Poster: Mitigating Persistent Personal Data Exposure in Vehicle Infotainment Systems

Bhargab Acharya
University of Memphis

Sam Lauzon
Bishop Fox

Spiros Thanasoulas
University of Memphis

David Balenson
USC Information Sciences Institute

Christos Papadopoulos
University of Memphis

Abstract

Personally Identifiable Information (PII) routinely persists on vehicle infotainment systems after ownership changes, and retrieving it has been shown to be easy with off-the-shelf forensic tools. Such data can be abused by malicious actors. The cryptographic and storage elements needed to address this already exist and are widely deployed in phones and laptops but not vehicles. The challenge is not a gap in technology, but adapting existing mechanisms to vehicle-specific realities: shared use, physical keys instead of passwords, messy identity, and limited OTA updates. We analyze these constraints, identify deployable fixes that require no new cryptographic or hardware primitives, and outline what is needed to implement them in practice. Our goal is to provide actionable guidance for OEMs, regulators, and consumers.

1 Problem Statement

Modern vehicles accumulate personal data over their operational life such as contacts from paired phones, navigation history, call logs, paired Bluetooth device identifiers, application credentials, and personal media. Our prior forensic work [1] has shown this data persists across ownership transitions on commodity hardware. For example, in a field study we conducted of 38 used vehicles for sale, only three contained no visible personal data, and all nine vehicles with built-in navigation retained navigation history from prior owners. Our threat model is an adversary who acquires a vehicle or an extracted module (infotainment or other) through legitimate secondary-market channels, armed with commodity forensic tools, and no manufacturer credentials, looking to cause harm to prior owners such as phishing or extortion.

2 Why Vehicles are Different than Smartphones

Smartphones are the closest working model for what vehicle infotainment may need to emulate. Several pieces port over directly: file-based encryption with per-user keys, hardware-backed keystores, and crypto-erase on factory reset. The hard part is structural. Phones are personal, disposable, and single-user. Vehicles are typically shared, durable, and long-lived. Table 1 shows what breaks in the translation. We find these three differences particularly important. *Authentication is weaker.* A phone needs a PIN or fingerprint, but a car just needs the key fob. Whoever holds it has full access. *Ownership transfers aren't clean.* Today's systems assume one owner hands the car to the next. They have no good answer for valets, mechanics, rentals, family sharing, repossession, or salvage — all cases where someone loses control without meaning to transfer the vehicle. *Credentials can leave with the owner.* A fob can be destroyed in a crash. A car can be stolen, totaled, or repossessed before the owner has any chance to wipe it. Phones don't fail this way — the PIN and biometrics stay with the owner. On top of all this, vehicles have no consistent OTA story yet. While many cars on the road today will get firmware updates, some will probably get none. Moreover, given that often updates require a dealer visit, any fix that depends on pushing an update later may not reach them.

Table 1: Properties that do not translate from phones to vehicles.

Property	Phone	Vehicle
Users	Single primary	Driver, passenger, valet, mechanic, renter
Auth factor	PIN or biometric	Possession (fob) only
Connectivity	Assumed for remote wipe	Often off-network
Update cadence	6+ years of patches	Often zero post-sale
Identity anchor	Apple ID / Google Account	Fragmented or absent
Credential form	In user's head	Physical, transferable at sale

Two consequences deserve emphasis. One, *Authentication*

degrades from a knowledge or biometric factor on the phone to a possession factor only on the vehicle: whoever holds the key fob has full access. Two, *Ownership transitions are not binary*: Current architectures model only full transfer and have no clean answer for valet, mechanic, rental, family-sharing, repossession, or salvage, all of which involve partial loss of control without intent to transfer.

