FCAI Submission to Attorney-General's Department Issues Paper - Privacy Act Review

December 2020

Federal Chamber of Automotive Industries
Level 1, 59 Wentworth Avenue
KINGSTON ACT 2604

Contact: [redacted]
Phone: [redacted]
Facsimile: [redacted]

EXECUTIVE SUMMARY

The Federal Chamber of Automotive Industries **(FCAI)** is the peak industry organisation representing most of the vehicle manufacturers and importers of passenger vehicles, light commercial vehicles and motorcycles in Australia.

FCAI member organisations represent 68 brands offering 380 different vehicle models, sold and serviced by almost 4,000 authorised dealers. Together, Australian new vehicle distributors and their authorised dealers employ more than 75,000 employees and contribute significantly to Australia's economy, lifestyle and communities big and small[1].

FCAI welcomes the opportunity to make a submission to the Attorney-General's Department Issues Paper linked to its review of the Privacy Act (the **Issues Paper**).

FCAI members recognise the aims of the Privacy Act (the **Act**) and have invested, and will continue to invest, substantial resources on ensuring their ongoing compliance with its obligations.

FCAI believes that the Act currently strikes an effective balance between supporting appropriate protection of individuals' personal information in line with community expectations and encouraging the development of innovative products and services that support consumers needs without the addition of unnecessarily prescriptive and burdensome regulation.

As is the case in all sectors of the Australian economy, rapid technological advances are transforming the automotive products and services that are able to be offered to Australian consumers. The introduction of "connected" vehicles (and the future introduction of autonomous vehicles) to the Australian market relies on the collection, storage, use and transfer of the vehicle-generated data and user-introduced data described further in our submission to deliver significant benefits to individual consumers and to the broader Australian community.

FCAI strongly believes that any changes proposed to the Act to reflect the rapidly changing technological environment must be practical and continue to strike an appropriate balance between protection of individuals' personal information and encouragement of innovation. Care should also be taken to ensure that any terminology used is not too specific or technical and therefore subject to becoming outdated as technology continues to evolve.

As a result, the focus of this submission is on the areas of the Issues Paper, and the Act, which have particular application to the operation of connected and autonomous vehicles in the Australian market.

As an additional matter, FCAI notes that the Issues Paper has been produced in response to recommendations made by the ACCC in its recent Digital Platforms Inquiry – Final Report (the **DPI**

[1] FCAI website (fcai.com.au).

Report), and in particular the ability of current laws to respond to concerns about some behaviour of digital platform operators.

While the issues raised in the DPI Report about the operation of digital platforms are wide-ranging and require serious and practical consideration, care must be taken when determining the extent to which the ACCC recommendations made in relation to the Act are applicable outside the digital platforms environment. FCAI is particularly concerned to ensure any proposed changes to the Act are closely tailored to addressing the specific concerns raised in the DPI Report and do not have unintended and potentially far-reaching implications for broad sections of the Australian economy.

FCAI would welcome the opportunity to participate in any consultations which are held in relation to potential changes to the Act to help ensure that they are practical and effective and do not result in any unintended consequences to consumers or the business community.

INTRODUCTION AND BACKGROUND TO DATA USE IN CONNECTED VEHICLES

Complex and rapidly changing technology, including a plethora of products and services using digital platforms for delivery to consumers, now touches most aspects of everyday life in Australia. Access to data of different kinds, each requiring varying levels of security and protection, is required to unlock the significant consumer and community benefits these technologies are able to deliver.

Automotive products and services are at the forefront of some of these developments.

Vehicles available in Australia already generate and collect large amounts of technical information, described further below, for a range of purposes. In the past, this information was stored within various modules in the vehicle and could only be accessed through a physical connection between the vehicle and specialist diagnostic equipment.

Recently, however, vehicles are being launched in Australia with "connected" features in the sense that they can exchange information wirelessly with the vehicle manufacturer, third party service providers, users, infrastructure operators and other vehicles. These features can increase comfort and convenience for customers, improve automotive products and services and contribute to achieving societal goals such as improving road safety, reducing fuel consumption and vehicle emissions, as well as facilitating traffic management and parking[2].

Vehicles collect and process data relating to the vehicle itself and its surroundings. Some of this data may be regularly overwritten while other data may be stored for a certain period or aggregated for use in statistical form.

'**Vehicle-generated data**' in conventional and connected vehicles may relate to, but is not limited to:

- safety and security (e.g. Crash Event Data such as whether airbags have been triggered or whether doors and windows are locked or open, informing emergency services in the event of an accident when the driver is unable to do so);
- vehicle functionality status (e.g. engine injection, transmission behaviour, fuel level, battery charging level, Driver Assistance Systems, On-Board Diagnostic malfunctions);
- driving (e.g. fuel consumption, speed, use of brake and accelerator pedals, steering wheel movement, general vehicle operating parameters to inform predictive maintenance or repair);
- location of the vehicle: (e.g. navigation, advice about avoiding traffic jams and road hazards, access to "smart parking" information, providing locally relevant information, locating vehicles);
- surroundings (e.g. outside temperature, nearby vehicles or other objects);
- enabling remote vehicle operations: (e.g. remote engine start and climate control operation); and

[2] See FCAI Voluntary Code of Conduct – Automotive Data and Privacy Protection dated 8 December 2020 (effective on 1 July 2021). Available at fcai.com.au/news/codes-of-conduct.

