GM Privacy Penalty Signals A Change In Calif. Enforcement

By **Sonja Arndt-Johnson** (July 1, 2026)

Sonja Arndt-Johnson

On May 8, General Motors and its subsidiary OnStar LLC agreed to pay $12.75 million in civil penalties and be subject to restrictions on their use and sale of drivers' geolocation and driving-behavior data, resolving claims brought by California Attorney General Rob Bonta.

This enforcement action signals a structural shift in privacy law — one that moves beyond compliance as disclosure and into compliance as constraint.[1]

For years, privacy programs have been built around a simple premise: If companies disclose their data practices and provide meaningful user controls, downstream uses are generally permissible. That premise is now under pressure.

California v. General Motors LLC, in the Superior Court of the State of California, County of Napa, reflects a different model. It asks not what companies say about their data, but whether their actual uses of data remain meaningfully connected to the context in which it was collected. Where those uses diverge, disclosure alone is not enough.

The issue becomes whether the use itself is appropriate. This is not a technical shift, but a change in how California regulators define compliance.

The New Question: When Does Use Become Misuse?

At the center of the case is a straightforward but consequential problem. GM collected driving behavior and geolocation data through its connected vehicle services, data ostensibly used for safety, security and quality of services.[2]

Regulators allege that GM later unlawfully used that data in ways that were detached from those purposes, including selling it to third-party data brokers who used it to develop products for insurers.

This framing introduces a new analytical test. The question is no longer whether downstream uses were disclosed — it is whether the downstream uses can be justified at all given the context of collection.

Bonta's theory is explicit: The complaint alleges that GM retained and used data for purposes unrelated to the original purpose, suggesting that even disclosed uses may be impermissible where they are incompatible with the original context.

For companies, this is a critical distinction. Disclosure can inform users, but it cannot make an unrelated use related.

Use — Not Collection — Is Where Risk Now Accumulates

Most companies are designed to manage collection. Companies invest heavily in notices, consent mechanisms and user rights processes, but the highest-risk activities — aggregation, enrichment, retention-driven analytics, partnerships and monetization — occur

downstream. They emerge over time, across teams and often without a single moment of approval.

The GM case reflects a shift in enforcement toward these downstream practices. The Federal Trade Commission's parallel January action — In re: General Motors LLC — similarly focuses on how GM collected, used and disclosed sensitive driving data, including its transformation into products used for insurance-related purposes.[3]

This is an important change for California regulators. Regulators are no longer solely evaluating privacy at the point of collection — they are examining the life cycle of data across the enterprise. Where that life cycle reveals that data has drifted away from its original context, the issue is no longer solely whether the company disclosed that drift, but also is whether the drift itself is defensible.

Sensitive Data Narrows What Companies Can Do

The nature of the data at issue in GM matters. Driving behavior and geolocation data are highly revealing, reconstructing patterns of conduct over time and enable predictions about individual behavior. That sensitivity constrains downstream use.

Practices that might be tolerated for less sensitive information, such as broad analytics and cross-context data sharing, become significantly harder to justify when applied to data that reveals where people go and how they behave.

This leads to a more differentiated model of privacy law. The more sensitive the data, the narrower the set of permissible uses. Context matters, but so does the nature of the information itself.

Monetization Is the Boundary Test

If there is a single inflection point in the GM case, it is monetization.

When data collected to provide a service is later shared, licensed or transformed into an independent commercial product, the inquiry changes. The company that is collecting the data is no longer using data to deliver value to the customer; it is extracting value from the data itself. That shift makes misalignment visible.

In GM, the alleged sale of driving data to data brokers — who then used it to develop risk-scoring products for insurers — created a clear disconnect between the original purpose of collection and the downstream use.[4]

Monetization therefore functions as a practical boundary test. It introduces new actors, new incentives and new purposes that expose whether data has moved beyond its original context. Even where monetization is disclosed, it may still be difficult to reconcile with that context, particularly for sensitive data. Disclosure may explain the practice, but it does not necessarily justify it.

Retention Is Not Neutral

The GM case also highlights a less recognized driver of risk: retention.

The complaint alleges that GM retained data longer than necessary to provide its core services and then repurposed that data for new uses, violating the California Consumer

Privacy Act's data minimization principle.[5] This is not incidental: retention enables repurposing.

The longer data is held, the more opportunities exist to aggregate it with other data, apply new analytics and deploy it in new business contexts. Over time, that process erodes the connection between data and its original purpose. The operative question is no longer how long this data can be stored, but instead, what justification remains for using it now.

Compliance Is Becoming Empirical

The GM matter suggests that compliance can no longer be demonstrated through policies alone. It must be demonstrated through actual data practices.

Regulators are increasingly focused on how data is used in practice, looking at how data flows across systems, how data is combined, and how data supports business activities over time. This is an empirical inquiry. It evaluates what data does, not just what companies say about it.

If those practices produce uses that diverge from the context of collection, disclosure alone will not resolve the issue. Companies must be able to show that their uses remain substantively aligned with purpose.

What Companies Should Do Now

The implications are operational, not theoretical.

First, identify context breaks. Companies should focus on uses that depend on extended retention, aggregation across datasets or secondary analysis. These areas are where divergence is most likely to occur.

Second, treat monetization and external sharing as trigger events. Companies should treat any movement of data into external commercial ecosystems as presumptively high-risk and reassess these risks accordingly.

Third, evaluate uses, not just disclosures. The relevant question for companies is no longer solely whether a use appears in a privacy policy, but whether a use can be defended as a continuation of the purpose that justified collection in the first place.

Conclusion

The GM enforcement action does not eliminate disclosure or user choice. It does, however, make it clear that disclosures and user choice are no longer sufficient to define the boundaries of permissible data use.

Where data collected in one context is used in another — particularly in ways that are sensitive or commercial — California regulators are asking whether that use can stand on its own. They are asking not whether the use was disclosed, but whether it is justified.

That shift relocates privacy risk from policy to practice — from what companies say to what they actually do.

Sonja Arndt-Johnson is special counsel at Buchalter LLP.

[1] People of the State of California v. General Motors LLC and ONSTAR LLC, No. 26CV001011 (Cal. Super. Ct. filed May 8, 2026). Complaint, ¶ 5 ("General Motors")

[2] Id. at ¶ 16. (alleging collection of driving behavior and geolocation data through OnStar services were sold to Lexis and Verisk).

[3] In re General Motors LLC, FTC File No. 242-3052 (F.T.C. Jan. 14, 2026).

[4] General Motors at ¶ 23 (alleging consumers were not informed their data was being used to set auto insurance rates).

[5] Id. at ¶ 24.