

Publications

July 10, 2026 • Updates

Plaintiffs' Bar Revs Up Claims Under the Driver's Privacy Protection Act

Key Takeaways

- A decades-old federal law is becoming a new source of privacy litigation risk for businesses that handle driver- or vehicle-related data as plaintiffs increasingly invoke the DPPA and analogous state statutes.
- The DPPA reaches beyond state DMVs to downstream recipients of covered information, creating potential class action exposure for businesses that use DMV-sourced data — even if they never obtain records directly from a state DMV.
- Organizations that collect, license, purchase, sell or otherwise use driver- or vehicle-related data should understand whether their activities involve information originating from motor vehicle records and may implicate the DPPA.

The plaintiffs' bar is increasingly turning to a once-arcane, three-decade-old federal law regulating state departments of motor vehicles (DMVs) to pursue privacy claims against private businesses that collect, buy, sell or use vehicle- or driver-related data. For legal departments considering privacy-related risks, the Driver's Privacy Protection Act (DPPA) is notably not limited to businesses that obtain records directly from state DMVs and can pose substantial class action litigation risk for a broad range of entities handling DMV-sourced data — even when the data is obtained through intermediaries. As a result, legal departments, privacy officers and compliance personnel are increasingly assessing how and why their companies process driver-related data and updating their privacy compliance programs to mitigate risk.

In this alert, we explain how the DPPA applies to downstream recipients of DMV-sourced information, highlight emerging litigation trends and outline practical steps businesses can take to assess compliance risk.

Hidden Risks Under the DPPA

The DPPA primarily regulates state DMVs by limiting when they may disclose personal information from motor vehicle records. However, it also imposes liability for downstream recipients that knowingly obtain, use, disclose, resell or redisclose such information for a non-permitted purpose. Permitted purposes are tightly defined and include uses in

Related People

- Starr Turner Drum
- Alexander S. Altman

Related Capabilities

- Privacy & Cybersecurity
- Privacy Counseling
- Privacy Litigation
- Automotive
- Mobility & Vehicle Use

connection with claims investigation, antifraud activity, rating or underwriting by insurers; vehicle emissions, safety and recall activities; and providing notice to owners of impounded vehicles.

The DPPA also allows private actors to obtain and use personal information from a motor vehicle record with “the written consent of the individual.” Businesses that use covered personal information outside of a permitted purpose or without consent may face private litigation. Because the DPPA authorizes liquidated damages of at least \$2,500, plus punitive damages, attorneys’ fees, costs and equitable relief, even narrow uses of driver-related data can lead to meaningful class action exposure.

Because the law can impose obligations on a broad range of businesses that handle personal information from motor vehicle records, DPPA risk can be hidden in ordinary business functions — like vendor-supplied vehicle history data, parking and tolling operations, collections, fleet management, insurance support, fraud investigation, recall outreach, private investigation services and integrated uses of automated license plate reader (ALPR) technologies.

The threshold DPPA-related question for companies to ask is not simply whether they use driver or vehicle data. Rather, businesses must consider whether any personal information in their workflows originated from a motor vehicle record, whether they have established a permitted DPPA purpose for each use and disclosure and whether contracts and records support those purposes.

Increased DPPA Activity and ALPR-Related Risk

Recent filings and decisions suggest renewed plaintiffs’ bar interest in DPPA theories, and the rapid adoption of ALPR technology is providing an additional factual hook. ALPR systems, which are often used by private commercial entities as well as governments, convert plate images into searchable data and can associate scans with time, location, vehicle characteristics and other identifiers. License plate numbers themselves generally are not understood to be “personal information from a motor vehicle record” subject to the DPPA, but private companies using ALPR data may match license plates with DMV records to identify vehicle owners for parking, tolling, collection or enforcement-related notices, creating another use case in which DPPA risk may arise.

Courts are also addressing adjacent vehicle-data claims under state ALPR laws. For example, at least one California court recently allowed claims to proceed under Cal. Civ. Code § 1798.90.5 et seq., which imposes transparency and use-limitation obligations on certain private ALPR operators and end-users.

Open questions in the case law magnify the legal risk to businesses. Courts have not been uniform in interpreting key DPPA provisions, including the scope of “motor vehicle record,” defined as “any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration or identification card issued by a department of motor vehicles”; the scope of “personal information,” defined as “information that identifies an individual” but excluding “information on vehicular accidents, driving violations and driver’s status”; and how broadly the statute’s permissible uses should be interpreted.

What Businesses Should Do Now

Businesses should not wait for courts to settle every DPPA issue before evaluating their own exposure and compliance programs. Organizations in the traditional DPPA ecosystem — auto insurers, manufacturers, towing companies, trucking companies, private investigators, parking and tolling operators, and data brokers — should review and enhance their compliance measures. More broadly, any business that collects, licenses,

purchases, enriches, sells or rediscloses driver- or vehicle-related data should consider:

- Mapping whether any data originates from DMV records;
- Identifying the permitted DPPA purpose for each use and disclosure;
- Reviewing vendor and customer contracts, resale restrictions, audit rights and recordkeeping;
- Evaluating whether any consent workflow is specific and practical enough to support the intended use; and
- Coordinating DPPA compliance with state ALPR, privacy and consumer-protection requirements.

In many downstream or historical-data workflows, obtaining DPPA-compliant consent may be impractical, making data-source diligence and permitted-use documentation critical.

Polsinelli's Technology Transactions & Data Privacy team continues to monitor privacy litigation and enforcement trends and assists clients in defending ALPR and other privacy litigation, conducting compliance assessments, implementing due diligence processes and managing regulatory risk. Please reach out to our team for further guidance.