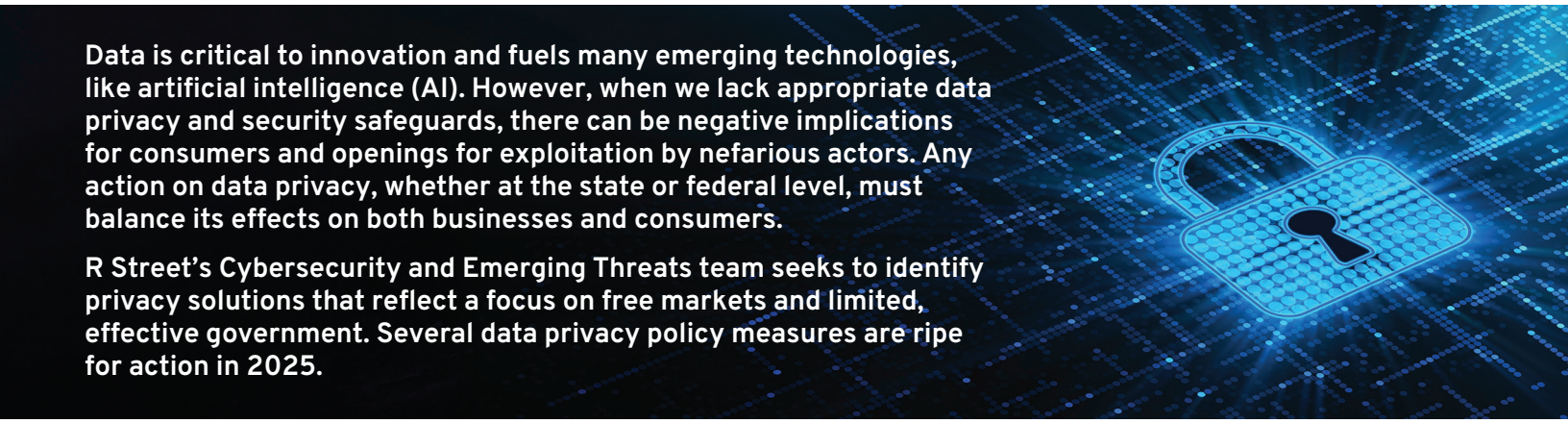
R Street

Free markets. Real solutions.

EXPLAINER

Key Data Privacy and Security Priorities for 2025

January 2025



Data is critical to innovation and fuels many emerging technologies, like artificial intelligence (AI). However, when we lack appropriate data privacy and security safeguards, there can be negative implications for consumers and openings for exploitation by nefarious actors. Any action on data privacy, whether at the state or federal level, must balance its effects on both businesses and consumers.

R Street's Cybersecurity and Emerging Threats team seeks to identify privacy solutions that reflect a focus on free markets and limited, effective government. Several data privacy policy measures are ripe for action in 2025.

Advancing a Federal Comprehensive Data Privacy and Security Law

Without a federal law governing consumer privacy, the United States has become an outlier. States have acted to fill this void with a patchwork of requirements, but most Americans remain unprotected. We strongly support a federal data privacy and security law, understanding that compromise is necessary and that details matter.

SEVERAL THEMES AND PRINCIPLES SHOULD BE CONSIDERED

I Consumer Rights, Transparency, and Applicability to Children

Individuals should be able to control their data, and entities should be transparent about the data they collect; how they intend to use the data; whether they will sell, share, or transfer it to a third party; and how long they will retain it. This includes rights to delete, access, and port data. These are common themes in most of the state-level privacy laws enacted to date, all of which aim to give the consumer control over their data. However, there should be exceptions to these rights for legitimate business and law enforcement needs like fraud prevention, law enforcement investigations, and other legal processes. Some laws provide different rights and protections based on the type or sensitivity of data, but defining "sensitive" is not always straightforward. Policymakers must carefully differentiate between sensitive and non-sensitive data to avoid accidentally restricting useful data. Likewise, specific categories of sensitive data should be exempt when used for specific purposes, like ad measurements.

A federal privacy law should also protect the rights of all Americans, regardless of age or position. While child-specific provisions may be appropriate in specific circumstances, they should only be passed as part of comprehensive legislation. Doing so helps avoid the free speech and identity verification issues some child-specific proposals face.

