Privacy + Security Forum

Session:
Under the Hood - Security and Privacy Risks in Connected Vehicles

Privacy+ Security Forum

Speakers

Emily Storm-Strong
Senior M&A and Corporate Legal Counsel, Wabash

Geoffrey Irving
General Counsel, AnySignal

Isaiah Soval-Levine
Director, AlixPartners

Privacy+ Security Forum

Introduction to Automotive Connectivity

The automotive industry is a vast global ecosystem

$3 trillion in annual revenue and a major regional employer

Approximately 60 million vehicles manufactured every year, involving roughly 50 countries

Highly regulated environment where road user safety remains the overarching priority

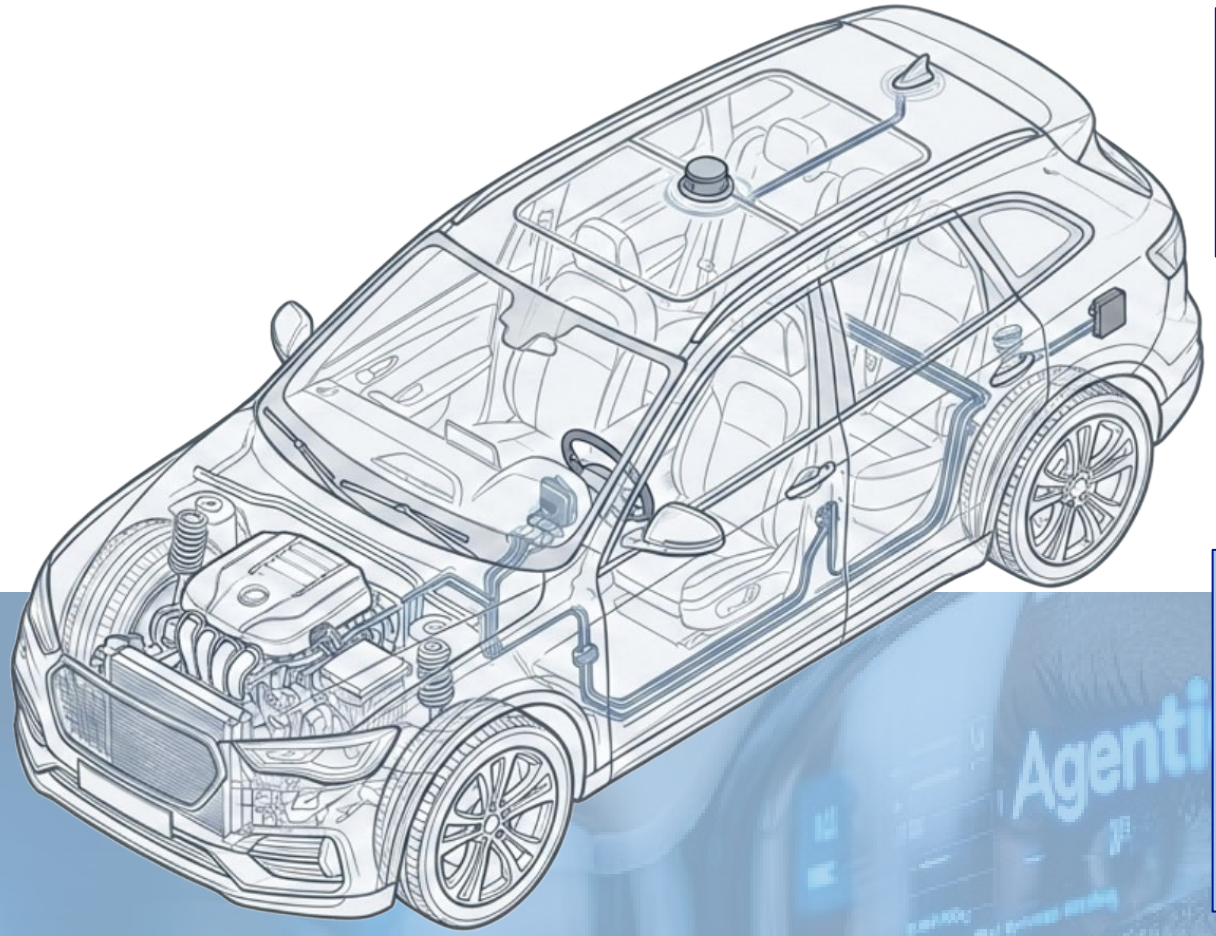
Connectivity has transformed vehicles from “steel on wheels” into networked computers

Privacy+ Security Forum

Modern Vehicles Generate Staggering Amounts of Data

Cabin Controls and Infotainment

Infotainment system and display; Bluetooth, USB, and Wi-Fi connections to smartphones; microphones for voice commands; cameras to detect distracted or drowsy driving; OBD-II port; climate control; seat position; weight detection.



