



**FEDERAL
CHAMBER OF
AUTOMOTIVE
INDUSTRIES**

18 September 2026

Privacy Reform Team
Attorney-General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

Submitted via Have your say

Dear Privacy Reform Team,

I attach for your consideration a submission by the Federal Chamber of Automotive Industries (FCAI) responding to *Privacy Reform – Consultation on Exposure Draft legislation*.

The FCAI would be pleased to provide further information if that would be of assistance.

Yours sincerely

Dianne O'Hara
Director Industry Operations

FCAI submission in response to: Attorney-General's Department's Consultation Paper on Privacy Reform

1. Introduction

The Federal Chamber of Automotive Industries (FCAI) welcomes the opportunity to respond to the Attorney General's Department Consultation on Privacy Reform.

The FCAI is the peak Australian industry organisation representing over 60 global automotive brands that design, manufacture, import, distribute and sell light duty passenger vehicles, light commercial vehicles, and motorcycles in Australia. During 2025, FCAI members supplied more than 1.2 million new vehicles to the Australian market across more than 380 models. A full list of FCAI members is available at <https://www.fcai.com.au/about-fcai/member-manufacturers/>.

The FCAI brings its members together through various committees in compliance with the *Competition and Consumer Act 2010* (Cth) to consider the Australian legislative and regulatory environment, develop industry-wide perspectives and drive collective outcomes for the benefit of its members, the broader industry and Australian consumers.

2. Executive summary

The FCAI supports reform that gives individuals stronger privacy protections while providing regulated entities with clear, workable and internationally aligned obligations. The proposed framework should, however, recognise the distinct characteristics of connected vehicles and should not make consent the sole practical basis for safety-critical, security, diagnostic and vehicle-centred data handling. In the connected vehicle environment, these data flows are often necessary to maintain cyber security resilience, protect road users and increase public safety, support emergency response and preserve the safe operation of vehicles across their lifecycle.

- **Connected vehicle data.** The FCAI supports modernising the definition of personal information, but considers that the framework must distinguish personal information about an individual from vehicle-generated information that has continuing safety, security, maintenance, damage, efficiency and roadworthiness utility beyond a particular owner or driver.
- **Permitted general situation.** The FCAI recommends a specific permitted general situation for connected vehicles. This permitted general situation should authorise defined handling of connected vehicle data, as well as authorising necessary collection of precise geolocation tracking data where consent from every driver, passenger or other affected individual is impracticable, subject to appropriate controls such as transparency, data minimisation, and an opt-out where compatible with the relevant function.
- **Geolocation and consent.** The FCAI does not support a model under which unambiguous consent from every passenger or occasional driver becomes the only reliable basis for vehicle location functions. The current proposal is out of alignment with comparable international regimes, including EU and US privacy and data protection laws. The legislation should distinguish ongoing individual tracking from one-off or transient location events and should accommodate navigation, emergency response, theft recovery, roadside assistance, safety, security, diagnostics, fleet operations and subscribed connected services.
- **International alignment.** The FCAI strongly supports outcomes that align with leading overseas privacy regimes that apply to major international vehicle markets and avoid Australia-specific product design requirements. The Australian new vehicle market is a taker of technology from overseas vehicle manufacturers. Specific local requirements will delay or prevent Australian consumers from receiving connected features that are available in larger global automotive markets.
- **Fair and reasonable handling.** The FCAI supports a fair and reasonable test in principle, provided guidance confirms that safety, cyber security, recalls, diagnostics, warranty, roadworthiness and fraud

prevention are legitimate benefits and that an absence of consent or individual choice is not determinative.

