Berkeley Media Studies Group · Campaign for a Commercial-Free Childhood · Center for Digital Democracy · Color of Change · Consumer Action · Consumer Federation of America · Fight For the Future · Public Citizen · U.S. PIRG

Preemption of State Laws: Good for Big Tech, Bad for the Public

FAQ | May 2019

As the push for federal comprehensive data privacy legislation builds, Big Tech lobbyists are resorting to their specious claim that national protections must preempt state laws, lest a "patchwork" of state laws makes it impossible for tech companies to do business. But federal privacy legislation that preempts stronger state laws would only benefit technology companies at the expense of the public.

Local regulators are better positioned than the federal government to understand which communities are being disproportionately impacted and why. They often are the first to notice and take action when consumers are harmed by corporate business practices. Since data processing intersects with nearly every sector of society, the job of protecting Americans' privacy is big enough to require the shared involvement of states and the federal government.

1. Why would preemption of state laws in a federal privacy bill hurt consumers?

Many states have adopted laws that safeguard people's privacy and security, including data breach notice requirements, identity theft protections, electronic health record protections and data disposal rules. If preemption of state laws is included in a federal privacy bill, existing laws would be put in jeopardy.

Given the rapid pace of changes in technology, any law enacted today – even the best and strongest law possible – will soon be out of date. States, by contrast, have long acted as the "laboratories of democracy," able to respond quickly to emerging privacy challenges and develop innovative solutions. Amending federal legislation to account for changes in technology is a process that can take years or decades. Preventing states from enacting privacy laws in the future would leave consumers vulnerable to threats and inadvertently could dismantle state civil rights protections, putting already marginalized groups in greater danger.

A federal privacy law that preempts state laws could leave consumers worse off than they are now.

For example, from the 1990's to 2004, the U.S. Office of the Comptroller of the Currency and the U.S. Office of Thrift Supervision preempted numerous state and city laws intended to prevent the mortgage crisis that led to the 2008 Wall Street collapse. If state regulators' hands had not been tied by preemption, they could have reined in banking and finance abuses long before the collapse – and would have reduced the scale of the largest financial crisis in the U.S. since the Great Depression.

2. What is really driving the push for the preemption of state laws?

Many of the largest technology companies have spoken publicly over the past year to the press and members of Congress in favor of federal privacy legislation – but don't be fooled! The technology industry's version of federal legislation, which includes preemption of state laws, mostly would benefit Big Tech at the expense of public safety and personal privacy long into the future. Big Tech wants to satisfy the public's appetite for privacy protections and broadly preempt existing state privacy laws so that the industry doesn't have to comply with stronger state laws already on the books and can avoid strong state protections in the future as technology develops.

The battle for preemption of state laws is driven in part by the technology industry's desire to avoid complying with the California Consumer Privacy Act (CCPA), set to take effect in 2020. The reason that technology companies have waited until now to discuss comprehensive privacy legislation at the federal level is because they want to continue business as usual, are afraid of the CCPA and fear other states implementing effective safeguards to protect consumers and their civil rights.

3. Which existing state laws could be in jeopardy if preemption is included in a federal privacy bill?

Some examples of existing state laws that could be wiped away by preemption include:

- The California Consumer Protection Act (protects personal data);
- The Illinois Biometric Information Privacy Act (safeguards biometric data);
- The Vermont Data Broker Act (protects consumers from fraudulent data use);
- The Massachusetts Data Security Law (establishes strong security and date breach notification standards);
- Alaska and Nevada's Genetic Privacy laws (safeguards genetic data);
- Dozens of state laws that specifically protect the privacy of schoolchildren and prevent the commercial use of their educational information; and
- Laws that protect consumers in data breaches, which have been enacted by all 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands.

4. What are some examples of existing federal laws that do not preempt state laws?

Many federal privacy laws have not preempted stronger state protections or enforcement efforts. Examples include:

- The Electronic Communications Privacy Act (limits government access to electronic communications);
- The Right to Financial Privacy Act (limits government access to personal financial records);
- The Cable Communications Privacy Act (prohibits cable operators from collecting personal data of subscribers without consent);
- The Video Privacy Protection Act (bans the disclosure of personally identifiable video rental information without consent);
- The Employee Polygraph Protection Act (prohibits employers from using polygraph tests on employees);
- The Telephone Consumer Protection Act (bars most autodialed and prerecorded calls, texts or faxes unless express consent given);
- The Driver's Privacy Protection Act (prohibits the release or use by any state DMV of personal information obtained for licensing purposes); and
- The Gramm-Leach-Bliley Act (requires financial institutions to safeguard sensitive data and explain their information sharing practices).

###