Connectivity Systems

GPS, satellite, radio, RFID, V2X (Vehicle-to-Everything) environment mapping, and external temperature.

Engine & Drivetrain Sensors

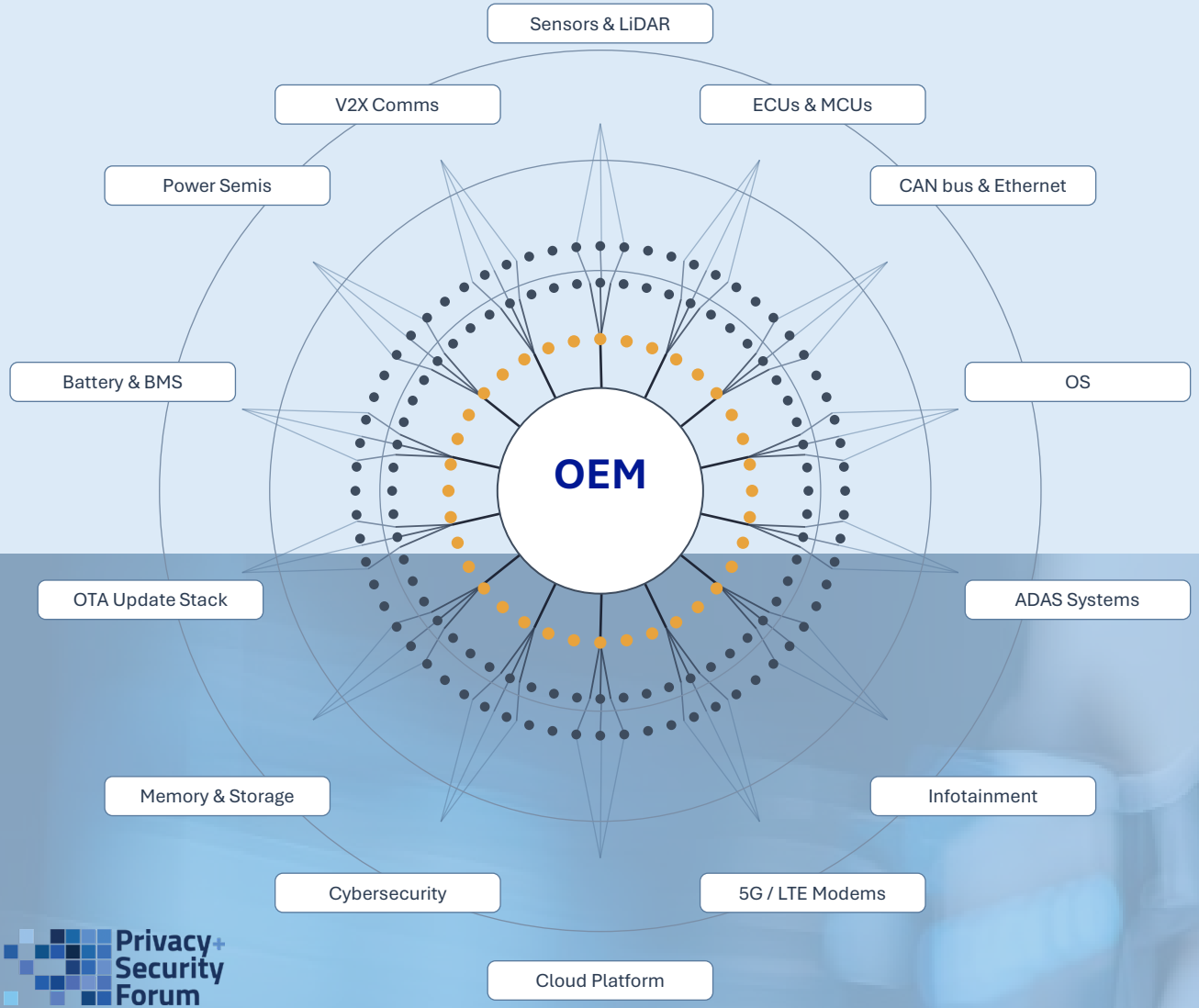
Real-time telemetry on speed, engine performance, acceleration, braking, turns, tire pressure, and EV propulsion systems.

Exterior Cameras, LiDAR & Radar

Lane markings, obstacle detection, traffic sign recognition, blind-spot monitoring, and 360° surround awareness for ADAS.

Privacy+ Security Forum

A Complex Hardware and Software Supply Chain



Hardware Complexity

A modern ICE vehicle integrates **~30,000 distinct parts** orchestrated through **1,400+ Tier 1 suppliers** and a vast network of Tier 2 and Tier 3 vendors.

