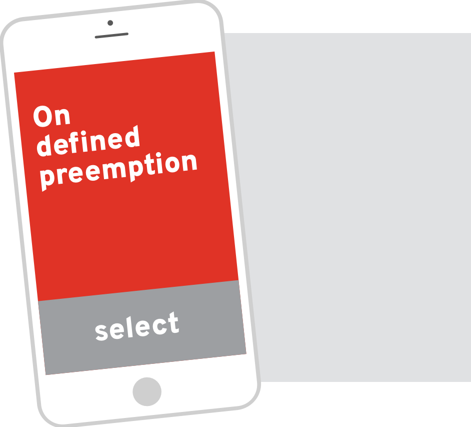
Federal Data Security and Privacy Law:

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:

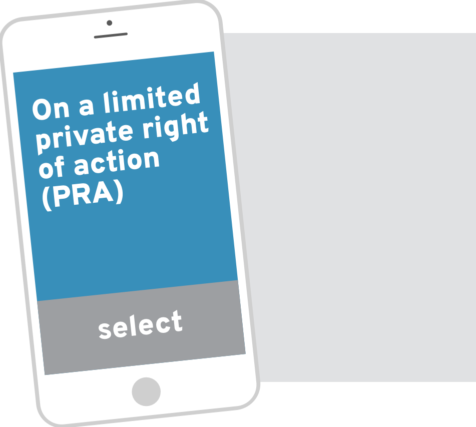


On defined preemption

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.

On the role of the Federal Trade Commission (FTC)

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.



On a limited private right of action (PRA)

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

Federal Data Security and Privacy Law:

Finding Compromise On Federal Legislation

Project Leadership Team

Tatyana Bolton
tbolton@rstreet.org
@TechnoTats

Tatyana Bolton is the policy director for **R Street**'s Cybersecurity and Emerging Threats team. She crafts and oversees the public policy strategy for the department with a focus on secure and competitive markets, data security and data privacy, and diversity in cybersecurity. Previously, Tatyana worked as the senior policy director for the U.S. Cyberspace Solarium Commission focusing on U.S. government reorganization and resilience portfolios, and the Cybersecurity and Infrastructure Security Agency.

Lauren Zabierek
lauren_zabierek@hks.harvard.edu
@lzxdc

Lauren Zabierek is the executive director of the Cyber Project at **Harvard Kennedy School's Belfer Center**. Here, she runs a cybersecurity and technology policy research program. Her work focuses on strategic, national security issues ranging from international conflict, cooperation and norms to domestic collaboration, diversity, privacy and supply chain issues. Lauren is also the co-founder of the online social media movement called #ShareTheMicInCyber, which aims to dismantle racism in cybersecurity and privacy.

Cory Simpson
cory.simpson@resolutestrategicservices.com
@corysimpsonwv

Cory Simpson is an executive vice president at **Resolute Strategic Services**, where he partners with business leaders in navigating the most complex and significant challenges they and their organizations face in the area where security, technology, government and business interests converge. Cory is also an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security.

Brandon Pugh
bpugh@rstreet.org
@Brandon_J_Pugh

Brandon Pugh is a senior fellow and policy counsel for the Cybersecurity and Emerging Threats team. He also serves as an international law officer in the U.S. Army Reserve. Prior to **R Street**, Brandon was legislative counsel for the New Jersey General Assembly Minority Office, where he handled nearly all policy and legislation on cybersecurity, emerging technology and privacy for the office. He also served as an elected and appointed official at the local, county and state level.

Sofia Lesmes
slesmes@rstreet.org
@soflescas

Sofia Lesmes is a senior research associate for **R Street**'s Cybersecurity and Emerging Threats team. Her work focuses on data security, data privacy, encryption policy and international cybersecurity norms. She is also an advisory expert on cybercrime to the Permanent Observer Mission of the Holy See to the United Nations, where she previously covered the Peace and Security portfolio as an intern.

Presented by:

R Street
Free markets. Real solutions.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs