A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA

ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

1. Create a single set of data privacy rules for the United States.

- ✓ Create a comprehensive federal data privacy law and preempt state and local governments from passing legislation that would add to or diminish from these rules.
- ✓ Create a single data breach notification standard for all users while simplifying compliance by preempting any conflicting laws from states.

2. Create a common set of federal protections for all types of data.

- ✓ Rescind existing federal data privacy laws and create a common set of federal protections. Ensure sector-specific regulators stay in place to oversee these changes and continue future enforcement.
- ✓ Scope rules to apply to all types of data.
- ✓ Exempt publicly available information.
- ✓ Exempt de-identified data.

3. Create data protection rules based on both the type of data and the type of entity collecting the data.

- ✓ Distinguish between nonsensitive and sensitive personal data.
- ✓ Designate a subset of services provided by covered entities as "critical services," which are subject to higher standards and requirements. Do not exempt organizations based on size.
- ✓ Require notice for nonsensitive personal data used in noncritical services. Allow opt-out of data collection when organizations provide critical services collecting nonsensitive personal data, or noncritical services collecting sensitive personal data. Require an opt-in standard when organizations provide critical services collecting sensitive personal data.
- ✓ Create specific, non-consent-based exceptions to the collection and use of both sensitive and nonsensitive personal information.

4. Enable consumers to make more informed decisions.

- ✓ Include transparency requirements and provide consumers with information on what types of organizations can access personal data and how it is being used.

5. Establish clear consumer rights.

- ✓ Include a limited right of access that accounts for costs.
- ✓ Include a limited right to data portability that accounts for costs.
- ✓ Include a limited right to rectification for sensitive data collected by critical services.

6. Address concrete consumer harms, rather than hypothetical ones.

- ✓ Give FTC jurisdiction over privacy enforcement. Oversight requirements should weigh costs of compliance with benefits.
- ✓ Focus enforcement on substantial consumer harms, not hypothetical ones.
- ✓ Expand the FTC's authority to fine companies that violate the law, taking a deliberative harms-based approach.

7. Protect innovation.

- ✗ Do not restrict covered entities from having incentive programs or penalizing users who do not consent to data sharing.
- ✗ Do not include data-minimization provisions.
- ✗ Do not include purpose-specification provisions.
- ✗ Do not include limitations on data retention.
- ✗ Do not include a right to deletion or a right to be forgotten.

8. Minimize compliance costs for U.S. organizations.

- ✗ Do not include a private right of action.
- ✗ Do not specify how covered entities protect information, but instead require them to disclose certain details about their security practices.
- ✗ Do not include privacy-by-design provisions.
- ✗ Do not include personnel requirements.

9. Improve enforcement.

- ✓ Provide the FTC with limited rulemaking authority for data privacy.
- ✓ Establish the FTC as the federal agency in charge of receiving and processing privacy complaints, and provide it with the resources necessary to process these complaints.

10. Promote international interoperability.

- ✓ Extend protections extraterritorially.
- ✗ Do not place limits on cross-border data flows.

Read the full report at itif.org/data-privacy