatives
H-232, the Capitol
Washington, DC 20515

RE: Request to block H.R. 8152, the American Data Privacy and Protection Act, from a floor vote unless it is first strengthened in the specific ways enclosed.

Dear Speaker Pelosi,

Firstly, thank you for your work in your many years in the U.S. Congress as a lawmaker, and as Speaker of the House. Your calm, your unshakeable and powerful leadership, even in the midst of terrible events like the Jan. 6th attacks, are truly remarkable.

We are writing to ask you to block the advancement of the American Data Privacy and Protection Act (ADPPA) until it is strengthened, and we would like to offer a specific blueprint for what we mean by strengthening this bill.

While there are some groups who have asked you to bring this bill to the floor, we are clear that this bill will not meaningfully and sufficiently protect people in its current form. We are writing with strong experience in reviewing Data Privacy laws in a manner that is deeply intersectional, and investigates how each aspect of the bill will affect various individuals and communities most at risk of data privacy harms.

For instance, when we look at the specific data privacy harms to abortion and gender-affirming care seekers via data flows and commercial surveillance *post-Dobbs*, as well as the particular ways in which Immigrants, Black and Indigenous, poor and LGBTQ2SIA+ members of this group of healthcare-seekers – who are *already* disproportionately at risk of both state and social violence and injustice – are affected; we can clearly see that the American Data Privacy and Protection Act, in its current form;

- will not protect people with uteruses who are at risk of being targeted, surveilled, tracked, and harmed and/or arrested for exercising their right to bodily autonomy.
- will not explicitly protect LGBTQ2SIA+ people.
- will not halt unwarranted access to people's data via data brokers, private entities, and third parties.

- will not require companies to use encryption, which is one of the most important ways that everyone's data can be immediately secured.

- does not allow states and local municipalities to pass stronger consumer privacy laws, right as we are on the cusp of a huge array of new and developing threats to privacy and security via the unchecked collection and use of biometric data, AI and virtual reality applications, as well as the use of algorithms, machine learning, and automated decisions systems in literally every area of our lives.

- does not have strong enforcement mechanisms, and (sadly) more.

The risk that a bill this impactful, which is already flawed in critical ways, and is preemptive, could very likely be weakened rather than strengthened if brought to the floor now, in a rush to pass it before Congress-members leave for the holidays, *is simply too great*. There is much to be done to make this a strong enough bill to warrant preemption at such a critical time for our democracy.

As we've seen with the federal removal of the right to our bodily autonomy, securing the right to privacy and bodily autonomy in the United States is neither an issue we can isolate to reproductive healthcare, nor is it a right to take lightly in terms of its deep effect on the workings of our democracy, and its impact on due process for every person and community, regardless of gender, race, sexuality, language, national origin, ethnicity, religion, ability, immigrant status, wealth (or lack thereof), age or occupation.

Madame Speaker, we respectfully request that you, and/or our incoming Speaker in 2023, do not advance the ADPPA to the floor unless the following key flaws in the bill are addressed:

1. Fix the definition of precise geolocation information (§2(24)), and include all types of location data as "covered."

   - Limiting the exemption to a particular range of feet, as ADPPA's current version does, will not protect pregnant people who visit clinics or pharmacies in rural or suburban areas at all. Consumers, and now, particularly abortion seekers, MUST be able to secure our persons and identities via disallowing companies' access to our locations.

   - Location information derived from images taken by surveillance cameras or automated license plate readers (ALPRs) is not treated as sensitive. ADPPA allows it to be bought and sold without consent. This data needs to be covered.

2. Do not exempt important categories of data, such as

   EMPLOYMENT DATA:
   - ADPPA does not cover employee data, including benefits, so if companies provide benefits for employees or contractors seeking reproductive or other health care – or if

employees exchange email with their manager arranging time off to get reproductive or other health care – their data is vulnerable (§2(8)(B)&(C)). California's CCPA, by contrast, protects employee data.

"DE-IDENTIFIED" DATA:

- The current version of ADPPA has several loopholes allowing data brokers to buy and sell location (and possibly other types of) data – including selling it to government(s) or vigilantes doing "civil enforcement" of laws criminalizing abortion.

- Because all data can be personal and highly sensitive in the right combination, de-identification is a tricky practice. Data that has been "de-identified" [exempted from the definition of covered data in (§2(8)(B))] often still contains markers that can be used fairly easily to re-identify, or re-aggregate, the data with other saved, shared or purchased data. One method that's been highlighted post-Roe is the tracking of location data alongside other data. ADPPA does not require companies to delete existing data. This means that re-aggregating (re-identifying) data under the guise of internal research or analytics purposes, or to make inferences, is still available to companies (and their affiliates) under ADPPA. We consider exempting "de-identified" data to be a major loophole.