- **Access, retention and erasure.** The FCAI supports meaningful individual rights, which must also allow proportionate access and continued retention of vehicle-centred information where reasonably necessary for safety, security, servicing, recalls, warranty, regulatory, second-hand sale and fraud-prevention purposes. Prior owners' identifiers, destinations, contacts and infotainment data should not follow the vehicle.
- **Large digital platforms.** The FCAI does not support a definition that can capture a global vehicle manufacturer merely because it operates websites or connected vehicle services and meets a whole-of-group revenue or end-user threshold. The proposed definition should be amended so that it is confined to the categories of consumer digital platforms at which the proposed erasure right is directed.
- **Data breach mitigation.** The FCAI supports prompt, risk-based steps that reduce harm following a data breach. Guidance should confirm that the duty to mitigate harm is limited to reasonable and proportionate steps within an entity's control and does not make entities insurers of all downstream loss.
- **Transition.** The FCAI recommends a transition period of a minimum of 24 months commencing only after the legislation, regulations and material regulatory guidance have been finalised, with separate staged arrangements for legacy and embedded systems. This would allow changes and expectations to be assessed and understood, while allowing changes to platforms to be designed, tested and security validated to have the minimum desirable impact on vehicle safety, cyber resilience, and connected vehicle features.
- **Legacy vehicles and data.** The FCAI does not support the unqualified application of new definitions and personal information lifecycle obligations to legacy vehicles, archived datasets and products whose design has been completed. A prospective, staged or reasonable-steps approach is required.

3. Commentary on specific measures proposed

3.1 Particular nature of connected vehicles and connected vehicle data

While connected vehicles are consumer-grade smart technology like many modern technological devices, they fulfil a broader function, having impacts that go beyond a specific consumer or household. Connected vehicles generate and use information across integrated vehicle, mobile application, dealer, repair, roadside assistance, supplier and manufacturer systems. Some of that information relates directly to an individual. Other information is principally about the condition, operation or history of the vehicle, even though an individual may be identifiable from the surrounding context.

The distinction is important because vehicle-centred information remains useful after a vehicle changes owner or driver and cannot always be de-identified, as new owners may know the identity of the immediately previous owner. Safety, security, emergency, service, maintenance, accident and damage history, odometer, fuel or energy efficiency, roadworthiness and diagnostic records may be needed by manufacturers, distributors and other participants in the vehicle ecosystem. Removing or rendering that information inaccessible merely because it was generated during an identifiable former owner's use may reduce safety, obscure vehicle history and impair maintenance, recall and fraud-prevention functions.

The FCAI therefore recommends recognition of a defined category of *connected vehicle data*. The category should be confined to vehicle-centred information with continuing utility and should exclude prior owners' or users' direct identifiers, destinations, contacts, communications and infotainment content. Where practicable, identity should be de-linked from this useful vehicle history rather than the history itself being destroyed.

FCAI recommendation: The legislation should define and recognise *connected vehicle data* as vehicle-centred information with continuing utility, while excluding prior users' direct identifiers, destinations, contacts, communications and infotainment content.

3.2 Precise geolocation tracking data and consent

The proposed definition of precise geolocation tracking data would capture device-generated or derived personal information that identifies an individual's location within 500 metres and is collected and held by reference to the individual's location over time. Because that information would be sensitive information under the proposed new definitions, its collection would ordinarily require unambiguous consent, even if it otherwise meets the fair and reasonable test and associated considerations.

That approach creates particular difficulty for connected vehicles. A manufacturer or service provider commonly has a relationship with the purchaser, registered user or account holder, not every occasional driver or passenger. Rental, fleet, leased, shared, loan and borrowed vehicles, along with the operation of the commercial passenger vehicle (CPV) industry, make individual consent for all cases impracticable. Vehicle systems may also be unable to distinguish a passenger from a driver or determine whether a particular person has previously given a current, specific and (under the new definition) unambiguous consent. Guidance should clarify that it is reasonable to rely on the purchaser, registered user or account holder to obtain relevant consents, where obtaining consent is practicable; in many cases it may not be. Care should also be taken to ensure that any consent requirements for tracking the location of vehicles under privacy law are not inconsistent with the requirements under State and Territory based legislation, such as section 8 of the *Surveillance Devices Act 1999* (Vic) and the *Workplace Privacy Act 2011* (ACT).

This proposed treatment is more restrictive than comparable overseas regimes. Under the European Union General Data Protection Regulation (GDPR), by contrast, location data is not a special category and may be processed under Article 6(1)(f) legitimate interests (including safety, security and fraud-prevention purposes) or Article 6(1)(b) contractual necessity.

