The Internet of Things in the Automobile Industry: Legal Compliance Challenges

- Zoya Khan[1], Dr. Monika Kothiyal[2]

Abstract

The integration of the Internet of Things (IoT) into the automobile industry has created a transformative but legally complex ecosystem. Connected vehicles generate vast volumes of personal and operational data across multiple jurisdictions, simultaneously engaging data protection statutes, cybersecurity mandates, product liability doctrines, and intellectual property regimes. This paper surveys the principal legal compliance challenges arising from automotive IoT, analyses key regulatory frameworks — including UNECE WP.29 R155/R156, GDPR, the US CCPA, and India's DPDP Act 2023 — and advances normative recommendations for a coherent global governance architecture.

Keywords:- *Internet of Things (IoT), Connected Vehicles, Cybersecurity Management System (CSMS), Data Privacy, UNECE WP.29, Product Liability, Autonomous Vehicles*

1. Introduction

The modern automobile is no longer a purely mechanical device. Embedded with hundreds of sensors, telematics control units, LiDAR systems, GPS modules, and wireless communication hardware, it now functions as a rolling data centre operating within a global information network.[3] The Internet of Things — a network of physical devices equipped with sensors, software, and connectivity to collect and exchange data — has become architecturally inseparable from contemporary automotive engineering, enabling features such as predictive maintenance, real-time navigation, autonomous driving, and pay-as-you-drive insurance.[4]

This technological evolution has fundamentally outpaced the legal frameworks designed to govern it. No single global instrument comprehensively addresses automotive IoT. Instead, original equipment manufacturers (OEMs), software vendors, telematics providers, and data processors must navigate a fragmented mosaic of data protection statutes, cybersecurity obligations, product liability doctrines, telecommunications licensing requirements, and consumer protection laws across dozens of jurisdictions.[5] The automotive industry faces significant legal challenges as it navigates these new technologies and markets, with questions of liability, data ownership, and cybersecurity accountability remaining dangerously unresolved.[6] This paper systematically examines those challenges and proposes a normative pathway forward.

2. Architecture and Legal Exposure

A connected vehicle integrates three functional layers, each carrying distinct legal consequences. The **device layer** consists of physical hardware — ECUs, diagnostic ports, telematics control units, ADAS sensors, and infotainment systems. The **connectivity layer** governs communication through cellular networks (4G/5G), Bluetooth, DSRC, and Vehicle-to-Everything (V2X) protocols. The **platform layer** encompasses cloud infrastructure that aggregates, processes, and monetises vehicular data while enabling over-the-air (OTA) software updates.[7]

The device layer implicates product safety and design defect liability; the connectivity layer engages telecommunications licensing and cross-border data transfer rules; the platform layer attracts data protection obligations

---

[1] LL.M., Cyber and Security Law, ICFAI University, Dehradun
[2] Assistant Professor, Law, ICFAI University, Dehradun
[3] Bombay Softwares, IoT in Automobile Industry: A Complete Guide for 2025 (January 2025)
[4] Ibid.
[5] IoT Now, *Regulatory Compliance Continues to be the Most Critical Theme in IoT* (December 2024)
[6] Squire Patton Boggs, *Top 10 Legal and Policy Issues for General Counsel in the Automotive Industry* (2025)
[7] https://www.bombaysoftwares.com/blog/iot-in-automobile-industry

and contractual duties spanning the vehicle's full commercial lifecycle.[8] Connected vehicles generate significant personal information including driving patterns, precise location histories, biometric inputs, and payment records.[9] Critically, hackers can exploit vulnerabilities across these interconnected layers to compromise sensitive data or seize direct control of vehicle functions — creating simultaneous regulatory violations and acute physical safety hazards, with the legal responsibility for prevention still unresolved.[10]

3. Global Regulatory Landscape

European Union

The EU has constructed the most comprehensive regulatory architecture for automotive IoT. The **General Data Protection Regulation (GDPR)** applies to all processing of personal vehicular data connected to EU residents, mandating explicit consent, purpose limitation, data minimisation, and individual rights of access, erasure, and portability, with fines reaching €20 million or 4% of global annual turnover.[11] The **NIS2 Directive** extends mandatory cybersecurity risk management to the road transport sector, while the **EU AI Act** classifies autonomous driving systems as high-risk AI subject to mandatory conformity assessments and post-market monitoring.[12]

Most operationally significant internationally are the **UNECE WP.29 Regulations R155 and R156** (2021). R155 requires OEMs to implement a certified Cybersecurity Management System (CSMS) governing threat identification, risk assessment, and mitigation across the entire vehicle lifecycle.[13] R156 mandates secure management of all OTA software updates. Annex 5 of R155 catalogues 69 distinct attack routes across 7 threat categories, with 23 mandated mitigations.[14] The WP.29 framework transformed cybersecurity from a commercial differentiator into a regulated obligation, compelling manufacturers to fundamentally rethink vehicle design, update management, and post-production security.[15]