Software Interdependence

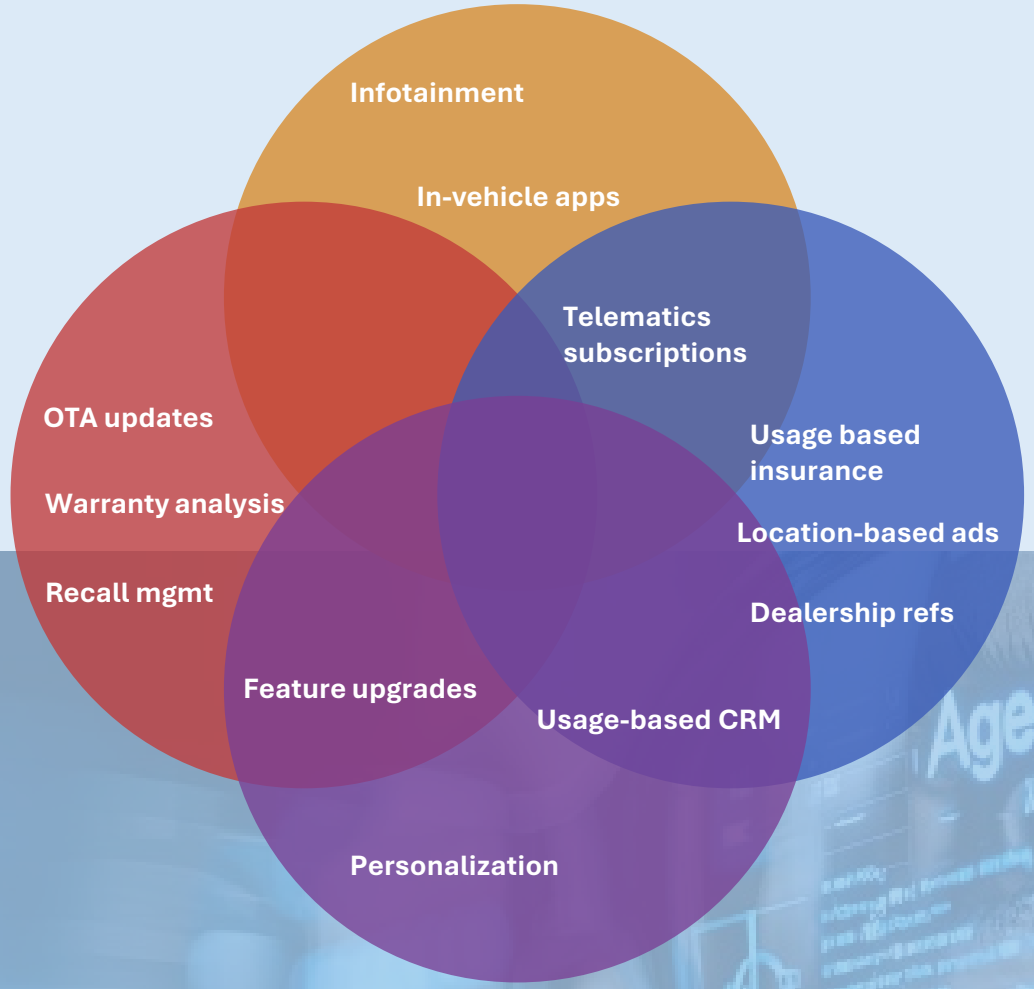
100+ companies contribute to the software stack with **complex hierarchical relationships**

Privacy+ Security Forum

Connectivity Creates Value for the Industry and Consumers

New customer acquisition

Operational efficiencies
(cost reduction)



