Consumer Reports

2026

STATE LOCATION PRIVACY ACT

What is it?

Consumer Reports' **State Location Privacy Act** is model legislation intended to guide lawmakers interested in creating stronger protections for their constituents' location data. It is informed by our extensive advocacy work on this topic at the state level, including in Oregon and Maryland, both of which recently banned the sale of location data.

Why do states need location privacy bills?

Geolocation can be useful for pro-consumer applications such as turn-by-turn directions and finding a nearby restaurant; however, all too often this information is secretly collected by apps and websites, and sold to dozens, if not hundreds, of data brokers and other third parties with whom consumers have no relationship or even awareness.

Individuals' visits to health care facilities, political rallies, places of worship, and more have been sold by data brokers to marketers, law enforcement, and stalkers. Car companies have sold consumers' location data to insurance companies, which have raised consumers' premiums based on it. Some retailers are creating individualized prices for every consumer, partially based on commercially available location data. Even the precise movements of service members at military installations have been sold to third parties.

What have other states done?

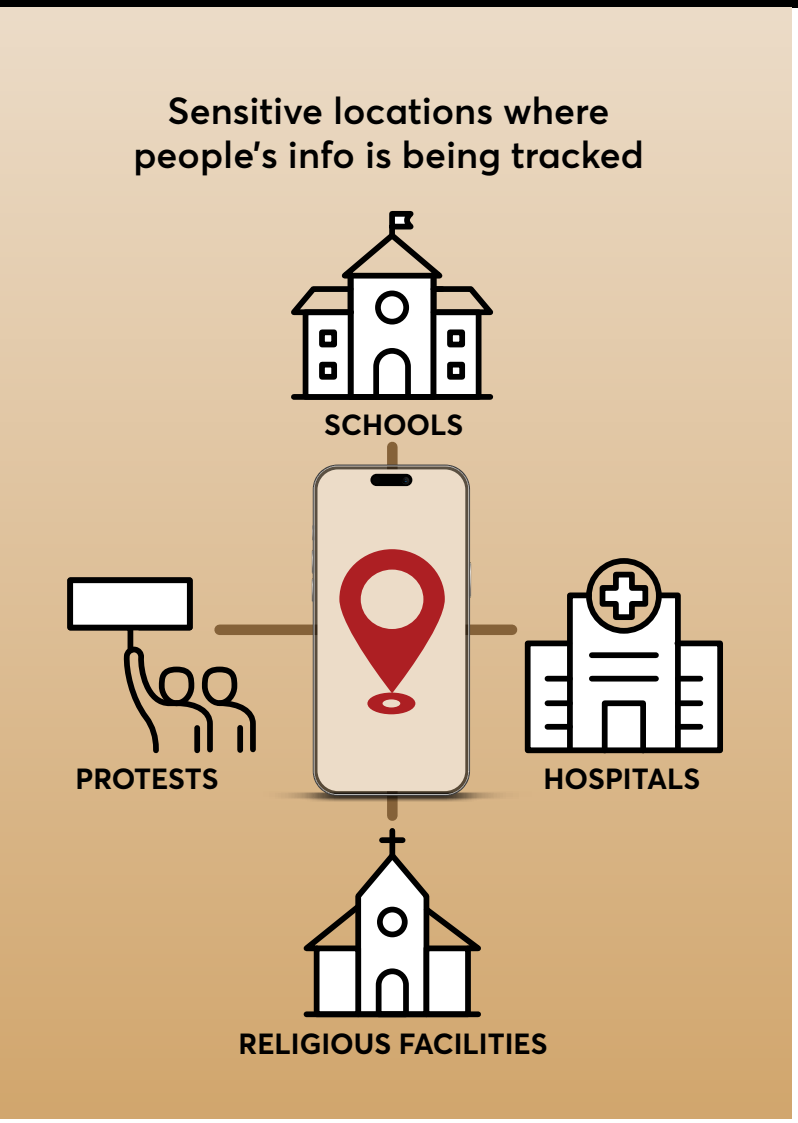
States are increasingly stepping into the void left by federal inaction on this issue. Maryland and Oregon recently banned the sale of location information and other sensitive categories of information. Legislation in California, Maine, New Mexico, Vermont, and Virginia, all proposed in 2025, would've done the same.

Some of these efforts are standalone, and some of them are components of larger comprehensive privacy packages. Some of the bills simply ban the sale of geolocation data, while others include provisions about how geolocation data is collected and used.

What is Consumer Reports' recommended approach?

Consumer Reports recommends both banning the sale of location data and instituting data minimization provisions that prevent companies from misusing location data. Consumers generally don't expect their location information to be sold or used for adversarial purposes, and there is virtually no evidence that the commercial sale of this information enhances consumer wellbeing.

By contrast, industry participants tend to recommend an "opt-in" approach for managing location data. That is, they recommend putting the burden on consumers to read company privacy policies and make individual



choices about how their location information is used relative to each business. But we know privacy notices often fail to provide actionable information, since they are long and hard to parse. And consent is requested so often that it leads to "consent fatigue," which renders many consumer choices meaningless. Ultimately, there is very little that consumers gain from allowing their location information to be sold, and even when consumers do consent, it is very likely that they do not appreciate all of the risks.

Instead, we think that businesses should only collect and use consumers' location information when it is needed to provide the product or service requested by the consumer. This will prevent unwanted uses of location information without requiring the consumer to take any action to protect themselves, and will reduce the overall amount of location information that is collected by businesses in the first place.

To accomplish these goals, our model bill uses common terminology derived from state privacy laws already in effect in more than a dozen states, which is intended to increase interoperability and ease compliance. This model is also structured to function even in states that don't already have comprehensive privacy laws. We also recommend including meaningful enforcement via a private right of action to ensure that these protections are abided by in practice.

Limitations of our approach

Our model bill does not attempt to address every conceivable policy issue surrounding the collection or sale of consumers' location information. Most notably, we do not attempt to address the important questions relating to law enforcement's access to commercial location data, such as when a warrant should be required or how law enforcement agencies should internally handle this information after obtaining it. Generally, commercial and government data privacy frameworks have been separated, and CR's primary expertise lies in the commercial realm. We recommend consulting with other civil society organizations, like ACLU, EFF, or EPIC, to address concerns relating to government access to location data.

We also don't address business thresholds for coverage or specific sectoral exemptions, since many comprehensive laws already legislate these matters. However, in our view, any exemptions from location privacy bills should be carefully considered and narrowly tailored. For example, many state privacy laws exempt banks, hospitals, and/or small businesses wholesale, even though those sectors do not have commensurate protections. Given the sensitivity of consumer location data, we believe the protections of this bill should apply as broadly as possible.