- data that has been introduced by customers themselves. This '**user-introduced data**' may be collected and stored through certain features of the vehicle, including:
  - infotainment settings (e.g. preferred radio station);
  - convenience settings (e.g. seat & mirror positions);
  - navigation destinations; and
  - mobile phone address books.

FCAI members recognise consumers' rights to exercise choice and control over how their personal information is used as the technological environment evolves. They further recognise that retaining the trust of their customers is crucial to their ongoing relevance and success in the Australian market.

In recognition of the seriousness with which the industry takes these issues, the industry has recently launched a Voluntary Code of Conduct – Automotive Data and Privacy Protection[3] (the **FCAI Voluntary Code**) to demonstrate its commitment to transparency, choice and security when it comes to the management of vehicle-generated data and associated personal information.

The Voluntary Code requires members to ensure that their treatment of that data and information is driven by compliance with the following key principles:

1. We are open and transparent
2. We give customers choice
3. Privacy by design – we always take data protection into account
4. We maintain data security
5. We process personal information in a proportionate manner
6. We only share data responsibly, legally and driven by our customers' preferences

In particular, members acknowledge that vehicle-generated data and associated personal information may be used for:

- complying with legal obligations (for example: on-board diagnosis, consumer protection, recall and safety-related field monitoring, direction from law enforcement, courts, and regulators);
- providing vehicle support and services (e.g. repair and maintenance, roadside assistance, warranty, over the air updates, vehicle location and remote vehicle services);
- improving vehicle performance, quality, and safety (e.g. product development, accident research investigation);
- offering information and entertainment (e.g. communications, access to media, navigation, information about weather, traffic, and parking);

[3] Effective from 1 July 2021. Available at fcai.com.au/news/codes-of-practice.

- facilitating access to services (e.g. fleet management, pay-as-you drive insurance, trip logbook services which may enable business compliance with certain requirements such as Fringe Benefits Tax); and

- enabling vehicle-to-vehicle or vehicle-to-infrastructure communication (e.g. road hazard warnings, re-routing or traffic management).

The following sections of this submission provide FCAI's response to the areas of focus in the Issues Paper which have specific relevance to the automotive industry, with a particular focus on the operation of connected and autonomous vehicles.

OBJECTIVES OF THE PRIVACY ACT

Question to Stakeholders:

1. **Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?**

FCAI supports the current objects of the Act.

Any changes to the objects which are proposed should continue to strike a balance between supporting appropriate protection of individuals' personal information in line with community expectations and encouraging the development of innovative products and services that support consumers needs without the addition of unnecessarily prescriptive and burdensome regulation.

In particular, FCAI does not support the removal of the current requirement to balance the privacy of individuals with "the interests of entities when carrying out their functions or activities"[4]. The appropriate protection of individuals' personal information cannot be neatly divorced from the consumer expectation of ongoing access to increasingly intuitive and powerful products and services that are made possible by evolving technology.

Recognising this complexity must continue to be an objective of any modern, effective privacy regulation scheme.

[4] Consideration of the removal of this balancing requirement was recommended by the ACCC DPI report. See page 15 of the Issues Paper.

DEFINITION OF PERSONAL INFORMATION

Questions to Stakeholders:

2. **What approaches should be considered to ensure the Act protects an appropriate range of technical information?**
3. **Should the definition of personal information be updated to expressly include inferred personal information?**
4. **Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?**
5. **Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?**

FCAI members support the existing principles based and technology neutral approach to the definition of "personal information" in the Act.

This definition, together with detailed supporting regulatory guidance, has proven capable of being applied clearly to vastly differing products and services across all industries, including the conventional and connected vehicle features referred to above which have already been launched in Australia, despite many of those technologies not being foreseen at the time of drafting.

"Personal information" is not currently limited to information which identifies an individual, but also applies to information from which an individual is reasonably identifiable. Some of the vehicle-generated and user-introduced data referred to above may not be personal information when held by itself (because it is not about an identified individual), but if it can be matched with other information available to the manufacturer or otherwise used by the manufacturer to identify an individual (for example by searching a customer database), then it will be considered personal information under the current law.

FCAI members are sophisticated businesses which take their obligations under the Act very seriously and invest substantial resources in their privacy compliance systems, as well as working closely with their dealer networks to support adherence to privacy requirements at the retail level. As a result, despite the complexity of applying existing rules to the collection, use and management of vehicle-generated and user-introduced data, privacy compliance within the industry is high.

As the automotive products and services available in Australia are developed globally with often long lead times, FCAI members do not support any change to the definition of "personal information" that would reduce its current flexibility and add uncertainty or unnecessary regulatory burden to its application to future automotive products and services, including the introduction of autonomous vehicles into the market in the near future.