United States

The United States lacks a single comprehensive federal data privacy statute. The **California Consumer Privacy Act (CCPA)**, as amended by the CPRA, grants California residents rights to access, delete, and opt-out of the sale of personal information — including telematics and location data — collected by automakers.[16] NHTSA has issued non-binding cybersecurity best-practice guidelines, while proposed federal legislation such as the SPY Car Act has not yet been enacted.[17] The Commerce Department's **Connected Vehicle Rule**, which prohibits hardware and software linked to adversarial nations in connected vehicles, is described as one of the most sweeping ICTS regulations ever applied to the automotive industry, reflecting the national security dimensions of automotive data governance.[18]

India

India's **Digital Personal Data Protection Act, 2023 (DPDP Act)** designates OEMs as "Data Fiduciaries" obliged to process personal data only with informed consent from the "Data Principal."[19] MoRTH has domesticated the UNECE WP.29 framework through **AIS-189** and **AIS-190**, adapting R155 and R156 for Indian type-approval purposes. While technical standards are defined and a 2027 homologation deadline is understood by industry, MoRTH has not yet issued

[8] Squire Patton Boggs, *Top 10 Legal and Policy Issues for General Counsel in the Automotive Industry* (2025)
[9] https://www.bombaysoftwares.com/blog/iot-in-automobile-industry
[10] Ibid.
[11] The Consultant Global, *Data Privacy in Connected Cars* (March 2025); Crypto Quantique, *Building Trust in Automotive Security* (2024)
[12] https://theconsultantglobal.com/data-privacy-in-connected-cars-protecting-user-information/
[13] Cybellum, *Understanding UNECE WP.29 Automotive Cybersecurity Regulation* (May 2024)
[14] Ibid.
[15] Device Authority, *WP.29 Automotive Cybersecurity and Beyond* (December 2025)
[16] The Consultant Global
[17] https://theconsultantglobal.com/data-privacy-in-connected-cars-protecting-user-information/
[18] Ibid.
[19] Hammurabi & Solomon, Navigating Compliance Under the DPDP Act in the Automotive Sector (July 2024)

the formal enforcement notification making compliance mandatory, leaving OEMs in regulatory uncertainty.[20] The Motor Vehicles (Amendment) Act, 2019 does not comprehensively address autonomous or connected vehicle liability, creating a legislative lacuna that poses acute risks as semi-autonomous features proliferate in the Indian market.[21]

4. Key Legal Compliance Challenges

Data Privacy

A connected vehicle is estimated to generate 25 gigabytes of data per hour, encompassing GPS coordinates, driving behaviour metrics, biometric data, occupant profiles, and financial records.[22] OEMs must identify every category of data collected, establish a lawful basis for each processing purpose, and honour data subject rights throughout a vehicle's operational life — often 10 to 20 years spanning multiple ownership transfers.

Consent architecture presents a particular challenge. Manufacturers gather data through multiple touchpoints and facilitate third-party service provider access through various vehicle interfaces, requiring comprehensive data-sharing agreements and renewed consent whenever the scope of data usage changes.[23] **Data localisation** requirements in China, India, and Russia mandate domestic data storage, yet a connected vehicle constantly traverses jurisdictions, generating data subject to multiple and potentially contradictory localisation regimes simultaneously.[24] Additionally, whether an OEM requires a telecommunications licence to import eSIM-equipped vehicles depends on the services being provided, the jurisdiction of use, and the commercial model deployed — non-compliance risks import prohibition, service suspension, or administrative penalties entirely independent of data protection liability.[25]

Cybersecurity

ETSI EN 303 645 mandates 13 baseline IoT cybersecurity provisions, including vulnerability disclosure management, regular software updates, and system resilience.[26] UNECE R155 imposes a dual compliance burden: OEMs must obtain organisational CSMS certification and secure vehicle-type approval for individual models — obligations applicable throughout the production lifecycle. An automotive company suffering a cyberattack faces concurrent GDPR fines, NIS2 enforcement, civil tort liability, and consumer protection investigations across multiple jurisdictions simultaneously.[27]

The **vulnerability disclosure problem** is particularly acute. Security researchers discovering exploitable flaws in connected vehicle systems occupy a legally uncertain position under statutes such as the US Computer Fraud and Abuse Act, which may criminalise good-faith system access. This chilling effect on legitimate security research means that dangerous vulnerabilities may remain unpatched longer than the public interest demands, underscoring the urgent need for statutory safe harbour provisions for responsible automotive security research.[28]

Product Liability

Traditional product liability doctrine — designed for static mechanical products — is ill-suited to continuously updated, software-defined vehicles. A software vulnerability introduced through a post-sale OTA update creates temporal and causal ambiguity about whether the defect arose at manufacture, deployment, or failure. Design defect analysis applying the risk-utility test requires courts to assess AI system safety performance against human alternatives — an empirical exercise poorly suited to conventional adversarial adjudication.[29]

