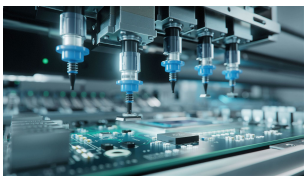

# “Computers on Wheels”: Key Takeaways from AutoConnect’s Security & Privacy Frontiers Panel

May 15, 2026

**Categories:**

Publications

**Authors:**

Mason C. Clutter

Brooke Bishop

When you think about the legal issues facing today’s automotive industry, what comes to mind? Safety standards. Product liability. Quality control. But what about data privacy and security?

At this year’s AutoConnect conference hosted by FBT Gibbons, the “Technology, Security & Privacy Frontiers” panel brought into focus the key data privacy risks that vehicle manufacturers can no longer afford to ignore. Featuring a global cybersecurity executive, a director of cybersecurity engineering for an international automobile company, and the former chief privacy officer at the U.S. Department of Homeland Security, the panel explored how modern vehicles, often described as “computers on wheels,” are collecting and generating vast amounts of data and why privacy and security considerations must be part of the conversation from the outset.

One message resonated throughout the discussion: privacy and security cannot be afterthoughts. Instead, automotive manufacturers should be building privacy and security into vehicle design, development, and deployment from day one.

## What Data Are Vehicles Collecting?

Today’s vehicles collect a wide range of information, much of which extends well beyond what most drivers realize. Panelists discussed several categories of data commonly gathered by connected vehicles, including:

- **Operational and diagnostic data —** such as battery levels, engine performance, and maintenance indicators.
- **Driver behavior data —** including speeding frequency, braking patterns, and seatbelt usage.
- **Geolocation data —** typically collected to support navigation and GPS functionality.




FBT Gibbons

- **Personalization data** — such as phone contacts, call logs, messages, and other information transferred when a driver syncs a mobile device to the vehicle.
- **Images and video** — captured by external cameras used for safety features like blind-spot detection and collision avoidance.

Individually, these data points may seem benign. Collectively, however, they can paint an exceptionally detailed picture of a driver's habits, movements, and personal life — raising significant legal and regulatory concerns.

## What Does Enforcement Look Like?

The panelists emphasized that the automotive sector is not exempt from existing data privacy and security laws. Federal and state privacy frameworks apply broadly across industries, and the automotive industry is no exception.

Manufacturers must also account for international regulations, particularly as vehicles are sold and used globally. The European Union's General Data Protection Regulation (GDPR), for example, imposes strict requirements on how personal data is collected, processed, and secured.

Failure to comply can result in meaningful consequences, ranging from regulatory investigations to significant financial penalties, along with reputational harm that may be even harder to repair.

## How Can Manufacturers Stay Ahead?

Rather than reacting to enforcement actions or public scrutiny, panelists encouraged manufacturers to adopt proactive governance models. One suggested approach includes **three lines of defense**:

- **Board room and senior leadership —** responsible for establishing the company's culture with respect to risk, compliance, and trust with consumers.
- **Consultation with key stakeholders —** including legal, privacy, security, IT, marketing, and outside stakeholders to address potential compliance and other issues on the front end of design, development, and deployment.
- **Governance frameworks —** to ensure that the data lifecycle is considered at each stage of data collection and use and to adjust processes and procedures as needed to address ever-changing technological and legal considerations.

One practical example discussed involved mobile device syncing. Currently, the responsibility often falls on drivers to manually remove their personal data from a vehicle, an effort that may require multiple steps and may not fully erase the data. This creates particular risk in rental vehicles, shared household cars, or even sales through an unaffiliated dealer. The panel suggested that manufacturers explore automated solutions that default to data deletion, reducing reliance on user action while minimizing legal and regulatory exposure.

In addition, panelists recommended considering a data review board to promote consistent, well-documented decision-making around data use, transparency, and accountability. It was also recommended that vehicle manufacturers keep a thorough log of these decisions to ensure they can later be audited or defended if challenged.

## Security by Design: The Core Takeaway

Many of these risks can be significantly reduced through transparency and thoughtful design choices. Clear notice

disclosures, affirmative consent before data collection, and built-in technical safeguards are all essential components of an effective privacy and security strategy.

The overarching takeaway from the "Technology, Security & Privacy Frontiers" panel was clear: automotive manufacturers that embrace *privacy and security by design*, rather than relying on reactive risk mitigation, will be better positioned to comply with evolving data protection laws, changes in technology, and consumer expectations, enabling them to build and maintain consumer trust in an increasingly connected world.

Visit the AutoConnect® 2026 event page for more information about this session and each of our featured panelists. You can also contact the authors or any attorney with FBT Gibbons' Mobility and Data Security & Privacy teams if you have questions or need assistance.






FBT Gibbons