3 The Bottleneck Is Deployment, the Primitives are there

The tools to fix this already exist and are deployed elsewhere, but haven't been integrated into vehicle infotainment. Properly architected, we believe these two approaches work well, and the silicon for both is already in many vehicles. **Encryption-based wipe.** Encrypt the user-data partition from first boot with a key held in a secure element. "Wipe" then just means destroying the key, which can happen in milliseconds, regardless of disk size. iOS works this way. The hardware is already there: automotive HSMs following the EVITA and SHE [2] specs ship in modern vehicles for secure boot on engine, brake, and gateway ECUs, and infotainment SoCs from Qualcomm [5] and NXP [4] include TrustZone-based TEEs [2]. What's missing is software that uses any of it for user data. In our prior forensic work [1] on seven infotainment units across Honda, Hyundai, BMW, and Jeep (model years 2011–2021), none used encryption at rest. **Overwrite-based wipe.** This is slower, but viable when encryption isn't in place. The JEDEC eMMC spec defines SECURE ERASE and SANITIZE commands that destroy spare-area copies on flash [3]. The host just has to call them. We confirmed the gap on a 2016 Honda Pilot and a 2021 Hyundai Palisade: factory reset on both didn't even zero the user-visible blocks, let alone reach the spare areas. **Easy wins are available.** OEM factory resets don't zero visible blocks — the weakest tier in NIST 800-88. Calling SECURE ERASE or SANITIZE can be done in one command. Pairing-scoped data doesn't need a reset at all: contacts and call logs from a paired phone could be deleted when the phone unpairs, the way phones already handle it. And a user-accessible "thorough wipe" menu could cover partial-transfer cases — rental returns, valet, service appointments — that no dealer process touches today. Fortunately, none of this needs new cryptography or new silicon. It just needs to be wired it up.

4 Responsibility and Regulation

What exists. The closest hooks are cybersecurity, not privacy. UNECE R155/R156 [6] (mandatory in the EU since July 2024) and ISO/SAE 21434 gate type approval on a CSMS and cover decommissioning, but treat it as an attack-surface concern, not a departing-user concern. EVITA and SHE specify HSM primitives. GDPR and Oregon's 2025 amendment grant erasure rights but presume a reachable controller. The Alliance for Automotive Innovation Privacy Principles are voluntary and silent on infotainment wipe. Privacy4Cars is a manual dealer service — an existence proof, not a standard.

What they miss. No regulation mandates verifiable deletion at ownership transition with a tamper-evident artifact a non-OEM party can check. R155 protects the vehicle, not the departing user. GDPR-style rights fail in the secondary-market case where the seller is gone. None of the frameworks distinguishes partial transfers (valet, rental, mechanic, repossession) from full title transfer.

5 Our Poster

Our poster will summarize the following concepts. Vehicle infotainment systems accumulate personal data across their operational life, and that data routinely survives ownership and control transitions. The forensic primitives needed to prevent this—crypto-erase, hardware-backed key storage, SANITIZE-invoking resets—are already deployed in adjacent domains and require no new hardware or cryptographic research. The gap is integration and accountability: OEMs must ship the primitives, Tier 1 suppliers must expose attested-wipe APIs on reference platforms, and dealers and salvage operators must invoke them at every transition. Regulation already reaches this space through R155 and GDPR but covers neither verifiable deletion at ownership transfer nor partial-control scenarios such as rental, valet, or repossession. Closing that gap requires extending R155's CSMS scope to mandate an attested wipe path and amending title-transfer law to require a signed deletion certificate—narrow asks that would enforce responsibility allocation without waiting for new technology.

References

[1] ACHARYA, B., ESPINOZA, D., THANASOULAS, S., LAUZON, S., BALENSON, D., AND PAPADOPOULOS, C. Persistent personal data exposure across vehicle ownership and control transitions. In *Proceedings of escar USA 2026* (May 2026). To appear.

[2] AUTOSAR. Specification of secure hardware extensions. Technical Report AUTOSAR_TR_SecureHardwareExtensions, AUTOSAR Consortium, 2022. Release R22-11. Republication of HIS SHE Functional Specification v1.1.

[3] JEDEC SOLID STATE TECHNOLOGY ASSOCIATION. Embedded MultiMediaCard (eMMC) mechanical standard, with MMC electrical standard 4.41. Tech. Rep. JESD84-A441, JEDEC, Arlington, VA, June 2010.

[4] NXP SEMICONDUCTORS. Security and trusted execution environment (tee). Fact Sheet, Document Number: TRUSTEXECENVIRFS REV 0, Sept. 2016. Accessed: 2026-05-05.

[5] QUALCOMM TECHNOLOGIES, INC. Trustzone and secure application. Qualcomm Documentation, Doc. 80-88500-4, Topic 77. Accessed: 2026-05-05.

[6] UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE. UN Regulation No. 155 – uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Tech. Rep. E/ECE/TRANS/505/Rev.3/Add.154, UNECE, Geneva, Switzerland, Mar. 2021.