New revenue streams

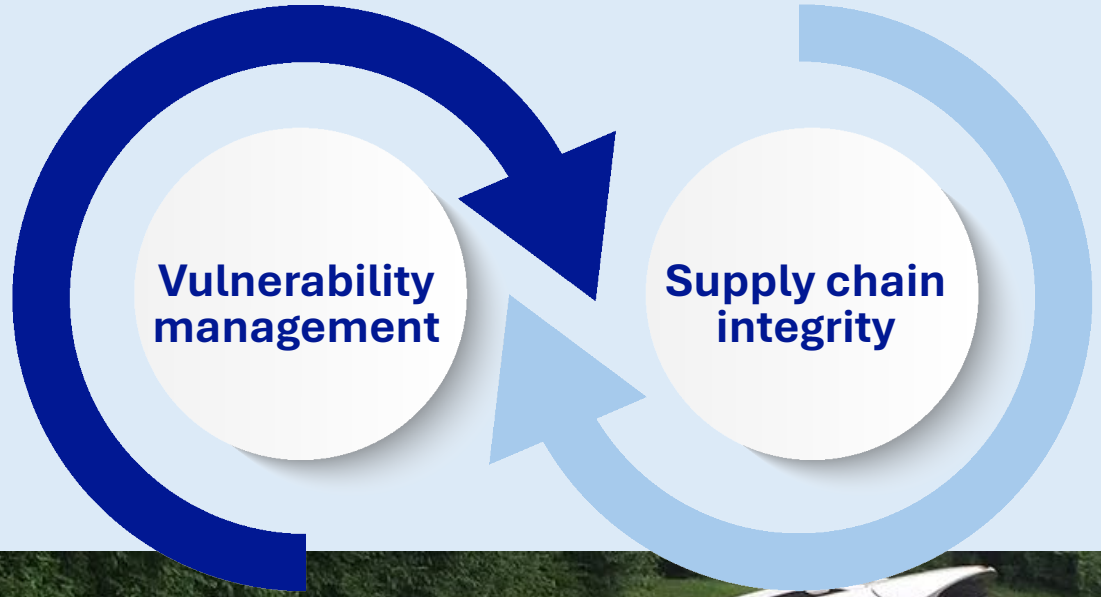
Brand & customer loyalty

Privacy+ Security Forum

Security Implications of Connectivity are Enormous

Challenge: The cyberattack surface is vast and expanding

Response: Industry standards: ISO/SAE 21434 for cybersecurity engineering; UNECE WP.29 establishing CSMS framework and requirements



Challenge: OEMs are integrators; a vulnerable Tier 2 component can compromise an entire fleet

Response: Software Bills of Materials (SBOMs) and Hardware Bills of Materials (HBOMs) are emerging as core compliance artifacts

Privacy+ Security Forum

Privacy Implications: Scope, Notice, and Sensitive Information

Scope

Advances in AI make possible re-identification of technical data like braking and acceleration patterns

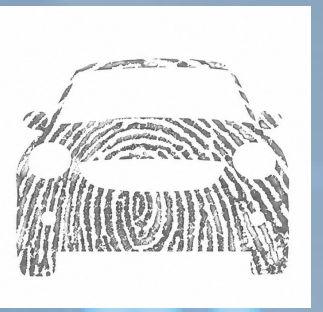
Notice and consent

Consumers need to be informed about the data that is collected as they drive, how it used, and who receives it.

Sensitive information

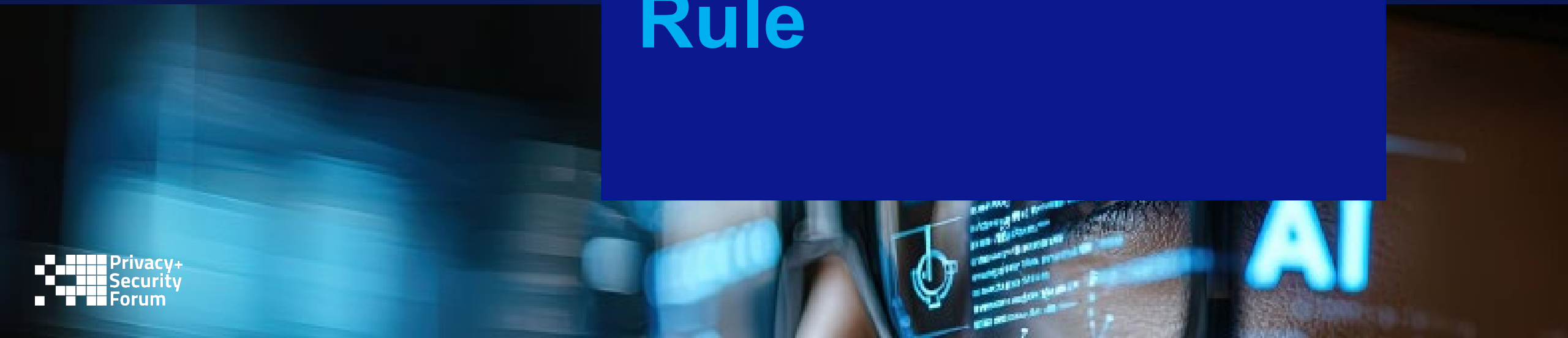
Geolocation reveals intimate daily details; voice recognition and eye-movement tracking systems collect biometric data

Timestamp	CAN-ID	Req	Len	Data
1481492683.285052	0x0208	000	0x8	0x00 0x00 0x32 0x00 0x0e 0x32 0xfe 0x3c
1481492674.736055	0x02c4	000	0x8	0x82 0xc8 0x00 0x0f 0x03 0x00 0x92 0x3c
1481492674.736055	0x02c4	000	0x8	0x82 0xc9 0x00 0x0f 0x00 0x00 0x92 0x4c
1481492674.736055	0x02c4	000	0x8	0x82 0xcc 0x00 0x0f 0x08 0x00 0x92 0x5a
1497323915.123844	0x018e	000	0x8	0x03 0x03 0x00 0x00 0x00 0x00 0x07 0x3f
1497323915.112910	0x00f1	000	0x6	0x28 0x00 0x00 0x40 0x00 0x00
1481492674.736055	0x02c4	000	0x8	0x82 0xd2 0x00 0x0f 0x0c 0x00 0x92 0x5d
1481492674.736055	0x02c4	000	0x8	0x82 0xa1 0x00 0x0f 0xa1 0x00 0x92 0x4d