Location information supports navigation, SOS calling and emergency response, theft recovery, roadside assistance, charging, diagnostics, warranty analysis, safety, cyber resilience, security and subscribed connected services such as GPS navigation and "find my car" features. These functions can be integral to rapid incident response, resilience against malicious interference with vehicle systems, the detection of unsafe conditions and the protection of drivers, passengers, and other road users. Requiring repeated start-up consents risks driver distraction and "consent fatigue". It could also make beneficial or safety-related functionality contingent on the actions of people who do not own or control the vehicle.

The FCAI recommends that Australia ensure that consent is not the sole practical basis for handling such information. Accordingly the FCAI has proposed at section 3.3 of this submission an exception by way of an additional 'permitted general situation' to be included in the *Privacy Act 1988* (Cth) (Privacy Act) to address these considerations.

The proposed paragraph (c) of the section 6(1) definition of precise geolocation tracking data, which extends collection and holding "over time" to location "identified at points in time, by reference to an aggregation of information or in any other way", creates particular uncertainty, because it is capable of capturing multiple isolated location events. While the consultation paper states (at page 6) that the definition is not intended to extend to "one-off disclosures of location information", that statement addresses only single events and does not resolve the treatment of multiple isolated or transient events that are not assembled into a longitudinal record.

The FCAI recommends that the expression "over time" should also be clarified in the statutory text of the section 6(1) definition, so that a single location event, or multiple isolated events that are not assembled or held as a longitudinal record of an individual's movements, should not amount to tracking over time.

Transient or on-board processing should also be treated differently from centralised retention of a location history.

FCAI recommendation: Recognise a new permitted general situation in the connected vehicle context as set out further in this submission. In addition, amend the proposed definition so that the reference to geolocation data collected “over time” requires a longitudinal record capable of tracking, monitoring or analysing an individual’s movements, and does not include isolated location events or transient on-board processing that is not retained as such a record.

3.3 A connected vehicle permitted general situation

The exceptions in proposed Australian Privacy Principle (APP) 4.3 are not sufficient for the connected vehicle context. The ‘strictly necessary’ exception in APPs 4.3(d) and 4.4 depends on goods or services requested by the individual whose personal information is being processed. That formulation may assist a registered user who is at least 18 and who has deliberately subscribed to a connected service, but it does not resolve collection relating to drivers who are under 18 where the feature is not ‘strictly necessary’ for the limited purposes set out in the proposed APP 4.4(b), or for passengers, occasional drivers, fleet users, future owners or automatic safety and security functions. Nor does it provide a stable basis for retaining and disclosing useful vehicle history or for handling associated information when a vehicle is transferred.

The FCAI recommends that section 16A of the Privacy Act be expanded to include a specific permitted general situation for connected vehicles. The public interest basis for the exception is that connected vehicle data handling provides public utility even where vehicle owners may be reasonably identifiable, including as necessary to preserve cyber resilience, support emergency and roadside response, detect and remediate safety defects, maintain roadworthiness, and protect drivers, passengers and other road users. Locating the exception in legislation, rather than relying only on guidance that may change from time to time, would provide an authoritative and clear basis for its operation. Constructing it as a permitted general situation would also operate coherently across the proposed fair and reasonable requirement, consent to collect sensitive information, consent to trade personal information and the erasure right, each of which will recognise the permitted general situations set out in section 16A of the Privacy Act.

This new permitted general situation should apply to APP entities that include vehicle manufacturers, distributors and dealers. It should permit collection, use, disclosure including trading, retention and de-linking of *connected vehicle data* (and associated personal information, to the extent appropriate to the relevant function) where reasonably necessary for vehicle safety, security, cyber security, emergency response, crime prevention or detection, servicing, maintenance, recalls, roadworthiness, accident or damage history, odometer verification, energy or fuel efficiency, warranty, regulatory compliance, mobility services, second-hand sale, transfer of vehicle history, product safety investigations, dispute management, the safe development and operation of automated driving functions, or trip history kept for the safe and efficient administration of CPV and fleet services and vehicles.