3. Close the "internal research or analytics" loophole (§101(b)(2)(C), which allows companies to use any personal data for a company's research purposes, including "to improve a service," which is entirely too broad.

   - Companies can, and will, abuse the lack of express consent required by this exemption to perform all kinds of research that consumers have not expressly consented to, including building AI tools and algorithms related to their businesses that consumers may be vehemently opposed to, but would not even know about, because there are no open disclosure and consent requirements for this kind of activity.

   - In the current version of ADPPA, companies may also share consumer data across affiliates, and use that data for research purposes.

4. Close the loophole that gives broad leeway to companies to refuse to delete data if it would interfere with "reasonable efforts to guard against, detect, prevent, or investigate ... unlawful activity." (§203(e)(3)(A)(vii)) This opens people to threat of harms in many different ways, and in states that have criminalized abortion, this gives "crisis pregnancy centers" license to keep any personal data people have provided to them.

5. Provide protection for LGBTQ2SIA+ people by restoring "sexual orientation" to the list of sensitive covered data (§2(28)(A)(ix)), and *add* "gender expression and identity", to provide comprehensive protection for all genders.

6. Make ADPPA's civil rights protections substantive and meaningful by

- restoring the requirement for independent algorithmic impact assessments;
- removing the exemption for government contractors and other service providers;
- adding whistleblower protections; and
- adding a right to opt-out of automated decision making systems (similar to California's CPRA).

7. Remove preemption of state and local laws.

    - ADPPA preempts all current and future state and local privacy laws on biometric information (apart from face recognition), genetic data, broadband privacy, and data brokers.
    - ADPPA would eliminate existing legislation like Maine's ISP law, the Seattle Broadband Ordinance, and Washington's biometric privacy law.
    - ADPPA would prohibit pro-immigrant states like Washington, and cities like Seattle from passing stronger legislation to protect our residents. This is vitally important from an immigrant rights perspective, "sanctuary city" protections are virtually moot if immigrants' data is not protected.

8. Remove barriers to state Attorneys General's ability to investigate and enforce the law.

    - Remove §404(b)(2)(A) ("a violation of this Act shall not be pleaded as an element of any such cause of action") to allow AGs to investigate and enforce the law. Ten Attorneys General sent a strong letter in July asking the Congress not to preempt states' abilities to protect their residents.

We understand that legislation is not always perfect. We understand that there is great pressure on lawmakers to "just pass ADPPA!" However, Madame Speaker, advancing (and possibly passing) the ADPPA with not just imperfections, but the gaping holes and critical flaws we've detailed here; this would set a precedent that privacy laws don't actually need to protect the people who are the most at risk of the greatest harm. For many years, that has been poor, Immigrant and BIPOC people. Right now, that includes anyone who can become pregnant. Tomorrow, that may include LGBTQ2SIA+ people, disabled or unwell people, or people who simply stand up for their right to cast a ballot.

The claim that there is a narrow window in which Congress may act is untrue. The world will not end if ADPPA doesn't move to the floor this session. Bringing a strengthened bill forward in the next session is politically viable. CA's law (and the GDPR) will still be the standard most U.S. companies adhere to; and organizations like ours, and so many others, will still be out here pushing and advocating for strong laws, and for companies to do better. Just this past week we've seen advocacy yield two significant victories for people's privacy. A key social media platform has expressed they are committed to working toward encrypting direct messages as the default setting for all users, and Apple has announced it will not pursue the scanning of people's personal photographs without their consent, and will also move toward encrypting people's iCloud backups.

As you are well aware from your own great state of California, states and municipalities are often laboratories for model laws and protections for people. Not only that, the FTC has initiated a rulemaking process on commercial surveillance and data security, and the Biden administration has released A Blueprint for An AI Bill of Rights. There is a lot of ongoing work to protect people, and that work will continue.

The ADPPA doesn't get it all wrong: there are some really good things in the bill! But, for now? We know we need to speak up: the American Data Privacy and Protection Act gets far too little right to risk preempting our ability to protect people from those who wish ill to our democracy, and seek to roll back the critical human and civil rights that our democracy must afford all of its residents in order to maintain its integrity.

Thank you for your time, and for your work, Speaker Pelosi.

Signed,

WA People's Privacy
Indivisible Washington's 8th District
Japanese American Citizens League, Seattle Chapter
Whatcom Human Rights Task Force
Seattle Indivisible
PDX Privacy
Washington State Poor People's Campaign
Indivisible Vashon Immigrants/Refugee Rights Group
Wallingford Indivisible
Snohomish County Indivisible
Indivisible Plus Washington
Indivisible Eastside (WA)
Washington Indivisible Podcast & Town Hall Series
Indivisible Whidbey