Privacy+ Security Forum

OICTS Connected Vehicle Rule



Privacy+ Security Forum

Office of Information and Communications Technology and Services (OICTS)

Overview

Sits within the Bureau of Industry and Security (BIS) at the U.S. Department of Commerce

Authorities derived from EOs 13873 and 14034, formalized by the ICTS Final Rule (Dec. 2024)

Empowered to investigate, mitigate, or prohibit ICTS transactions involving foreign adversaries that pose undue or unacceptable national security risk

Led by an Executive Director; organized around investigations, policy, and enforcement functions

Privacy+ Security Forum

Connected Vehicles Present National Security Risks

Data exfiltration

Theft of sensitive information from vehicles, including personal data on U.S. drivers and owners

1

Sensitive site exposure

Collection and export of GPS, camera, and sensor data revealing military bases, critical infrastructure, and data centers

2

Remote manipulation

Foreign-adversary control of vehicles via compromised connectivity or automated driving systems

3

Supply chain dependence

ICTS supplied by entities linked to China or Russia, exposing U.S. fleets to governmental pressure

4

Large-scale cyberattacks

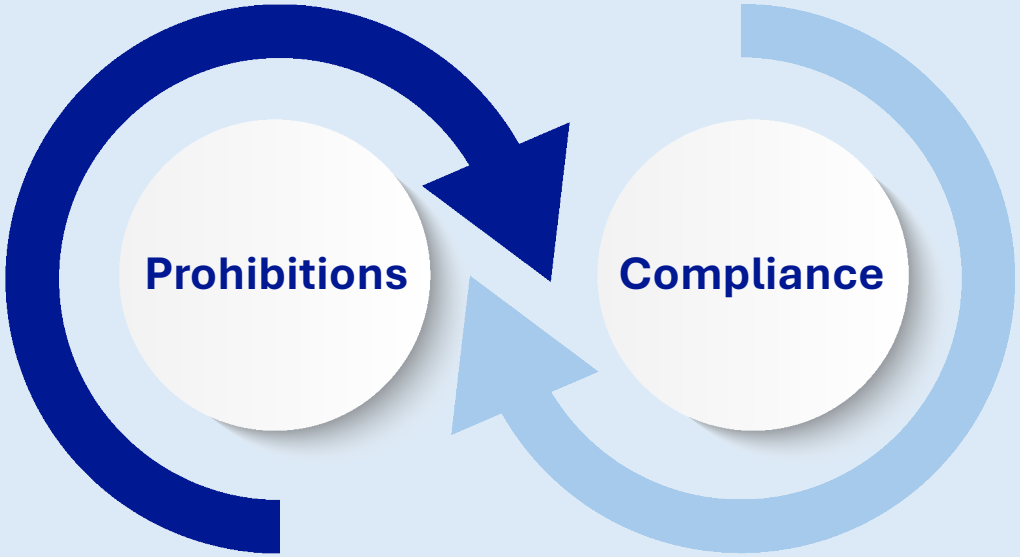
Vulnerabilities in vehicle connectivity and related cloud services could disrupt U.S. transportation networks

5

OICTS Issued the Connected Vehicle Rule to Address These Risks

Restricts the import and sale of connected vehicles incorporating covered software or hardware

Targets components designed, developed, manufactured, or supplied by entities owned, controlled, or directed by China or Russia



OEMs and importers must submit Declarations of Conformity at least 60 days before first sale or import

Supported by documented due diligence: third-party assessments, HBOMs, and SBOMs; 10-year recordkeeping


```
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "alpine",
  "documentNamespace": "https://anchore.com/syft/image/alpine-0f87c686-5633-421b-b5e2-620ade3fd5f9",
  "creationInfo": {
    "licenseListVersion": "3.23",
    "creators": [
      "Organization: Anchore, Inc",
      "Tool: syft-1.4.1"
```

How OEMs and Tier 1 Suppliers Are Preparing

1

Mapping the supply chain

Tracing hardware/software components to identify any PRC or Russia affiliations

Identifying and qualifying alternate suppliers where covered links exist

2

Updating supplier contracts

Adding supply chain mapping, SBOM/HBOM disclosure, recordkeeping, and reporting clauses to support BIS standards

3

What makes this rule different

Targets country-of-origin and ownership, not cyber posture. ISO/SAE 21434 or UNECE WP.29 compliance does not satisfy it

Demands tiered visibility into Tier 2 and Tier 3 suppliers most companies have never had

Industry Engagement and Enforcement Priorities

Industry engagement leading up to 2027

ANPRM in March 2024 and a public comment process produced significant changes between proposed and final rules

Advisory opinion process via the Compliance Application and Reporting System (CARS) for prospective transactions

Monitoring and enforcement priorities

Quality and accuracy of Declarations of Conformity, supported by 10-year recordkeeping

Visibility into Tier 2 and Tier 3 sourcing, including ownership-and-control attestations from foreign suppliers

Coordination with CBP at import for screening covered hardware and complete vehicles

The Final Rule Did Not Cover Commercial Vehicles

1

Why commercial vehicles over 10,001 lbs. were excluded

Different supply chain structure: smaller production volumes, heavier reliance on aftermarket telematics, and longer product cycles

OICTS recognized the need for a tailored regulatory approach rather than a “one-size-fits-all” framework

2

Are the national security risks different?