The same exception should be capable of justifying continued retention of *connected vehicle data*, including information that may still be personal information because it remains associated with a vehicle or VIN, where the information is retained for defined vehicle-centred purposes and prior users’ direct identifiers, destinations, contacts, communications and infotainment content are removed or de-linked. A particular benefit of having this *connected vehicle data* set out in its own exception (as a permitted general situation) will be clarity and certainty across the industry that this data which has public utility can be collected and processed, and be available to manufacturers, distributors, dealers and future owners as permitted, without leaving it dependent on regulatory interpretation through an entity by entity application of a ‘fair and reasonable’ test. As a permitted general situation it would also support retention (under APP 11), recognising the utility of long-term, purpose-based vehicle-centred data.

This new permitted general situation should also separately permit collection of precise geolocation tracking data without the consent of every driver and passenger, where reasonably necessary for those purposes or for navigation and subscribed connected services. Consent should not be the sole practical basis for this. Safeguards in the exception should include clear transparency through privacy policies and vehicle or service materials, data minimisation, access controls, on-board processing where reasonably practicable, and an accessible opt-out where disabling the collection is compatible with safety, security, emergency, legal, audit, fleet management and requested service functions.

These concerns are not currently reflected in any other permitted general situation in section 16A of the Privacy Act. A statutory exception of the kind proposed is the international norm: United States State privacy laws (for example, Virginia, Colorado and Connecticut) contain enumerated processing exceptions permitting controllers to process personal data to provide a requested product or service, to prevent and investigate security incidents and fraud, to protect the life and physical safety of individuals, to comply with legal obligations, and to conduct internal product-improvement research; and the GDPR achieves the same result through its legitimate-interests, contractual-necessity, legal-obligation and vital-interests bases.

Locating the connected vehicle exception in section 16A would support these issues by giving it automatic effect as an exception to the fair and reasonable test (proposed APP 3.3), to consent for the collection of sensitive information (proposed APP 4.3), to consent to trade personal information (proposed APP 4.6), to the ability to retain *connected vehicle data* (proposed APP 11.2), and to the erasure right (proposed APP 14.3(a)).

FCAI recommendation: Insert a new, specific connected vehicle permitted general situation in section 16A, with defined purposes and safeguards, that applies across APPs 3, 4, 11 and 14. Guidance should also confirm that provision of a connected service deliberately subscribed to by a user can satisfy proposed APPs 4.3(d) and 4.4.

3.4 Fair and reasonable handling

The FCAI supports a single fair and reasonable test in principle. Its operation should not, however, treat the absence of consent, an opt-out or an alternative service as fatal. The proposed factors require a holistic assessment, and connected vehicle functions often deliver substantial benefits even where it is not practical for a person to meaningfully choose whether a minimum data flow occurs.

Guidance should include connected vehicle examples. It should recognise safety, cyber security, theft prevention, emergency response, recalls, diagnostics, maintenance, warranty, roadworthiness and fraud prevention as legitimate benefits. It should also explain how reasonable expectations, transparency, minimisation and proportionality apply where disabling a data flow would impair safety, security, compliance or a requested connected function.

FCAI recommendation: Include detailed connected vehicle examples in Office of the Australian Information Commissioner (OAIC) guidance and confirm that limited or absent individual choice does not, by itself, prevent handling from being fair and reasonable.

3.5 Alignment with leading global markets

Vehicles supplied in Australia are overwhelmingly developed through global product programs. Hardware, embedded software, telematics platforms, supplier arrangements, cloud architecture and release governance for global vehicle platforms are commonly designed and deployed on multi-year development cycles, for multiple jurisdictions, well before an Australian model launch.

