State AGs Step Up Privacy Enforcement

March 31st, 2025 | and Erik Kosa

With attention on Democratic Attorneys General vowing to fill the void left by weakened federal regulators, and perhaps a more partisan divide on enforcement generally, a bipartisan consensus is quietly emerging in the states when it comes to privacy enforcement.

On February 26, Attorney General Tim Griffin (R-AR) announced that Arkansas has sued General Motors and its subsidiary OnStar for selling consumer data to third parties without consent. GM marketed its OnStar products as beneficial to consumers, claiming the data collection would be used for safety reasons and by allowing its collection, consumers could lower their insurance bills. The complaint alleges GM used OnStar to collect driving data from over 100,000 Arkansans' vehicles which it then sold to data brokers who later resold it to insurance companies without telling consumers. The complaint alleges this conduct constitutes deceptive practices in violation of the Arkansas Deceptive Trade Practices Act.

This follows on the heels of Attorney General Ken Paxton's (R-TX) lawsuit against GM in August of last year for the same conduct, alleging violations of the Texas Deceptive Trade Practices Act. Attorney General Paxton has been aggressively pursuing privacy violations. In January, Texas sued Allstate and its subsidiary Arity for unlawfully collecting, using, and selling data about the location and movement of Texans through software surreptitiously embedded in mobile apps on their smartphones in violation of the newly enacted Texas Data Privacy and Security Act ("TDPSA"). The TDPSA requires clear notice and informed consent before certain categories of sensitive data, including precise geolocation information, may be processed.

To date, California has been most aggressive, with Democratic Attorney General Rob Bonta pursuing privacy violations using the first-in-the-nation landmark California Consumer Privacy Act ("CCPA"). Enforcement actions have been brought against Sephora for selling consumer personal information without consumers' permission, and DoorDash for sharing consumer personal information with a marketing cooperative without making the appropriate disclosures and without providing a data sharing opt-out mechanism to consumers. Additionally, on March 7th, the California Privacy Protection Agency finalized a settlement with an auto manufacturer, alleging its consumer rights request and consent mechanisms were more difficult to use than necessary. But other states are catching up.

Texas in particular appears to be staking a claim to become the nation's preeminent privacy enforcement jurisdiction. In standing up his privacy enforcement unit, which has a $5 million budget to enforce the TDPSA, Attorney General Paxton warned, "Any entity abusing or exploiting Texans' sensitive data will be met with the full force of the law. Companies that collect and sell data in an unauthorized manner, harm consumers financially, or use artificial intelligence

irresponsibly present risks to our citizens that we take very seriously." So far, his office's actions have been consistent with his words. The Texas Attorney General netted the largest ever state privacy settlement from Meta, who must pay $1.4 billion to settle allegations it misused biometric data collected from Facebook users in violation of the Texas Capture or Use of Biometric Identifier Act ("CUBI"). Last June, Attorney General Paxton sent letters to over 100 companies alleging they have failed to comply with the new Texas Data Broker Law's registration requirements. And late last year, the Attorney General warned Sirius XM, MyRadar, Miles, and Tapestri that they appeared to be sharing consumers' sensitive data in violation of the TDPSA.

Aggressive privacy enforcement is the new normal, and an investigation into your privacy practices can come from any state. To date, nineteen states and counting have enacted comprehensive privacy laws, imposing novel restrictions on how consumer data may be used and granting their respective Attorneys General enforcement authority with monetary penalties for violations. The California, Texas, Virginia, and New Hampshire Attorneys General have all established dedicated privacy units to focus on enforcing these laws. There are also numerous subject-specific privacy laws like Texas' CUBI, which tripped up Meta. Even states that have not yet enacted comprehensive privacy laws can still use their UDAP authority to pursue much of the same conduct, as Arkansas has shown with General Motors. This trend is likely to continue, so keep these takeaways in mind:

- **Know your data.** What types of data are you collecting? Some data (*e.g.*, precise geolocation data, biometric information, data revealing membership in a protected class) is more sensitive than others and subject to greater restrictions, such as "opt-in" requirements that represent a change from the traditional "notice and opt-out" approach to privacy.
- **Know what your partners are doing.** Be careful about sharing personal information with third parties. Even if you are not in the business of "selling" data in the traditional sense, your sharing may accidentally violate state privacy law restrictions. Consider adopting data processing agreements to govern the sharing of personal information with your business partners to protect how shared data is handled.
- **Consent must mean something.** A common theme in these actions is the allegation consumers did not meaningfully consent to the use of their data. A privacy policy buried on a website is not enough. For example, the Texas DPSA explicitly excludes "acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information" from its definition of consent.
- **Mind the details.** The states' privacy laws all vary slightly from one another. Make sure you understand how your data is regulated by the states in which you operate.