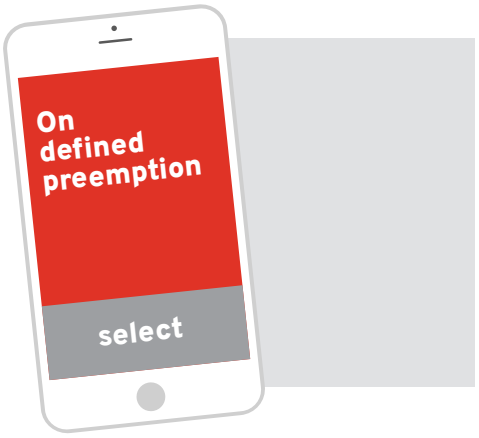
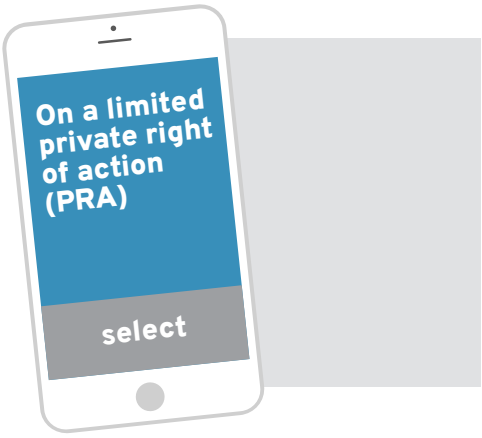
Federal Data Security and Privacy Law: Finding Compromise On Federal Legislation

This explainer is part of a series considering roadblocks to a federal data security and privacy law, drawing upon research and engagement with stakeholders to identify and recommend appropriate courses of action to find compromise on federal legislation. Ongoing research also includes topics like civil rights in privacy, arbitration and covered entities and data. We offer the following initial recommendations:



1. **Strong preemption language with carve-outs.**
   This prevents a patchwork of frameworks across the country; provides consistent rights for consumers; and recognizes the role of states. Recommended carve-outs include:
   - **Traditional areas of state concern** like civil rights, specific relationships and gaps in federal law.
   - **Emerging areas and gap fillers** such as cybersecurity laws and areas not addressed by federal law.
   - **Existing federal laws** such as student, health (HIPAA), financial (GLBA) and children's privacy.
2. **Balancing state and federal provisions.**
   States are less likely to oppose strong preemption if a federal law is as robust as existing legislation. A federal law should be conscious of this dynamic.
3. **Include state Attorneys General or other agencies.**
   States should be a part of enforcement, whether through their attorney general or another agency. State data protection entities could, among other roles, handle carve-outs, serve as an ombudsman for state perspectives and provide subject matter expertise.

1. **Administrative Procedure Act (APA) Rulemaking.**
   A federal privacy bill should grant the FTC targeted rulemaking authority (notice and comment) under Section 5 with ample time for covered entities to comment.
2. **Defined Areas for Rulemaking.**
   A federal privacy bill should define the areas for FTC rulemaking, including sensitive covered data; opt-out of transfers of covered data; explicit consent for processing; requests for verification; dark patterns and choice; data security; civil rights and privacy; and data collection.
3. **Enforcement.**
   The FTC should be the primary enforcer, and allow state Attorneys General to bring suit on behalf of that state's constituents. First-time fining authority should be used as a tool to halt the most egregious or urgent practices. The FTC should use warning and remediation letters, safe harbor frameworks, and best practice guidance to achieve broad compliance.
4. **Victim's Relief Fund.**
   Collected funds from fines spent to help small- to medium-sized business compliance and victim relief.
5. **Increase Capacity.**
   $500 million for a new FTC Bureau of Privacy with 500 personnel over five years.



1. **Create a PRA.**
   A federal data security and privacy bill should empower everyday Americans to assist in the enforcement of the new law in a clear, confined and meaningful way. This new statutory right should cover data breaches, and extend beyond that by explicitly articulating privacy harms Congress intends to prevent or reduce with a PRA. The greater the harm priority for Congress, the greater the relief made available to the individual.
2. **Limit the PRA.**
   To strike the right balance between the American consumer and business, Congress should place clear limits on the created PRA. Congress should creatively and narrowly tailor remedies made available to the individual by (1) leveraging a **tiered damage system**; (2) **permitting injunctive relief** in certain circumstances; and (3) allowing for **safe harbors** where appropriate. Furthermore, Congress should create pathways for consumers and businesses to come together outside of the courtroom to resolve their differences by (4) establishing a **right to cure**.

Presented by:

R Street
Free markets. Real solutions.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs