

Privacy Reform

ITS Australia Submission

September 2026



Privacy Amendment (Personal Data Protection) Bill 2026

Executive Summary

ITS Australia sincerely appreciates the opportunity to comment on the Australian Government's consultation on the proposed Privacy Amendment (Personal Data Protection) Bill 2026 and related reforms. ITS Australia is the peak body for the transport technology sector and many of our 140+ member organisations play a role at the leading edge of new and emerging technologies to improve safety and efficiency on our transport networks. Our members support strong, clear and technology-neutral privacy protections that build public confidence while allowing Australia to realise the substantial safety, mobility, productivity and sustainability benefits enabled by connected transport.

ITS Australia has reviewed the Consultation Paper and Exposure Draft legislation and understands its aims to modernise and strengthen Australia's privacy laws for the digital age. ITS Australia supports reforms to bolster privacy protections for Australians and help tackle emerging risks from new technologies, including artificial intelligence and wearable devices such as smart glasses, and appreciates the measures in the Exposure Draft Bill are designed to better protect Australians while supporting innovation and providing greater certainty for regulated entities.

This submission focuses on particular reference to connected vehicles and related emerging technologies. For the transport technology sector and vehicle manufacturers, the proposals may materially affect the collection, generation, sharing, retention and overseas processing of vehicle and mobility data. Particular impacts may arise for connected-vehicle telemetry, precise geolocation, driver and passenger identifiers, behavioural and safety inferences, sensor and camera data, diagnostics, software services, research datasets, and information exchanged across manufacturers, technology providers, fleet operators, infrastructure operators and government agencies.

Connected vehicles — including vehicles communicating with other vehicles, road infrastructure, fleet-management systems and digital transport services — depend on responsible data handling. The data involved may include vehicle status, safety-event information, road and traffic conditions, system

performance and, in some cases, information capable of identifying or tracking an individual. ITS Australia therefore supports an approach in which privacy is designed into systems from their earliest stages, rather than treated as a compliance exercise applied after deployment.

The consultation paper appropriately recognises that personal information can include behavioural, movement and other information where it relates to, or can reasonably identify, an individual. It also proposes to classify precise geolocation tracking data — location data accurate to within a 500-metre radius and held over time — as sensitive information. These changes are directly relevant to connected-vehicle services and reinforce the need for clear governance, minimisation and safeguards across the transport-data ecosystem

Key position

ITS Australia recommends that the Government:

- Retain the principles-based, technology-neutral framework proposed in the consultation paper.
- Recognise connected transport as a distinct public-interest application of data-enabled technology, where appropriately governed data sharing can prevent harm and improve the efficiency and resilience of the transport network.
- Encourage privacy-by-design and privacy-by-default practices across vehicle manufacturers, fleet operators, road managers, infrastructure operators, service providers, data platforms and researchers.
- Ensure that regulatory guidance distinguishes between identifiable personal data and properly de-identified, aggregated or operational data used for legitimate safety, network-management, research and productivity purposes.
- Avoid measures that unintentionally prevent timely, proportionate and secure data flows necessary for road-safety interventions, incident response, cooperative intelligent transport systems, freight optimisation and transport research.

- Develop practical sector-specific guidance in collaboration with transport agencies, industry, consumer representatives, privacy experts and the Office of the Australian Information Commissioner (OAIC).

Why connected-vehicle data matters

Connected vehicles can provide safety-relevant information in near real time, including warnings about hazards, incidents, roadworks, adverse weather, emergency vehicles, vulnerable road users and changing traffic conditions. Where carefully designed and deployed, these services can help drivers and automated systems make safer decisions before a conflict or crash occurs.

For example, a connected-vehicle system may receive a verified warning that a vehicle has braked heavily around a blind corner, that a crash has occurred beyond a crest, or that a road worker is operating ahead. The value of the system lies in providing a timely warning to other road users or in enabling road operators to manage the incident more effectively. In many cases, that outcome can be achieved with event-based, short-lived or aggregated data rather than persistent identification of an individual driver.

The potential benefits extend beyond individual safety

Outcome	Connected-vehicle contribution	Privacy design implication
Road safety	Hazard alerts, cooperative safety warnings, improved incident detection, work-zone protection and support for safer driving behaviour	Collect only the data necessary for the safety function; prefer event-based and pseudonymised identifiers where practicable
Freight productivity	Better route planning, reduced delays, more reliable travel times, safer heavy-vehicle operations and improved asset utilisation	Separate fleet operational data from directly identifiable driver information unless identification is necessary and justified

Outcome	Connected-vehicle contribution	Privacy design implication
Network efficiency	More responsive traffic management, congestion reduction, incident clearance and improved use of existing road capacity	Use aggregated or de-identified insights for network planning and operations wherever possible
Infrastructure maintenance	Earlier visibility of road-condition issues and more targeted maintenance activity	Establish clear retention periods, access controls and purpose limitations
Research and innovation	Evidence-based road-safety analysis, evaluation of new services and development of Australian transport technologies	Enable secure, ethically governed research pathways and rigorous re-identification-risk management

A privacy framework that enables these outcomes while maintaining strong safeguards is essential. The consultation paper's proposed fair-and-reasonable test, data-minimisation considerations, assessment of reasonable expectations, and proportionality assessment provide a sound basis for this approach. The paper makes clear that entities should consider whether an objective can be achieved with less personal information or with de-identified information, and that higher-risk handling requires stronger justification and safeguards.