The FCAI strongly opposes privacy and data protection requirements that are inconsistent and more onerous for Australia than those applying in leading international vehicle markets. Australia-specific vehicle interface, consent or architecture requirements are generally not achievable through a specific local software change and need to be considered or applied on a global product development lifecycle basis. The commercial response to an incompatible Australia-specific requirement may be to delay a model, disable a connected feature or not offer it in Australia, reducing the public benefits available to Australian consumers and road users. That outcome would reduce consumer choice and may withhold, delay or fragment the implementation of technologies that improve security and cyber resilience, safety, mobility, productivity or convenience.

A practical middle ground can include layered notice, account-holder controls, vehicle-level indicators and opt-out settings where these are safe and technically feasible. The framework should allow equivalent outcomes rather than mandate an Australia-specific single interface or consent design.

FCAI recommendation: Ensure legislation and guidance are internationally interoperable, and avoid Australia-specific design mandates. In particular, specific and unambiguous consent for geographic location tracking of a connected vehicle from every occasional passenger should not be required without appropriate legislated exceptions.

3.6 APP 11 retention, destruction and de-identification

The FCAI supports effective data lifecycle management. In the connected vehicle context, the question whether information that is *connected vehicle data* is “no longer needed” must account for long-lived vehicle-centred purposes and should be assessed consistently with the proposed definition of *connected vehicle data* and the connected vehicle permitted general situation recommended at sections 3.1 and 3.3 above. Vehicle history may be required for resale, recalls, safety investigations, servicing, warranty, disputes, regulatory compliance, roadworthiness and fraud prevention long after the event that generated it.

The proposed broadened definitions of ‘personal information’ and ‘de-identified information’ may make some *connected vehicle data* difficult to treat as fully anonymous, particularly where information remains linked to a vehicle, VIN, component, service history or safety event and may be capable of being associated with a past, current or future user in context. It is not sufficient to assume that useful vehicle history can always be destroyed or fully de-identified or anonymised without loss of function.

Guidance should recognise de-linking identity as a practical control. Safety, service and vehicle-condition history may follow the vehicle, while prior owners’ identifiers, destinations, contacts and infotainment information should not. Where information falls within the proposed *connected vehicle data* definition and is retained for one of the defined purposes in the new permitted general situation the FCAI has proposed, APP 11 read together with the permitted general situation would permit retention of defined *connected vehicle data* for the recognised vehicle-centred purposes and not require destruction merely because the original transaction, trip or ownership period has ended. Guidance should also address immutable safety logs, encrypted backups and evidence required for product safety investigations.

Permitting long-term, purpose-based retention of vehicle-centred data is consistent with overseas law. The GDPR measures storage limitation against the purpose of processing (Article 5(1)(e)) and expressly permits extended retention for archiving and research; United States State deletion rights and the California Consumer Privacy Act 2018 (CCPA) deletion right are each subject to enumerated exceptions permitting retention to complete a transaction, provide a requested service, detect security incidents, comply with legal obligations, and establish or defend legal claims.

FCAI recommendation: Confirm that APP 11 permits legitimate long-term retention of defined *connected vehicle data* where reasonably necessary for a connected vehicle permitted general situation, and provide connected vehicle related guidance on de-linking, de-identification, immutable logs, backups and safety evidence.

3.7 Access rights and the proposed 'technical infeasibility' exception

The FCAI supports the proposed recognition that access may remain unreasonable or impracticable because of 'technical impossibility or infeasibility' after reasonable steps have been taken. The exception is important for raw telemetry, embedded systems, event logs, encrypted backups, sensor streams and systems, including where they may be indexed by vehicle rather than individual. Unauthorised access to this data may reveal cyber security controls, safety logic, information about multiple users, or proprietary information. In those contexts, a right to access should be assessed by reference to whether disclosure would protect the individual's privacy interest without undermining vehicle safety, cyber resilience, third-party privacy or system integrity.

However, there also needs to be recognition that there may be circumstances, particularly in the context of *connected vehicle data* (even where still able to be linked to an individual), where no reasonable steps should be taken. For example, where material responsive to an access request may cover mixed data about multiple drivers or passengers, proprietary diagnostics, trade secrets, or material that could expose cyber security or safety controls. Further, if it is possible to do so, proportionate extraction and redaction costs should be recognised. Summaries, visualisations, or partial access may provide an appropriate outcome where raw data would prejudice security, safety, third-party privacy or intellectual property.

