CONSUMER DATA PRIVACY

Guiding Principles & Legislative Checklist

The International Center for Law & Economics is a nonprofit, nonpartisan research center that promotes the use of law & economics methodologies to inform public policy debates. We believe that intellectually rigorous, data-driven analysis will lead to efficient policy solutions that improve consumer welfare and global economic growth.

Reason Foundation's mission is to advance a free society by developing, applying, and promoting libertarian principles, including individual liberty, free markets, and the rule of law. We use journalism and public policy research to influence the frameworks and actions of policymakers, journalists, and opinion leaders.

State legislatures are now tackling consumers' digital privacy. Given the internet's inherently international character, a federal bill setting a national standard for digital privacy would be ideal. Yet, in the absence of federal legislation, states are seeking to address consumer privacy.

Unfortunately, overly broad and burdensome regulatory obligations pose a real and immediate risk to digital innovation. Ensuring a globally robust market requires balancing consumer privacy and legitimate information exchange between consumers and digital services companies. The following principles and legislative checks seek to help legislators and stakeholders narrowly tailor state privacy policy to address concrete consumer harms while preventing disproportionately punitive responses that obstruct market performance.

For more information contact:

Ian Adams
Executive Director
International Center for Law & Economics
iadams@laweconcenter.org

Spence Purnell
Director of Technology Policy
Reason Foundation
spence.purnell@reason.org

PRINCIPLE	LEGISLATION CHECK
1 **FOCUS ON ACTUAL CONSUMER HARMS** ➔ Legislation should address concrete and demonstrable consumer harm rather than hypothetical concerns or theoretical injuries. Therefore, laws should focus on data use and not on data collection or retention.	✓ Are violations of the proposed legislation triggered by a consumer harm, or an administrative error? ✓ Does the proposed legislation react to demonstrated and proven consumer harms, or possible ones?
2 **LIMIT THE SCOPE** ➔ Legislation should explicitly articulate which data are implicated, and standards of care related to those data should grow more onerous as the data grow more sensitive. For example, pseudonymized data should face less restriction than personally identifiable or biometric data. Very small entities with fewer than 50,000 data records could be exempted. ➔ Data practices that reflect consumer expectations, seek to benefit consumers, and represent no direct consumer harm should be considered compliant. Data practices that will likely cause vulnerability to financial harm, physical harm, or harassment should not be considered compliant.	✓ Does the proposed legislation differentiate between types of data and/or their intended uses? If so, does it do so in a manner that allows use of data where no consumer harms are identified (a permissive approach)? ✓ Would the legislation cause per se violations for data use that would otherwise be consistent with consumer expectations?
3 **DISTINGUISH BETWEEN PRIVACY & SECURITY** ➔ Major data breaches such as Equifax are problems with data security, not necessarily privacy. States should ensure that privacy legislation doesn't unintentionally cover data security issues. Data security should be pursued or improved in existing data breach notification laws.	✓ Does the legislation add punishment for privacy harms to legal consequences for data breaches?
4 **TARGET OUTCOMES, NOT METHODS** ➔ Legislation should seek to promote compliance while avoiding prescriptive compliance obligations that disproportionately impact small and medium-sized firms. For example, requiring that all companies have a dedicated data privacy officer would prove onerous, without necessarily improving the overall privacy posture of industry.	✓ Does the proposal treat all firms identically, or do obligations grow with firm size and digital sophistication?

PRINCIPLE	LEGISLATION CHECK
5 **ENSURE REGULATORY RESILIENCE** ➔ States can encourage the development of consensus standards, which are more resilient and secure than legislatively codified standards, by creating "safe harbors" from adverse action under the law for companies that comply with such standards. Avoiding prescriptive technical standards further serves that goal.	✓ Does the proposal include a safe harbor? ✓ Does the proposal avoid overly prescriptive policy dictation of privacy notices, such as requiring a long list of things that must be provided to customers rather than setting standards?
6 **KEEP OBLIGATIONS NARROW AND COMPREHENSIBLE** ➔ **Notice and consent:** Once a privacy notice is provided, many sites use a default opt-in technology to smooth the consumer experience. Provided that uses of data are consistent with consumer expectations under the privacy notice, further consent is redundant and unnecessary. ➔ **Access & Correction:** Consumers should be able to request limited access to their data and ask for corrections if necessary. Firms need to be able to ask for personal authentication before access requests can be made. Pseudonymized data should not be covered under these requirements. ➔ **Deletion:** Deletion requests should be limited to sensitive personal information, but should otherwise not be permitted without proof of harm.	✓ Does the proposal allow reasonable use of data that is consistent with consumer expectations? ✓ Does the proposal's data access and correction provision provide reasonable timelines for a firm's response? Does it require long-term data retention? ✓ Does the proposal's right to deletion have limits?
7 **CONSUMER-FOCUSED ENFORCEMENT** ➔ Enforcement should focus on demonstrable consumer harms and seek to ensure proportionality between consequences and the nature and severity of the harm or compliance failure. ➔ There should be no dedicated data regulators. To the extent necessary, rules should be promulgated by attorneys general through voluntary consensus standards, but no state agency should be given broad rulemaking authority to regulate. ➔ No private right(s) of action should be permitted to consumers. If unavoidable, there should be a strong preference for limiting it to non-monetary/injunctive relief to chill the incentive for litigation. ➔ There should be a period for firms to cure violations once identified, verified, and acknowledged. ➔ Safe harbors promote consumer protection and prevent thematically duplicative standards. Such regulatory equivalency, in the form of a presumption of compliance, should be provided when there is compliance with: • AG adopted voluntary consensus standards; • The EU General Data Protection Regulation; or • Any other state digital privacy law.	✓ Do violations of the proposal turn on whether a consumer was actually harmed by a violation of its provisions? Or, are theoretical harms imputed by failure to comply with a technical component of the proposal sufficient to commence an enforcement action? ✓ Does the proposal rely on AGs for enforcement? ✓ Does the proposal avoid private rights of action? ✓ Does the proposal include a sufficient period to cure a violation?