Many risks are heightened: trucks routinely access ports and other critical infrastructure that passenger vehicles do not

Larger external attack surface from open CAN, tractor-trailer links, and body-equipment integrations

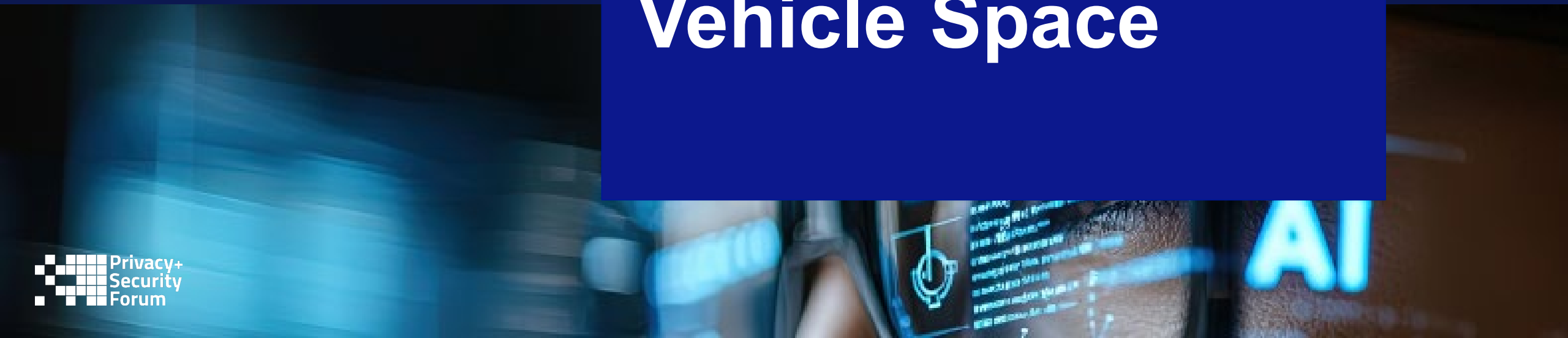
3

What might a commercial vehicle rule require?

Cover aftermarket telematics, upfitter add-ons, trailer systems, and logistics platforms

Privacy+ Security Forum

Privacy and Security in the Commercial Vehicle Space



Privacy+ Security Forum

The Commercial Vehicle Space at a Glance

Scale of the U.S. trucking industry

- ~302 billion miles traveled by all U.S. trucks; ~177 billion miles by combination (long-haul) trucks
- Trucks move approximately 11.8 billion tons of freight annually — roughly 72% of U.S. freight by weight
- Almost 15 million semi-trucks registered
- Average truck driver travels over 90,000 miles per year

Heightened safety concerns

Commercial trucks are larger, harder to maneuver, and carry hazardous materials

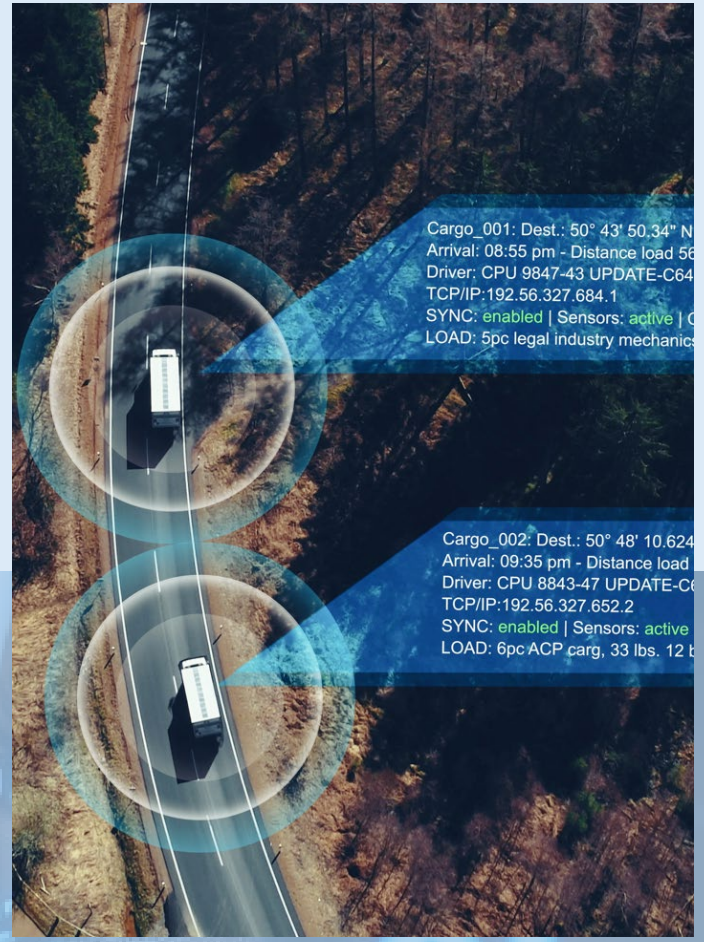
Safety pressure drives heavy investment in monitoring, telematics, and connected safety systems