These limitations would be consistent with overseas access frameworks. GDPR provides that the right to obtain a copy must not adversely affect the rights and freedoms of others (Article 15(4)) and protects trade secrets and intellectual property (Recital 63); United States laws permit businesses to withhold information whose disclosure would compromise security or reveal another individual's personal data or trade secrets. The FCAI's recommendation that it be clear no steps need be taken where access would expose mixed-user data, proprietary diagnostics, or safety and security controls is consistent with established international practice.

FCAI recommendation: Ensure the new exception to providing access also recognises that it may not be reasonable to take any such steps. Provide practical access guidance for telemetry, embedded systems, event logs, mixed-user data, encrypted backups and sensor streams, including when summaries or partial access are appropriate.

3.8 Trading and transfer of connected vehicle data

The new proposed definition of 'trade' may create uncertainty where a second-hand connected vehicle is sold and vehicle-specific information or associated vehicle history passes with it. Some information may remain capable of being connected with a previous owner even after obvious identifiers are removed because, for example, the new owner may know the identity of a prior owner. The transaction and provision of associated *connected vehicle data* should not become a prohibited trade merely because useful vehicle information is inseparable from the vehicle or its systems.

The connected vehicle permitted general situation proposed at section 3.3 above should address and permit disclosures and transfers that are reasonably necessary for sale, servicing, security and cyber resilience, repair, recalls, warranty, roadworthiness and safety. It should not authorise the transfer of prior

owners' direct identifiers, destinations, contacts, communications or infotainment content except where another lawful basis applies.

Comparable overseas regimes do not prohibit the transfer of vehicle history incidental to a genuine sale. Under the GDPR such a disclosure can rest on legitimate interests or contract, and United States law regulates the "sale" of personal information through an opt-out right subject to transactional and service-provider exceptions rather than a prohibition. The carve-outs to the definition of trade in proposed section 6FC(2) do not resolve the second-hand vehicle case: the carve-out in section 6FC(2)(a) applies only where the disclosure is to enable the recipient to provide a product or service to the individual to whom the information relates, whereas connected vehicle data passing with a resold vehicle relates to the prior owner, not the purchaser; and the business-transfer carve-out in section 6FC(2)(b) is directed at mergers and acquisitions, not consumer resales. The FCAI's recommendation should accordingly be given effect through the proposed connected vehicle permitted general situation and, if necessary, a specific carve-out in section 6FC(2).

FCAI recommendation: Clarify that the sale or servicing of a connected vehicle does not constitute prohibited trading without consent merely because defined *connected vehicle data* transfers with, or remains associated with, the vehicle. This should form part of the express permitted activity under the permitted general situation proposed at section 3.3 above.

3.9 Right to erasure and large digital platforms

The FCAI supports targeted rights that respond to the privacy risks of large consumer digital platforms. The proposed definition of 'large digital platform' is, however, overly broad because it draws on the *Online Safety Act 2021* (Cth) categories of social media service, relevant electronic service and designated internet service, and applies a whole-of-business-group revenue and end-user test to every entity in those categories. In particular, a designated internet service is defined to include any service that allows end users to access material using an internet carriage service, or a service that delivers material to users via an internet carriage service.

A global vehicle manufacturer may operate Australian websites, owner portals, mobile applications and connected services platforms and exceed either the group revenue or end-user thresholds. It should not become a large digital platform merely for providing digital services incidental to the manufacture, distribution, sale, operation or servicing of connected vehicles. That result would extend the erasure right beyond the social media, messaging, email, gaming, streaming and comparable online platform context described in the consultation paper.

The FCAI recommends narrowing the section 6EB definition so it does not capture manufacturers merely for providing websites, applications or connected vehicle services. Alternatively, if vehicle manufacturers remain intentionally within scope, the erasure exceptions in proposed APP 14.3 must include a connected vehicle exception to preserve defined *connected vehicle data* with continuing safety, security, service, recall, roadworthiness, warranty, regulatory and second-hand market utility. Recognising an exception for 'technical infeasibility' alone is too narrow. Information may be technically capable of deletion but should be retained because deletion would impair legitimate vehicle-centred purposes or the interests of future owners and road users, among others.

