Consumer Privacy Legislation

Over 90% of Americans feel like they have no control over their data or their online privacy. Congress should be actively working to give back control of each users' digital presence, instead of letting the companies with the worst privacy track records dictate users' legal rights. Strong privacy legislation in the United States is possible, necessary, and long overdue.

But any new federal data privacy regulation or statute must not preempt stronger state data privacy rules. State legislatures have long been known as "laboratories of democracy" and they are serving that role now for data privacy protections. For example, in 2018, California enacted the Consumer Privacy Act ("CCPA"). Also in 2018, Vermont passed the Data Broker Act, which begins the process of regulating data brokers. Back in 2008, Illinois passed the Biometric Information Privacy Act (BIPA), the gold standard for biometric privacy protection nationwide. Other states, including Washington State, Maine, Maryland, Massachusetts, New Jersey, New York, Oregon, and Texas, have considered various privacy protections for their residents.

While these laws could be strengthened, their swift consideration highlights how state legislators are often in the best position to respond to the needs of their constituents. 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 actually hurt consumers and prevent states from protecting the needs of their constituents.

In November 2018, EFF submitted a letter with more details on our position in response to the U.S. Department of Commerce's request for comment on "Developing the Administration's Approach to Consumer Privacy," urging the agency to consider any future policy proposals in a users' rights framework. We emphasized five concrete recommendations for any Administration policy proposal or proposed legislation regarding the data privacy rights of users online:

1. Requiring opt-in consent to online data gathering and sharing.
2. Giving users a "right to know" about data gathering and sharing.
3. Giving users a right to data portability.
4. Imposing requirements on companies for when customer data is breached.
5. Requiring businesses that collect personal data directly from consumers to serve as "information fiduciaries," similar to the duty of care required of certified personal accountants.

It is also important that any new regulations must be judicious and narrowly tailored, avoiding tech mandates and expensive burdens that would undermine competition — already a problem in some tech spaces — or infringe on First Amendment rights. To accomplish that, policymakers must start by consulting with technologists as well as lawyers. Also, one size does not fit all: smaller entities should be exempted from some data privacy rules.

EFF will continue to oppose any federal legislation that weakens today's hard-fought privacy protections. If Congress enacts weaker federal data privacy legislation that blocks such stronger state laws, the result will be a massive step backward for user privacy.

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