Mixed ownership of assets makes liability for accidents difficult to assign

Privacy+ Security Forum

What Data Do Commercial Vehicles Generate?

Operational	telematics, GPS location, route, hours of service, fuel and load data
Biometric	fingerprints for vehicle access, facial recognition for driver ID, iris scans, and drowsiness detection
Audio/Video	driver-monitoring systems, in-cab cameras, and exterior dash cams
Personal	commercial driver's license number, SSN, and contact information for compliance and onboarding
Financial	payroll, expense reimbursement, and per-mile / per-load settlements



Privacy+ Security Forum

Connectivity Stack: Commercial vs. Passenger Vehicles

Similarities

- Common building blocks: Telematics Control Units (TCUs), cellular modems, GPS/GNSS, RFID.
- Both segments increasingly rely on cloud-based fleet and OEM platforms for remote monitoring and updates
- Insurance companies driving cost reductions focused on driver safety

Key differences

- **Mixed fleets:** operators run multiple OEMs, classes, and ICE/EV mixes — aftermarket telematics often layer on top of OEM TCUs
- **More open external interfaces:** tractor-trailer link, body equipment, dock and yard systems
- **Multi-vendor build:** OEM, upfitter/bodybuilder, trailer maker, telematics provider, and logistics platform

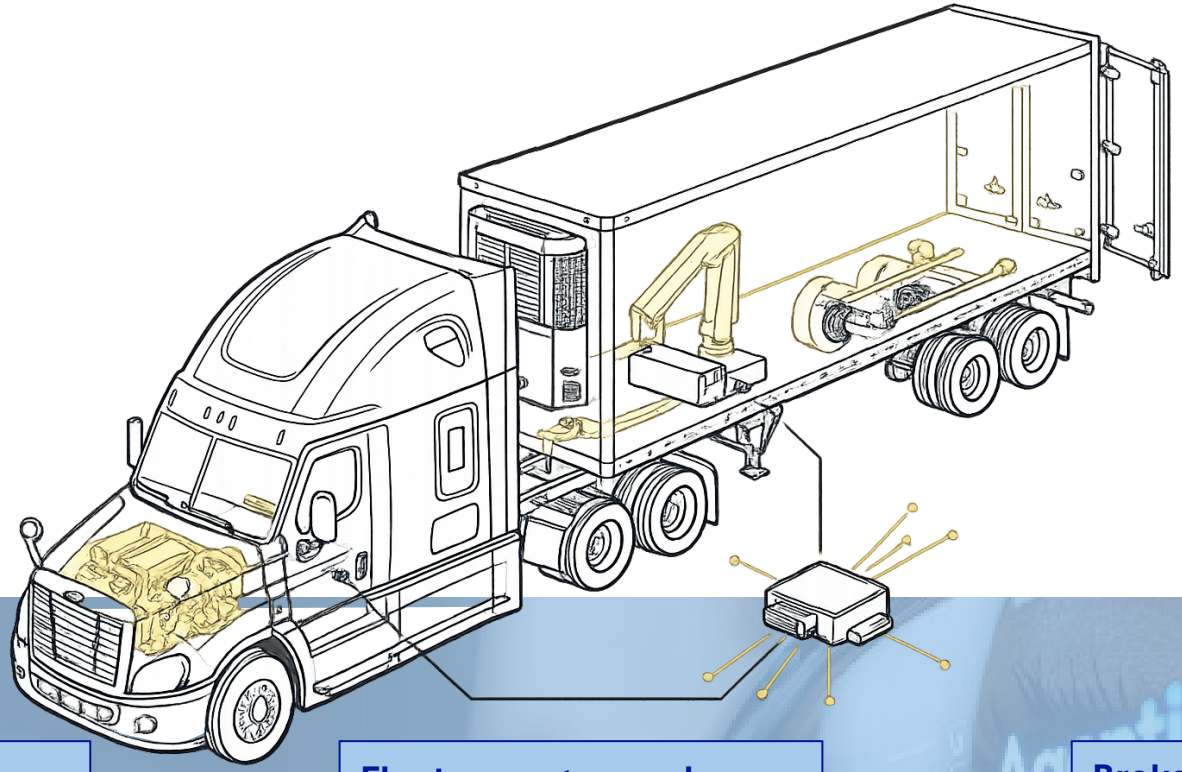
Privacy+ Security Forum

The Commercial Shipping Data Ecosystem

OEMs and upfitters:

