



In THIS Issue:

Feature Articles	1, 3
New Members	5
President's Message	5
Advertising Opportunities.....	10
Board of Directors	10

2025 NADC FALL CONFERENCE

October 19-21, 2025

The Ritz Carlton Chicago | Chicago, IL

SAVE THE DATE



Contact Us:

NADC
1800 M Street, NW
Suite 400 South
Washington, DC 20036
Phone: 202-293-1454
Fax: 202-530-0659
info@dealercounsel.com
www.dealercounsel.com

Recent Federal and State Actions, Laws Target Automotive Industry Over Location and Driving Behavior Data Practices



Botkin



Hutchins



Sprinkle

By Robert Botkin, Sarah Hutchins,
and Todd Sprinkle, *Parker Poe's*
Raleigh

Earlier this year, the Federal Trade Commission (FTC) announced that it was taking action against General Motors and OnStar over allegations that the companies did not adequately notify customers and obtain consent related to the collection, use, and sharing of data. The federal action comes on the heels of a complaint filed last August by Texas Attorney General Ken Paxton — also against GM — centered on the alleged unauthorized sale of consumer data. As of the start of this year, you can also add Connecticut to a growing list of states focused on consumer privacy. The Connecticut Data Privacy Act impacts certain auto dealerships as businesses covered under the law must honor a universal opt out preference from consumers over the use or sale of their personal data.

Taken together, the FTC proposed order, the Texas action, and Connecticut law serve as recent examples of enforcement against the automotive industry as it relates to the unauthorized sales of consumer data, highlighting the increasingly complex and often unclear regulatory landscape surrounding data privacy.

Automotive dealers should take this opportunity to review their data practices, especially in technologies that have not traditionally fallen under data privacy scrutiny, ensuring that they are transparent and that consumers are informed about how their data is used.

What the FTC Proposed Order States

Under the proposed FTC order, GM and OnStar will be banned for five years from disclosing consumers' sensitive geolocation and driver behavior data to consumer reporting agencies. The FTC's complaint alleges that GM used a misleading enrollment process for its OnStar connected vehicle service and the OnStar Smart Driver feature, failing to clearly disclose the collection and sale of consumers' data to third parties. GM collected data as frequently as every three seconds, which was used by consumer reporting agencies to compile credit reports affecting insurance rates.

Disclaimer: The *Defender* articles do not constitute legal advice and are not independently verified. Any opinions or statements contained in articles do not reflect the views of NADC. Cases cited in articles should be researched and analyzed before use.

The proposed order states:

- GM and OnStar are prohibited from misrepresenting how they collect, use, and share consumers' data.
- GM and OnStar must obtain affirmative express consent from consumers before collecting connected vehicle data, with exceptions for emergency situations.
- The companies must allow consumers to request and delete their data and provide options to limit data collection from their vehicles.

Texas's Complaint Also Centers on Consumer Data

The Texas Attorney General's complaint argues that the company's data practices may have violated the Texas Deceptive Trade Practices Act (DTPA). Specifically, the complaint alleges that vehicle models from 2015 and after used telematics systems to "collect, record, analyze, and transmit highly detailed data about each time a driver used their vehicle." The complaint goes on to allege that GM then sold this information to companies who generate "driving scores." These driving scores were then in turn sold to insurance companies for their own use. By prompting consumers to enroll in the telematics system services without clearly informing consumers of the data being collected by the system and its ultimate use in the driving scores, GM's practices qualified as "advertising goods or services with intent not to sell them as advertised," and "failing to disclose information concerning goods or services which was known at the time of transaction when such failure to disclose was intended to induce the customer into a transaction the customer would not have entered otherwise."

The central issue is whether consumers were fully aware of and consented to the collection and use of their data. The complaint also raises concerns about broader privacy violations, suggesting that GM's data practices may have exposed consumers to risks, including potential misuse of sensitive information by third parties.

The legal arguments put forth by Paxton reflect a broader tension between regulatory expectations and the practical realities of operating in a data-driven world. The complaint suggests that the company's consent mechanisms were inadequate, but it also raises questions about the effectiveness of applying traditional legal standards to modern, technology-driven business practices.

Final Takeaways

The recent FTC action, the Texas complaint, and Connecticut law serve as important reminders for the automotive industry when it comes to state and federal approaches to data privacy enforcement. Automotive dealers should take the following steps in light of these enforcement actions:

- Closely examine data collection practice to ensure they are obtaining clear and informed consent from consumers. This includes reviewing privacy policies and ensuring that they provide explicit information about how consumer data will be used, shared, and sold.
- Ensure privacy disclosures are straightforward and easily understood by consumers.
- Monitor regulatory developments and changes in state and federal laws.
- Implement robust data protection measures to safeguard consumer information. This includes ensuring that any data shared with third parties is handled securely and in accordance with applicable privacy laws.

Author Bio:

Robert Botkin is an associate in Parker Poe's Raleigh office. He helps clients of all sizes, from Fortune 50 companies to startups, navigate privacy and cybersecurity issues across different industries, including technology, retail, automotive, and finance.

Sarah Hutchins is a partner in Parker Poe's Charlotte office, serving as the firm's Cybersecurity & Data Privacy Team leader. She is certified as a legal specialist in privacy and information security law by the North Carolina State Bar. Sarah helps clients navigate business litigation, government investigations, and data privacy and cybersecurity.

Todd Sprinkle is a partner in Parker Poe's Atlanta office. His practice includes all aspects of civil litigation, both state and federal, at the trial and appellate levels. Todd focuses on business litigation, financial services litigation, real property dispute resolution, trade secrets, and alternative dispute resolution. He sits on the NADC board of directors.