II Preemption

Preemption remains one of the most important features of a federal privacy proposal. The increasing patchwork of state privacy laws creates many challenges for industry, including costly compliance with inconsistent state-by-state laws, especially for small and medium-sized businesses.

Preemption language must be crafted carefully to ensure the proliferation of state-level privacy laws ends. It is also imperative that a federal law not be a "floor" that allows states to go further, continuing the burdensome privacy patchwork. Federal legislation must be strong enough to provide adequate privacy and security protections to consumers while considering the needs of businesses and groups tasked with complying.

While preempting state privacy laws is vital, there are specific instances in which state and federal laws can work together. This includes areas where states have traditionally acted on privacy and/or areas not covered by federal law, including criminal law, civil law, and public records law. Existing federal privacy laws should also be streamlined to eliminate duplicative regulators, requirements, and reporting.

III Data Security

Currently, even sensitive data lacks adequate safeguards once collected. This can result in bad actors, such as nation states, easily acquiring data from data breaches. A federal privacy law should have provisions for securing data collected through a flexible, non-prescriptive approach. This is important because the security needs of all organizations must be tailored to their specific risk profile, industry requirements, and data types. However, clearer guidance from Congress and policymakers on what constitutes "reasonable security" is necessary because that goal can be a moving target, and regulators have taken different views over time.

IV Data Minimization

Notice and choice have been popular ways to collect and use covered data because that data can be processed if a consumer is notified and does not opt-out (or, for sensitive data, consents to it). However, very few consumers read or understand privacy policies. Data minimization is a privacy principle that limits the amount of data collected in the first place. Data minimization also offers security benefits—if a covered entity never collects the data, then the data is not at risk. This often forces entities to fully understand why they need the data and how it can be used. However, structuring data minimization in statute must be done carefully to ensure it is not too restrictive in legitimate uses or too inflexible to account for future needs we might not be aware of now.

Lawmakers should also focus on outcomes—like data efficiency, business benefits, and increased data security—rather than prescriptive requirements. A risk-based concept that requires increased requirements for sensitive data collection (such as children's data and biometric data) but a lighter touch on standard business data is helpful.

V Enforcement and the Role of the Federal Trade Commission

Many companies embrace privacy, but enforcement can be necessary for organizations with bad data privacy and security practices. To increase privacy in a non-burdensome manner that all companies can comply with, any well-constructed privacy law should include compliance incentives like a safe harbor provision, a right-to-cure provision that allows organizations to avoid penalties if they fix the issue and do not reoffend, and special considerations for small and medium-sized businesses without large amounts of data.

Enforcement can take several forms. For example, state attorneys general and/or the Federal Trade Commission (FTC) should be allowed to enforce the law. A private right of action (PRA) has emerged in recent proposals as a way for individuals to enforce their rights. Given the potential for abuse, we recommend avoiding a PRA. The FTC plays a role in enforcing and investigating violations; however, Congress must set policy and direct the FTC rather than cede the policymaking role.

PRIVACY IN OTHER CONTEXTS

I Addressing National Security Concerns

Adversaries will continue to exploit and collect sensitive information on Americans for many purposes, from potential espionage to more effective cyber incidents. A federal privacy law would help mitigate these risks through data security and notice provisions when data goes to select countries. With this in mind, Congress should consider additional action, and the White House should address other ways data can be accessed, including through data brokers and sales, select mobile applications, and technology products from connected vehicles to Internet of Things devices.

II State Privacy Laws

Especially in the absence of a federal privacy law, states will continue to act on comprehensive data privacy measures and more narrow measures from biometrics to health data. While we prefer a federal approach, states can look to existing frameworks like the Virginia Consumer Data Protection Act to help minimize the impact of variation across state lines. This will benefit industry and consumers, whereas some 2024 state privacy proposals (i.e., Vermont and Maine) would have suppressed innovation.

III Privacy in the context of other technology like AI

Privacy risks and opportunities apply across various forms of technology. We believe that holistic action on privacy is better than addressing it only in the context of one form of technology like AI, whether as standalone AI legislation or dedicated AI provisions in a privacy bill. Finally, it is important to maintain a pro-innovation environment that allows us to maximize the development of potentially privacy-enhancing technologies—including AI itself.

For more information, please contact:
Brandon Pugh | Director and Resident Senior Fellow, Cybersecurity and Emerging Threats | bpugh@rstreet.org
Steven Ward | Resident Privacy and Security Fellow, Cybersecurity and Emerging Threats | sward@rstreet.org