Consumer Privacy Legislation Considerations

The constant bad news about how big tech companies intrude on our privacy illustrates the need for new laws to protect data privacy. A federal law should include:

No Preemption Strong baseline federal privacy legislation would benefit consumers across the country, but any action that supplants stronger state laws would hurt consumers and prevent states from protecting their constituents. California's Consumer Privacy Act, Vermont's Data Broker Act, and Illinois' Biometric Information Privacy Act already protect consumers, and other states are looking at similar proposals. After years of opposing any data protection law, big tech companies now support creating "one federal standard" only because state laws are working.

Enforcement Any strong federal data privacy legislation must contain the most important enforcement tool: the right for consumers to enforce their privacy rights in court. Government agencies often lack the resources to enforce existing laws. Additionally, some industries have "captured" regulatory agencies, resulting in weak or no enforcement. A private right of action would ensure government agencies or consumers themselves can enforce any protections Congress designs. Also, users often effectively lose new rights when they "agree" to terms of service and end user license agreements that they haven't read—and aren't expected to read. Strong data privacy law should also prohibit waivers and mandatory arbitration requirements, which often allow companies to sidestep the users' rights.

Fairness Privacy is a fundamental human right. A federal privacy law must recognize this by including a non-discrimination rule that says companies cannot deny goods, charge different prices, or provide a different level of quality to those who exercise their privacy rights. Without this rule, pay-for-privacy systems will make privacy a luxury and exclude lower-income consumers from any intended protections.

Privacy Safeguards Consumer data privacy legislation should require companies to obtain consumers' opt-in consent before they collect, retain, use, or share consumers' personal information. If a consumer consents to collection of their information (such as location data to map a running route for a fitness tracker) for one purpose, companies must get additional consent before selling or using data for another purpose. Legislation must also require companies to: minimize their processing of consumers' data, i.e., process it only as strictly needed to give consumers what they asked for; tell consumers what personal information they have collected about them; provide consumers a machine-readable copy of their data; provide consumers a right to correct and delete their data; and act as information fiduciaries to the consumers whose information they have collected. Congress should also consider a tailored ban on targeted ads based on our online behavior.

Want more information? Please contact Director of Federal Affairs India McKinney at india@eff.org.