Driving Privacy Forward

Homomorphic Encryption and Oblivious AI in Smart Mobility

Privacy Awareness Week 2026 · Webinar slide deck

SHIELD — Automobility Cybersecurity Centre of Excellence, University of Windsor

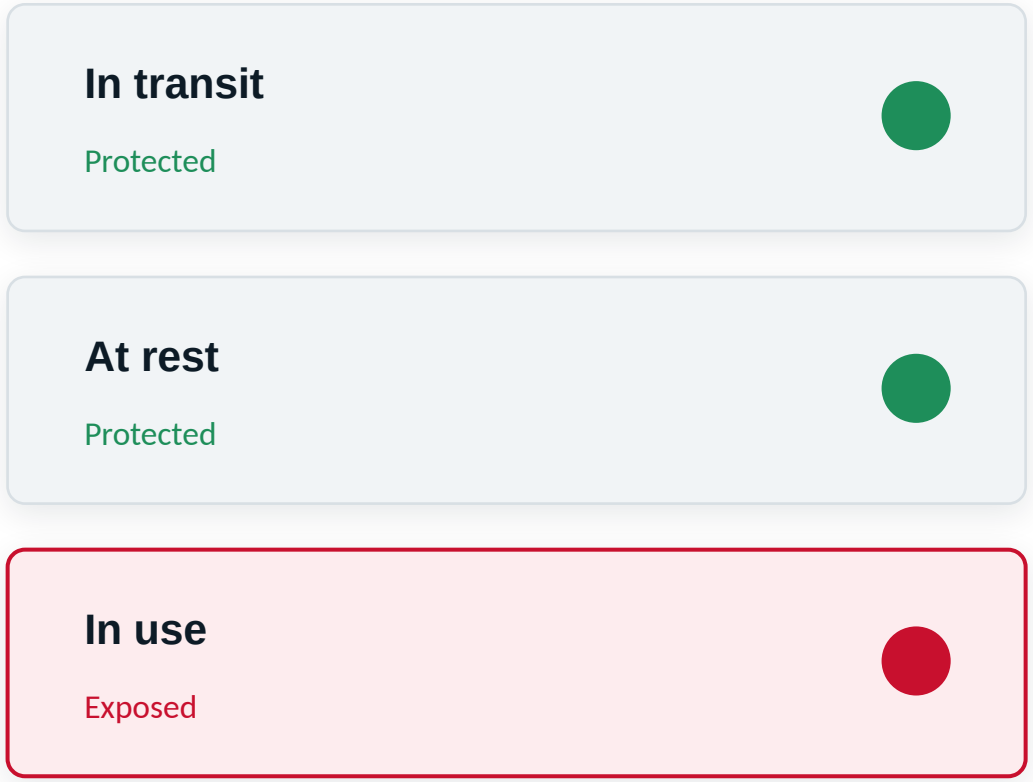
This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

The trust gap

Most privacy conversations stop at transmission and storage. The exposure happens somewhere else.

Data can be protected **in transit** and **at rest** — yet still be exposed at the moment it is **processed**.

Cloud analytics and AI services still rely on a decrypt-to-compute model, so raw or linkable telemetry can be visible inside service boundaries even when the channel is secure.



What today's vehicles share

Even many older vehicles are connected — and the data rarely stays in one place.

Location

Precise and repeated position, routes, travel patterns

Driving behaviour

Speed, braking, acceleration, usage profiles

Apps & infotainment

Accounts, media, phone pairing, in-cabin choices

In-cabin sensing

Occupancy and other cabin-derived attributes

Where it goes

Data may move across manufacturers, telematics providers, insurers, app providers, analytics platforms, cloud processors and dealerships.

Where privacy actually breaks

Risk does not come only from breaches or weak security.

1 Over-collection

Excessive collection, not data scarcity, was described as the central privacy problem.

2 Unclear downstream use

Once data leaves the vehicle, purpose and recipients become hard to trace.

3 Limited transparency

Long external policies do not tell people what is happening in the moment.

4 Exposure during processing

Raw data routinely revealed to the compute environment to produce a result.

The approach: compute without revealing

Homomorphic encryption and oblivious AI let analytics run on protected data.

Sensitive vehicle data is protected before it leaves the trusted edge domain. The cloud performs computation on the encrypted data and returns an encrypted result, which only the authorised party can open.

The goal was not to argue for privacy in principle, but to show that privacy-preserving computation can be engineered, tested and measured.

1

Encrypt at the edge

Data protected before it leaves the vehicle

2

Compute on ciphertext

Cloud never sees plaintext

3

Return encrypted result

Only the authorised party decrypts

What the demonstration showed

A bounded, service-oriented use case rather than a blanket claim.

Useful results

Cloud-based mobility analytics still produced a useful service outcome.

No routine raw exposure

The provider did not need to see raw personal data to deliver it.

Measurable cost

Performance and overhead were assessed, not assumed.

After the demonstration, participants became more receptive — the service scenario made the privacy-by-design logic easier to understand.

What stakeholders told us

Two interview rounds, before and after the demonstration.

1 Over-collection is the core problem

Excessive collection — not scarcity — was named repeatedly as the central concern.

2 Governance matters as much as technology

Encryption alone is not enough; trust needs minimization, roles, auditability and limits on reuse.

3 Privacy extends beyond the driver

Passengers, pedestrians and cyclists can be captured indirectly in public space.

4 Adoption needs bounded use cases

Implementation burden, standards alignment and clear value still gate uptake.

Best-practice guidance

Practical recommendations drawn from the build, the interviews and the demonstration.

Technical

Protect early in the lifecycle

Secure data before it leaves the trusted edge, not only once it is in the cloud.

Target by risk, not universally

Prioritise the flows where sensitivity and justification are strongest.

Co-design model and crypto pipeline

Encoding, model structure and evaluation should be built together, not retrofitted.

Operational

Pair the technology with governance

Key management, stewardship, auditability, roles and transparency still decide trust.

Make transparency layered

Just-in-time, role-specific notice at the vehicle and app interface.

Plan for the whole ecosystem

Accountability must span manufacturers, processors and downstream recipients.

Policy priorities

For PIPEDA modernization, CPPA-style reform and Transport Canada's connected-vehicle context.

1. Recognize mobility data as potentially high-sensitivity
2. Require privacy impact assessments for high-risk processing
3. Strengthen purpose limitation and restrict function creep
4. Create a practical mobility-data transfer right
5. Recognize privacy-enhancing technologies in guidance
6. Clarify de-identification and residual inference risk
7. Require layered, just-in-time transparency
8. Require accountable ecosystem governance

Three things to take away

1

Follow the data path

Privacy depends on the whole lifecycle, not the point of collection.

2

"Encrypted in transit" is not end-to-end privacy

Protection must hold while data is being used.

3

Privacy by design is actionable

It is a practical framework with concrete engineering steps.

Full report, policy brief and webinar recording: shieldautocybersecurity.com

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.