Consumer Privacy Legislation Considerations

There is a daily drip-drip of bad news about how big tech companies are intruding on our privacy. It is long past time to enact new laws to protect consumer data privacy. Specifically, Congress should consider the following:

No Preemption While strong baseline federal privacy legislation would benefit consumers across the country, any federal privacy regulation or legislation that preempts and supplants stronger state action would hurt consumers and prevent states from protecting the needs of their constituents. Current state laws, including California's Consumer Privacy Act, Vermont's Data Broker Act, and Illinois' Biometric Information Privacy Act already take action to protect consumers, and other states are looking at similar proposals. After years of opposing any data protection law outright, big tech companies are now proposing "one federal standard" only because the state laws are working. Allowing the states to continue to protect their constituents is in the best interest of all users.

Enforcement The real test of any new federal data privacy legislation will be how it is enforced and by whom. Any bill that truly protects internet users must contain the most important enforcement tool: the empowerment of consumers to go to court to enforce their privacy rights. All too often, government agencies lack the resources to enforce existing laws or simply choose not to pursue that case. Additionally, in some cases, industries have "captured" the agencies charged with oversight, resulting in weak or no enforcement. Including a private right of action in a federal consumer data privacy bill would ensure that the protections designed by Congress are enforced, either by government agencies or consumers themselves.

Fairness Privacy is a fundamental human right. A federal privacy law should recognize this by including a non-discrimination rule, forbidding companies from denying goods, charging different prices, or providing a different level of quality for consumers who exercise their privacy rights. Without this rule, pay-for-privacy systems will turn privacy into a luxury item and prevent lower-income consumers from enjoying the intended privacy protections.

Privacy Safeguards Consumer privacy legislation also should require companies: to obtain consumers' opt-in consent before collecting, using, and sharing their personal information; to tell consumers what personal information they have collected about them; to provide consumers a machine-readable copy of that information; and to act as information fiduciaries to the consumers whose information they have collected. Also, users gain often new rights only to effectively lose them when they "agree" to terms of service and end user license agreements that they haven't read and aren't expected to read. Any consumer data privacy law must prohibit waivers, and the mandatory arbitration requirements that often come with them, which often allow companies to sidestep the users' rights.

Notice and Consent Federal privacy legislation should require companies to get a consumer's consent before collecting, using, or sharing their personal information. And if a consumer consents to collection of their data for one purpose (like their movements for a fitness tracker or their activity for a productivity monitor), the company should be required to get additional consent before selling this data, or using it for another purpose.

Want more information? Please contact India McKinney at **india@eff.org**.