The paper proposes that consent be voluntary, informed, current, specific and unambiguous. It also recognises that genuine choice is supported by accessible privacy settings, clear opt-out mechanisms and plainly identified optional fields. These principles should inform any connected-transport guidance.

ITS Australia supports the proposed controller–processor clarification, under which primary APP responsibility generally rests with the entity that determines the purposes for which personal information is handled, while processors act under documented instructions. This is particularly relevant to multi-party transport ecosystems, where technical data may move through several providers before it is converted into a safety alert, traffic-management insight or fleet service.

To support implementation, the sector would benefit from guidance on:

- Allocating controller and processor responsibilities in complex transport data chains.
- Managing joint or shared decision-making where public and private entities co-design a service.
- Applying privacy impact assessments to cooperative and connected transport deployments.
- Procuring technology and data services using consistent privacy, cybersecurity, interoperability and audit requirements.
- Establishing governance for secure data access by researchers and transport agencies and other approved parties.

Updated definitions and collection

ITS Australia supports modernised definitions that recognise personal information may comprise data relating to activities, movements, interactions and behaviour, rather than only names or formal identifiers. This is important because transport data may identify or single out an individual through linkage, even where a name is absent. The proposed definition of “reasonably identifiable” appropriately requires consideration of other reasonably available information, technical feasibility, time, cost, effort and controls that reduce re-identification risk.

However, guidance should make clear that not all vehicle-generated data are personal information in every circumstance. Properly designed datasets may be aggregated, de-identified or operationally limited so that they do not relate to an identified or reasonably identifiable individual. Clear guidance will help organisations invest in privacy-preserving technical design rather than unnecessarily retaining identifiable data.

The proposed expanded meaning of “collects” should also be accompanied by practical guidance on derived and inferred data. Connected-vehicle systems may generate insights from raw sensor, event or operational data. The compliance framework should encourage entities to minimise the creation and retention of identifiable inferences unless they are necessary for a legitimate, clearly stated purpose.

Precise geolocation

ITS Australia acknowledges the strong privacy interests associated with precise location tracking over time and supports appropriate protections. The proposed definition captures personal information identifying a person's specific location within 500 metres and held by reference to location over time.

Application of this measure should be carefully calibrated for transport. Certain connected-vehicle safety and operational functions require location and timing information to work effectively, including emergency warnings, incident management, road-user safety, navigation, freight logistics and infrastructure operations. The policy objective should be to ensure those data flows are necessary, proportionate, secure and transparent.

Fair and reasonable handling

ITS Australia supports the proposed fair-and-reasonable test as a flexible and durable foundation for emerging transport technologies. It is especially appropriate where connected services may create public benefits that extend beyond the individual user, such as preventing a collision, improving incident response or protecting road workers.

In applying the test, guidance should recognise that safety, network resilience and public-interest transport outcomes may be legitimate and significant benefits. These benefits should not displace individual rights; rather, they should be assessed alongside necessity, data minimisation, reasonable expectations, mitigation measures and the availability of less privacy-invasive alternatives.

The consultation paper's proportionality approach is useful: the more significant the potential impact on individuals, the stronger the justification and safeguards required. It also directs entities to consider whether the same result could be achieved through a less privacy-invasive approach. This is precisely the discipline that privacy by design should introduce into connected-vehicle systems.

Conclusion

ITS Australia supports privacy reforms that give Australians confidence that connected transport services will handle their information responsibly. Privacy and innovation are not competing objectives. Well-designed privacy protections are a precondition for community trust, adoption and the safe scaling of connected vehicles and cooperative intelligent transport systems.

The Government should retain a technology-neutral, risk-based framework; support privacy-by-design practices; and issue practical, transport-specific guidance that enables legitimate, proportionate and secure use of data for road safety, freight productivity, network efficiency, infrastructure management and research.

A mature privacy framework should prevent unjustified surveillance, profiling and misuse of personal information while enabling the carefully governed data sharing needed to reduce crashes, protect vulnerable road users and road workers, improve travel reliability, and unlock the productivity benefits of a connected transport system. ITS Australia wants to highlight the need for connected transport to be recognised as a distinct public-interest application of data-enabled technology and would appreciate the opportunity for practical sector-specific guidance to be developed in collaboration with the OAIC.

To facilitate any future engagement, ITS Australia Policy Manager Stacey Ryan can be contacted at Stacey.ryan@its-australia.com.au.

Yours sincerely,



Susan Harris
Chief Executive Officer

ITS Australia Members

Platinum



Gold



Silver

