A FRAMEWORK APPROACH TO
STANDARDIZING CONSENT
MANAGEMENT IN SOFTWARE-DEFINED
VEHICLES

COVESA, All Member Meeting
April 16-18, 2024 - Gothenburg

Philippe Le Berre
Chief Technology Officer, 360ofme
TRUST IS A SYSTEMIC ISSUE, WHICH CALLS FOR A SYSTEMIC APPROACH
Please,
Don’t Read,
Don’t even try to Understand,
Just Mindlessly Consent,
And Forget about it,
Trust us...

By reading this slide, you signify that you have read and accept this Terms and Conditions and Privacy Policy.

Trust is the easiest thing in the world to lose, and the hardest thing in the world to get back.

— R. M. Williams —

CONSENT ILLUSION: TRUST IN CURRENT BUSINESS PRACTICES
• Trust and Privacy are now recognized as Systemic challenges.

• Global Legislation enacted to bridge the “Trust Gap” between OEMs and their customers.


• Personal Data Residency is emerging as a geopolitical concern.

• For OEMs, Privacy represents Cost, Liability, and Business Risk for connected car revenues.
• Connected car services require more (personal) data than the car can provide
  • Where is the car going? For what purpose?
  • Who is in the car?
  • How can we use biometric data to deliver better experiences (ie. keyless)?
  • How can we access medical data to provide safer post-crash care experiences?

• Collecting **personal data from multiple people**: car owner, drivers and passengers

• **Legal paradox**: Individuals buy and own cars, but the OEMs still “own” and “monetize” the data generated by the cars
“Handling of consent involves vehicle and cloud architectural subsystems that is out of scope in VISSv2. However, a VISSv2 vehicle server has a capability to enforce consent results, i.e. to allow or block access to requested data. This can be leveraged in a model where the server receives consent results from an ECF and uses that information to either grant client requests, or not, for data that is consent protected. How the ECF obtains the consent status is out-of-scope in this specification.”

“ECF (External Consent Framework). An agent that is responsible for inquiring a data owner about consent.”

The customer has not selected any of these parties to manage their personal data and privacy; consequently, trust is spread thin to the point of extinction.

NEED TO SHIFT FROM BUSINESS-CENTRIC TO CUSTOMER-CENTRIC TRUST
NEED TO SHIFT FROM BUSINESS-CENTRIC TO CUSTOMER-CENTRIC TRUST
A SYSTEMIC OPEN APPROACH TO BRIDGING THE TRUST GAP

DATA PRIVACY TRUSTED 3RD PARTIES
Intermediate delivery of personal data with consent of data owner

INDUSTRY BODY
Defining privacy layer and tech specs, ensuring interoperability and portability

CERTIFYING BODY
Gov. or industry body that certifies and oversees trusted 3rd party

OEM
“Our connected car services use an industry standard privacy layer to get consented data”

CUSTOMER
“I am selecting a trusted 3rd party to intermediate my consent and data sharing. I always have control of my data”
Unconsented Raw Data
- Non consented
- Non compliant
- Unverified, uncertain accuracy
- Incomplete

My <Trusted 3rd Party> Verified Identity
- All my consents
- All my data
- Vetted

Consented Enriched Data
- Informed consent backed
- Privacy compliant on mutual terms
- Always Accurate
- Enriched
- Real-time
- Cloud based service
TRUSTED 3rd PARTY AS SELECTED BY THE CUSTOMER

A CUSTOMER-CENTRIC APPROACH
Alice feels safe, respected, in control, and trusts her car’s privacy.

USER JOURNEY: ALICE ENTERS HER CAR AND USES TRUSTED THIRD PARTY

1. **Authentication**
   - Alice authenticates herself with her car.

2. **Privacy Settings**
   - Alice’s car shows her a list of trusted 3rd party privacy providers to select in her privacy settings. Every passenger gets to choose their preference for their privacy.

3. **Consent**
   - Alice sees a list of connected services that she has consented and subscribed to. She can change her privacy and consent preferences and consent at any time.

4. **Clean Telemetry**
   - Once Alice provides informed consent, the trusted 3rd party enriches and initiates a privacy clearance for the telemetry data feeds, which are delivered to the service provider.
To ensure the integrity of personal data management, it's essential to have a framework of independent oversight, akin to the principles in Common Criteria or EMVCo, which provides a structured approach to evaluating the security and trustworthiness of the 3rd parties.

- Identity Assurance
- Private Data
- Data Model
- SSO for streamlined sign-up and authentication
- Standardize Consent
- Privacy Levels for Fine Grained Pseudonymisation
- Data Privacy Integration

THE SOLUTION IS POSSIBLE: 360OFME LEADING BY EXAMPLE

https://github.com/w3c-cg/autoprivacy
https://wiki.covesa.global/display/WIK4/Privacy+and+Identity
BASIC PRINCIPLES: THE CONSENT POP-UP

360OFME’S CONSENT POP-UP

Privacy Levels
Fine-grained pseudonymisation

Policy Grading
Privacy policy analysis and grading
ROLES & RESPONSIBILITIES: AN ECOSYSTEM TEAMWORK

Data Delivery per Consent (Trusted 3rd Party)
Standard Specifications (Industry Body)
Oversight of Certification (Gov’t and/or Industry Body)

Personal Data Wallet Management (Trusted 3rd Party)
Registering Consent (Trusted 3rd Party)
Standard Specifications (Industry Body)
Certification of Trusted 3rd Party (Certifying Labs)
Oversight of Certification (Gov’t and/or Industry Body)

Customers & Consumer Protections Organisations
Gov’t Bodies & Officials

Contribution to Industry Bodies (OEMs, Tiers, Tech companies)
Certification of Compliance (OEMs, Tiers, Tech companies, Trusted 3rd Parties, Gov’t Bodies)
Defining Privacy Levels
Defining consent & privacy data model
Standard API for privacy enforcement on data operation by Trusted 3rd Party (VISS)

Join us in the W3C Automotive Privacy Principles group
Defining roles & mission of Trusted 3rd Party
Defining Privacy Policy grading principles & grades

CALL TO ACTION
Let’s connect and team-up to bridge the Trust Gap!

Philippe Le Berre
Chief Technology Officer

Philippe.leberre@360ofme.com
+41 79.726.1630