---

[20] ET Edge Insights, *India's Automotive Cybersecurity Law is Ready* (March 2026)
[21] Indian Journal of Legal Research, *Autonomous Vehicles and the Issue of Negligence* (2024)
[22] https://www.bombaysoftwares.com/blog/iot-in-automobile-industry
[23] Ibid. 17
[24] https://theconsultantglobal.com/data-privacy-in-connected-cars-protecting-user-information/
[25] Ibid.
[26] Trustonic, *ETSI EN 303 645 & UNECE WP.29: Legislation for IoT* (July 2023)
[27] Financial Worldwide, Evolution of the Automotive Sector – Data Privacy and Cyber Security
[28] https://www.squirepattonboggs.com/insights/publications/top-10-legal-and-policy-issues-for-general-counsel-in-the-automotive-and-transportation-industry-in-2025/
[29] Brookings Institution, *Products Liability and Driverless Cars* (March 2022

Liability attribution across multi-actor IoT incidents is especially complex. When an accident is caused by an autonomous system relying on a Tier-1 supplier's algorithm, transmitted via a cloud platform, and interpreted by a third-party AI model, proportionate liability among these actors cannot be determined by conventional causation analysis.[30] Some academic commentators have proposed attributing liability to the vehicle's in-context decision rather than any engineering defect — effectively treating the autonomous system as a quasi-legal entity — though no jurisdiction has adopted this approach.[31] OEM liability for post-sale third-party autonomous technology modifications also remains contested, with courts divided on whether original manufacturers bear pass-through liability for aftermarket IoT systems they neither designed nor authorised.[32]

Intellectual Property

Standard Essential Patents (SEPs) governing V2X communication and telematics protocols, held primarily by telecommunications companies, have placed OEMs in an unfamiliar patent licensing environment. FRAND licensing obligations are far more litigation-prone than conventional mechanical component procurement, and automotive manufacturers have been suddenly confronted with dealing with telecom standards and patents requiring licensing — a completely different world from the one to which they have been accustomed.[33] **Open-source software compliance** presents a second risk: connected vehicles incorporate millions of lines of open-source code carrying copyleft obligations such as publication of source code modifications. Supply chain complexity means non-compliant components may enter vehicle software stacks without OEM awareness, creating copyright infringement exposure that operates independently of safety or data frameworks.[34]

5. Recommendations and Conclusion

The foregoing analysis reveals a systemic misalignment between automotive IoT innovation and the legal frameworks governing it. Four normative recommendations are advanced.

First, international bodies should develop a **harmonised global framework** extending the UNECE WP.29 model into data privacy, liability allocation, and telecommunications interoperability, supported by mutual recognition agreements that reduce jurisdictionally contradictory compliance demands.

Second, product liability law should be **updated by statute** to clarify that OTA updates constitute product modifications for liability purposes, to designate the software deployer at the time of the harmful failure as the primary defendant, and to establish proportionate liability rules for multi-actor IoT incidents.

Third, **mandatory vulnerability disclosure safe harbours** should be enacted in all major jurisdictions, protecting good-faith security researchers who responsibly identify and disclose connected vehicle flaws, thereby accelerating remediation before malicious exploitation.

Fourth, **India** should urgently issue the formal enforcement notification for AIS-189 and AIS-190, reconcile the DPDP Act's consent framework with the practical realities of ambient vehicular data collection, and amend the Motor Vehicles Act to provide a clear statutory foundation for connected and autonomous vehicle liability.

The Internet of Things has irreversibly transformed the automobile into a networked platform embedded within the global data economy. The legal challenges this generates — fragmented privacy obligations, mandatory cybersecurity compliance, unstable product liability doctrine, SEP licensing conflicts, and cross-border jurisdictional complexity — are not isolated problems but interconnected expressions of a single fundamental tension: the law's reliance upon fixed, geographically bounded actors confronting technology that is continuous, distributed, and dynamically reconfigurable.

---

[30] https://theconsultantglobal.com/data-privacy-in-connected-cars-protecting-user-information/
[31] J W Zipp, A Reexamination of Tort Liability for Autonomous Vehicles (2016) University of Denver Transportation Law Journal
[32] Brookings Institution, *Products Liability and Driverless Cars* (March 2022)
[33] Squire Patton Boggs, Top 10 Legal and Policy Issues for General Counsel in the Automotive Industry (2025)
[34] RSM Global, 2025 Technology and Cyber Security Trends in the Automotive Industry (2025)

Sustained legislative reform, international coordination, and doctrinal adaptation are essential to ensure that the connected vehicle ecosystem operates with the accountability and safety that its users deserve.[35]

[35] IoT Now, Regulatory Compliance Continues to be the Most Critical Theme in IoT (December 2024)