Driving Privacy Forward

Privacy-Preserving Connected Mobility and Regulatory Priorities for Canada

At a glance

- **The problem:** Connected vehicles generate continuous, inference-rich personal data. Current privacy controls do not fully address over-collection, secondary use, or exposure during cloud processing.
- **What this project found:** Useful analytics can be carried out without routine cloud access to raw personal data, but technical protection alone is not enough. Stakeholders consistently pointed to data minimization, transparency, and clear accountability as equally important.
- **Priority actions:** Recognize high-sensitivity mobility data, require impact assessments for high-risk processing, tighten purpose limitation and transparency, and build privacy requirements into connected-mobility pilots and procurement.

Why this matters

Connected-vehicle ecosystems are not simple one-to-one service relationships. Data may move across manufacturers, telematics providers, insurers, app providers, analytics platforms, cloud processors, dealerships, and third-party vendors. In that environment, privacy risk does not arise only from breach or weak security. It also arises from over-collection, unclear downstream use, limited transparency, and routine exposure of raw data during processing.

Key findings

- **Over-collection is the main privacy concern.** Across the interviews, stakeholders repeatedly described excessive data collection, not data scarcity, as the central privacy problem.
- **Useful analytics can be done with less raw-data exposure.** The project showed that some cloud-based mobility analytics can still deliver useful results without the service provider routinely seeing raw personal data.
- **Governance matters as much as technology.** Participants consistently emphasized that encryption alone is not enough. Trust depends on data minimization, clear roles, auditability, meaningful transparency, and limits on reuse.
- **Privacy impacts extend beyond drivers.** Connected-mobility governance should also account for passengers, pedestrians, cyclists, and others who may be captured indirectly in public space.

Recommendations for PIPEDA modernization and related CPPA-style reform

1. Recognize high-sensitivity mobility data: Mobility-related personal information should be expressly recognized in law or binding guidance as potentially high sensitivity where it reveals precise or repeated location, travel patterns, driving behaviour, household associations, in-cabin attributes, or persistent identifiers linked to a vehicle, device, or user account.

2. Require privacy impact assessments for high-risk mobility processing: Organizations should complete and retain a documented privacy impact assessment before deploying high-risk connected-vehicle processing, including continuous geolocation tracking, in-cabin sensing, insurance or eligibility profiling, AI-enabled inference, or large-scale sharing across entities.

3. Strengthen purpose limitation and restrict function creep: Data collected for safety, diagnostics, maintenance, navigation, cybersecurity, or other core functions should not later be repurposed for unrelated advertising, generalized commercial profiling, or third-party monetization unless a separate lawful basis and a clear necessity test are satisfied.

4. Create a practical mobility-data transfer right: Individuals should have a practical ability to direct secure transfer of their mobility-related personal information between service providers where this can be done safely and within a recognized interoperability framework.

5. Recognize privacy-enhancing technologies in compliance guidance: Canadian law or accompanying regulatory guidance should explicitly recognize strong encryption, privacy-preserving analytics, secure multiparty methods, and well-governed de-identification as valid ways to reduce unnecessary exposure of identifiable information.

6. Clarify de-identification, anonymization, and inference risk: Connected-vehicle data can remain re-identifiable even after direct identifiers are removed because route histories, timing patterns, device linkages, and behavioural traces may still reveal individuals. Privacy law should require a documented residual-risk assessment before such data is treated as sufficiently de-identified.

7. Require layered transparency at the vehicle and app interface: Transparency should not rely only on long external privacy policies. Organizations should provide layered, just-in-time, role-specific notices through the in-vehicle interface, companion app, onboarding flow, and user dashboard.

8. Require accountable ecosystem governance: Lead organizations should maintain a privacy management program proportionate to the sensitivity and volume of the data under their control, including documented roles and responsibilities across manufacturers, service providers, analytics partners, and downstream recipients, along with vendor oversight, retention schedules, incident handling, and technical safeguards.

Recommendations relevant to Transport Canada's connected and automated vehicle context

1. Treat privacy as part of safe and trustworthy connected-mobility deployment: Public trust in connected and automated mobility depends not only on safety performance and cybersecurity, but also on credible privacy governance.

2. Require a privacy case for high-risk pilots and demonstrations: Connected-mobility pilots that rely on high-risk mobility data should include a privacy impact assessment or equivalent privacy case as a condition of participation, especially where continuous location, behavioural scoring, in-cabin sensing, or multi-party sharing are involved.

3. Encourage privacy by design across the full data lifecycle: Guidance should encourage architectures that minimize collection, support local processing where feasible, reduce plaintext exposure during processing, limit retention, and clearly distinguish essential from optional data flows.

4. Build privacy into procurement, assurance, and third-party governance: Privacy requirements should be reflected in pilot programs, procurement language, evaluation criteria, and supplier oversight so that privacy-preserving approaches are not treated as stand-alone research concepts.

5. Address bystander and public-space privacy: Connected-mobility policy should not be framed only around the registered driver or vehicle owner. It should also account for passengers, pedestrians, cyclists, and others whose information may be captured indirectly in shared public space.

Near-term priorities

- Make mobility-data sensitivity and high-risk processing triggers more explicit in Canadian privacy guidance and reform discussions.
- Use privacy impact assessments, transparency requirements, and accountability expectations more consistently in connected-mobility pilots and procurements.
- Support bounded, higher-sensitivity pilot deployments where privacy-enhancing technologies can be tested alongside governance, performance, and public-trust requirements.

Closing note

Connected-mobility privacy cannot be addressed by notice, transport encryption, or downstream controls alone. It is a governance issue across the full data lifecycle. Canada should modernize privacy obligations for mobility data and encourage privacy-by-design deployment in higher-risk connected-mobility contexts, especially where sensitive data moves across multiple organizations and platforms.

Prepared by the project team based on the completed technical work, stakeholder interviews, and policy analysis conducted during the project period.