FCAI recommendation: Narrow the definition of 'large digital platform' so it does not capture vehicle manufacturers merely because they provide websites, applications or connected vehicle services. Alternatively, add an express connected vehicle exception to the new APP 14.

3.10 Data breach mitigation

The FCAI supports prompt, risk-based action to prevent or reduce harm following an actual or suspected data breach. The proposed obligation to mitigate harm arising from a data breach must be accompanied by clear guidance on its scope and endpoint, particularly for incidents spanning manufacturers, distributors, dealers, suppliers, overseas engineering teams and multiple legal regimes.

Reasonable steps should be assessed by reference to actual risk, individual preferences, technical feasibility, causation, proportionality and matters within the entity's control. The obligation should not make an entity an insurer of downstream loss. It should not ordinarily require an entity to replace identity documents, contact every issuing authority, provide indefinite monitoring or impose remediation that an affected individual does not want.

This proportionate approach reflects overseas law. The GDPR (Articles 33 and 34) likewise calibrates breach obligations to reasonableness rather than guaranteed outcomes, and various United States state-based breach-notification laws require timely notice and, for defined breach types, limited monitoring, without making the entity responsible for all consequential harm.

FCAI recommendation: Issue clear guidance confirming that the "reasonable steps" standard for breach mitigation under s 26WDA is assessed by reference to reasonable and proportionate steps within the entity's control, actual risk, technical feasibility, and causation, and does not impose strict liability for downstream loss.

3.11 Commencement, transition and guidance

The reforms, including new specific consent requirements, broader inclusion of data in the definition of 'personal information', new overarching 'fair and reasonable' test replacing the former primary/secondary purpose tests, as well as the express obligation to record data inventories, could require substantial work across data inventories, classifications, notices, consent mechanisms, contracts, processor arrangements, access processes, retention rules, vehicle interfaces and incident response. For global vehicle programs, changes will also require coordination with overseas headquarters, software teams, suppliers and technology providers, and will need to be integrated into fixed product development cycles.

The FCAI recommends a transition period of a minimum of 24 months, having regard to transition periods for equivalent major privacy reforms (such as 24 months for the initial implementation of GDPR in the EU, 24 months for the automated decision making and Children's Online Privacy Code amendments in Australia, and 15 months for the previous significant changes to the Privacy Act in Australia). In addition to updating manufacturer information handling processes, that time period would help enable secure, tested and safer implementation to technologies used everyday by the public, rather than rushed changes to live or embedded systems.

Critically, the period should commence only when the legislation, regulations and material OAIC guidance are final and available. Experience under European frameworks suggests that organisations benefit from clear examples, safe harbours, and implementation guidance, particularly for product improvement, vehicle quality monitoring, diagnostics, cyber security, fraud prevention, and safety-related processing. Guidance should be published early enough to permit systems design, safety assessment and testing, cyber security validation, localisation, supplier implementation and consumer communications to be deployed at scale before obligations commence. A transition period that runs while critical guidance remains unsettled does not provide regulated entities with a meaningful implementation period.

Separate arrangements should apply to legacy vehicles, embedded systems, archived information and vehicles whose design or production decisions have already been finalised, as outlined at section 3.12 below.

FCAI recommendation: Provide a minimum of 24 months from finalisation of the legislation, regulations and material OAIC guidance, with separate arrangements for legacy vehicles, embedded systems and committed product programs.

3.12 Existing and legacy vehicles, systems and data

The exposure draft legislation would apply several amended definitions and handling obligations to information held after commencement of the amendments, even where the information was acquired or created earlier. The amended core definitions apply to information held on or after commencement “whether the information was acquired or created before, on or after that commencement” (Schedule 1, item 13(2)); the handling obligations in Schedule 2 apply on the same retrospective basis (Schedule 2, Part 1, item 13); proposed APP 11 applies to information held on or after commencement regardless of when it was acquired or created (Schedule 3, Part 2, item 23); and proposed APP 14 applies regardless of whether the organisation became a large digital platform, or the information was created, before or after commencement (Schedule 4, Part 2, item 12). The draft legislation contains no reasonable-steps safe harbour for legacy vehicles or embedded systems that cannot be re-engineered.