Diagnostics, warranty, OTA updates, product engineering

Telematics providers:
Aggregating, normalizing, and reselling location, behavior, and engine data



Insurers:
Underwriting, usage-based premiums, claims defense via dash cam and telematics

Government:

FMCSA hours-of-service, ELDs, IFTA, port and border systems

Warehouses, ports, yards:
Gate, dock, and slot management; chain-of-custody for freight

Fleet managers and carriers:
Safety, dispatch, fuel and asset utilization, driver coaching

Brokers and shippers:

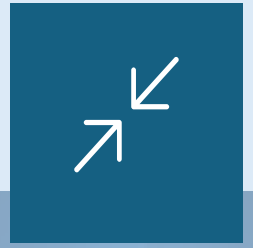
Shipment visibility, ETAs, proof of delivery, freight matching

Privacy+ Security Forum

Telematics Adds Value

Benefits and efficiencies

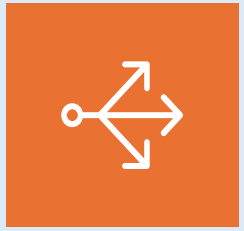
Route optimization, predictive maintenance, fuel savings (large retailers report up to ~8% diesel reduction)



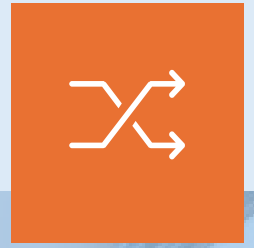
Real-time visibility for shippers, automated proof of delivery, and faster claims processing

Safety analytics: drowsiness detection, hard-braking events, lane departure, in-cab coaching

Contractual and governance gaps



Unclear data ownership and downstream sharing rights when telematics flow OEM → provider → carrier → broker → insurer



Inconsistent retention, deletion, and audit rights across providers; few contracts address employee privacy carve-outs

Emerging best practices: data minimization, role-based access, purpose limitation, and explicit retention limits in fleet contracts

Privacy+ Security Forum

Privacy Legal Context: Employment Relationships Drive the Rules

1

Most personal data collected sits inside an employment or contractual relationship

Drivers operate under a variety of contractual arrangements (employment, contractor, staffing agencies)

Each relationship triggers different notice, consent, retention, and access expectations: CCPA provisions, state notice laws, and common-law privacy all apply differently

Independent contractors and staffing-agency drivers raise tension between employer monitoring rights and the contractor's independent business interests in their own data

2

State-level regulation

CA AB 984: Employers may monitor via digital plates or other "alternative devices" only during work hours and only when strictly necessary for the employee's duties

Detailed pre-monitoring notice required; civil penalties of $250–$1,000 per employee per day for non-compliance

IL Biometric Information Privacy Act (BIPA) – Requires Opt-In consent and security program to ensure safe collection

- *Rogers v. BNSF Railway Co.* with Nuclear Verdict (*later settled*) – companies cannot escape liability by using third-part venders for data collection.

Privacy+ Security Forum

Cross-Border Compliance and Insurance-Driven Monitoring

Cross-border activity multiplies the rules

Which laws apply as drivers cross multiple states and international borders (US–Canada, US–Mexico): driver residence, fleet domicile, route, employer's headquarters?

Common practice: apply the strictest applicable standard fleet-wide rather than route- or state-specific compliance

Insurance and surveillance: granular data drives pricing

Carriers increasingly tie premiums and coverage to telematics scores

Raises fairness questions: data quality, opaque scoring models, and disparate impact across driver demographics

Privacy+ Security Forum

Dual-Facing Dash Cams: Safety Tool or Surveillance?

Driver perception drives acceptance

- Drivers accept cameras when they understand how footage is used
- Surveillance perception spikes when cameras are continuously on, benefits are not explained, or used for over-coaching
- Solving Driver issues – such as proof of visual inspection and DOT maintenance – provides higher engagement for connected solutions

Elements of a defensible policy

- **Notice:** written, conspicuous, signed at hire and refreshed periodically
- **Trigger-based recording:** save inward-facing footage on safety events rather than recording continuously
- **Retention limits:** short default windows; legal hold only when claims arise
- **Access controls:** role-based, audited; no review without a documented business reason
- **Off-duty protections:** cameras and tracking disabled outside hours of service where feasible

Privacy+ Security Forum

Stay in touch

Emily Storm-Strong

emily.stormsmith@onewabash.com

Geoffrey Irving

geoff@anysignal.com

Isaiah Soval-Levine

Isaiah.sovallevine@alixpartners.com

Privacy+ Security Forum