For connected vehicle businesses, this may require retrospective identification, reclassification, segregation and control across sold vehicles, unsupported embedded systems, dealer systems, warehouses, archives, backups and overseas platforms. Some vehicles and legacy vehicle architectures may not be capable of supporting new consent, deletion, segregation or data management requirements without substantial redesign, and some cannot be materially updated ‘over the air’. Historic datasets may not contain reliable information about the relevant driver, notice, purpose or consent status. Re-engineering legacy vehicle systems or datasets can involve significant technical complexity, cost, and timing constraints, and may be technically impossible, disproportionate or unsafe, including where changes could weaken existing cyber security controls, impair safety functions, corrupt vehicle-history records or remove data needed for recalls, servicing, product safety investigations or incident response. Vehicles already in production or on the way to Australia may also have passed the point at which hardware, software or telecommunications arrangements can reasonably and safely be changed specifically for the Australian market.

The FCAI recommends prospective-only, or staged, application for sold vehicles, legacy platforms, archived diagnostics and unsupported systems. At minimum, there should be a reasonable-steps safe harbour for situations where compliance would require re-engineering that is impossible, disproportionate or unsafe, or that could introduce unacceptable security risks or vulnerabilities. Ongoing uses of legacy information should remain subject to the appropriate privacy safeguards in place at the time of collection. New proposed uses of legacy information could be subject to the new requirements and overarching fair and reasonable tests.

Prospective application with grandfathering of legacy systems is the international norm, and the draft legislation’s application provisions noted above make a safe harbour especially important. The FCAI recommends that prospective-only or staged application, supported by a reasonable-steps safe harbour for technically impossible, disproportionate or unsafe re-engineering, or where this could introduce unacceptable security risks or vulnerabilities, be added to these application provisions.

FCAI recommendation: Adopt prospective-only, or staged, application provisions for legacy vehicles and data, supported by a reasonable-steps safe harbour for technically impossible, disproportionate or unsafe re-engineering, and re-engineering that could introduce unacceptable security risks.

4. Conclusion

The FCAI supports privacy reform that strengthens protection for individuals and gives regulated entities clear, workable and internationally aligned obligations. To achieve those objectives in the connected vehicle context, the framework must distinguish vehicle-centred information that retains legitimate utility across the life of a vehicle, even if that information can also be associated with an identifiable former owner.

The FCAI's central request is for a specific connected vehicle permitted general situation, supported by clear definitions and safeguards. That exception should provide an authoritative basis for proportionate handling of *connected vehicle data* and precise geolocation tracking data for safety, security, emergency, servicing, maintenance, recall, roadworthiness, fleet, subscribed service and related vehicle purposes where consent from every affected individual is impracticable.

The FCAI also requests that the Government:

- clarify that isolated or transient location events are not collection and holding by reference to an individual's location "over time";
- provide specific connected vehicle examples in guidance related to the fair and reasonable test and consent exceptions;
- recognise long-term vehicle-centred retention, proportionate access and de-linking of identity from useful vehicle history (*connected vehicle data*);
- ensure the trading and erasure provisions do not disrupt the sale, servicing, safety or continuing utility of connected vehicles;
- narrow the large digital platform definition so that it does not inadvertently capture vehicle manufacturers and connected vehicle services;
- clarify the proportionate scope of the data breach mitigation obligation;
- provide a transition period of a minimum of 24 months from finalisation of the legislation, regulations and material OAIC guidance, with staged arrangements where required; and
- adopt prospective, staged or reasonable-steps and safe harbour arrangements for legacy vehicles, data and embedded systems.

These changes would preserve meaningful privacy safeguards while supporting safety, consumer choice, international alignment and the continued availability of connected vehicle technologies in Australia.