Such changes would lead to a risk that Australian consumers will have their access to future automotive product features and technology, and the associated consumer and community benefits which they could deliver, reduced or delayed.

FCAI recognises that question 2 in the Issues Paper is drawn from the ACCC concern, expressed in its DPI Report, that "given advances in data analytics technologies and the volume of technical data relating to identifiable individuals that is collected, used and shared in digital markets, the ACCC considers that it is important to clarify that technical data related to an identified individual is considered "personal information" within the scope of the Privacy Act.[5]"

It is important to note that the ACCC's use of the phrase "technical data" therefore has a very specific meaning linked to its concerns about particular data use practices identified within digital platform operators. This use is different to the ordinary understanding in the community of what "technical information" includes.

FCAI urges that extreme caution be exercised when assessing whether the ACCC recommendation should result in a change to the definition of "personal information" that applies across all sectors covered by the Act, or whether specific regulation (or OAIC guidance) applicable only to digital platform operators should be considered instead to address the ACCC's particular concerns.

If a change to the "personal information" definition is to apply to all entities covered by the Act, it is critical that it be very carefully drafted to apply only to the specific concerns sought to be addressed, and does not inadvertently cause the significant regulatory burden of the privacy legislation to be applied to a broad swathe of technical information that, while being able to be linked to an identifiable individual vis the individual's vehicle, would not be considered by consumers to require regulation to protect their genuine concerns about appropriate treatment of personal information (including many of the types of vehicle-generated data described above).

Likewise, any additional protections in relation to de-identified information (which is not currently considered to be personal information under the Act) or anonymised and pseudonymised information, must be carefully drafted to ensure that they are practical and do not have an unintended chilling effect on the ability for aggregated data to be used for purposes which provide significant community benefit, including:

- De-identified traffic data can be used to build up a picture of travel times, and suggested routes, minimising congestion, vehicle emissions and lost productivity as well as assist in road safety incident detection, traffic signal prioritization and long term road infrastructure planning.

- De-identified vehicle-generated data can be used to:
    - help identify unsafe sections of road (eg where vehicle traction is lost or pot-holes are detected); and
    - analyse product issues to narrow potential fields of investigation into geographical locations and operating conditions. While one vehicle with an identified issue cannot be used to draw robust conclusions, identifying multiple vehicles with a similar issue in particular circumstances can lead to accurate diagnosis and remediation of potential safety and reliability issues across defined groups of vehicles.

[5] See page 459 of the DPI Report.

- The operation of autonomous vehicles will be highly dependent on the synthesis of vast amounts of aggregated vehicle, crash, road, infrastructure and human behaviour data to optimize vehicle and pedestrian safety in line with community expectations.

Given the size of the Australian market, FCAI members rely on their overseas parent companies and other sources of vehicles for the development of future products and technologies. Many of these future products and technologies will focus on solving consumer dilemmas, needs and wants identified through the use of aggregated, globally sourced technical information. Unnecessarily restrictive regulation on the collection and use of this data in Australia may prevent it being taken into account in the development of global products and could cause those products to be less tailored to unique Australian conditions than would otherwise be the case.

NOTICE OF COLLECTION OF PERSONAL INFORMATION

Questions to Stakeholders:

20. **Does notice help people to understand and manage their personal information?**
21. **What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?**
22. **What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?**
23. **Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?**
24. **What measures could be used to ensure individuals receive adequate notice without being subject to information overload?**
25. **Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?**

FCAI members recognise consumers' rights to exercise choice and control over how their personal information is used. The provision of clear and transparent information about what information is collected and how it will be used is a critical requirement to achieve this.

As mentioned earlier, conventional and connected vehicle technology already provides consumers with access to a range of features that increase their comfort and convenience while also contributing to achieving societal goals such as improving road safety, reducing fuel consumption and vehicle emissions. These advances rely on the collection of a range of both vehicle-generated and user-introduced data to operate.

FCAI supports the current drafting of the requirements for the provision of notices of collection of personal information. The concepts of reasonableness and practicality which are central to that drafting provide businesses with the flexibility required to design notification strategies that are practical and effective in their vastly varying individual circumstances. FCAI would be concerned if this flexibility were reduced as recommended in the ACCC DPI Report[6].

The Act currently recognises that a business may meet its notification requirements before, or at, the time it collects personal information and where this is not practicable, it must take reasonable steps as soon as practicable to do so after collection[7].

As a result of the increasing complexity of automotive products and services, and the range of ways in which consumers interact with them, FCAI members already use a range of strategies to ensure that the required notifications are made effectively. The FCAI Voluntary Code notes that this may be done:

---

[6] ACCC DPI Report page 461.
[7] Australian Privacy Principle 5.

- in a contract or policy (including privacy policies and collection statements);
- in a user manual;
- via a special menu / agreement in the vehicle's infotainment system;
- via specific icons, pictures, or graphics in the vehicle;
- in mobile applications (apps);
- on websites and web portals; or
- in any other appropriate manner.

A very broad range of consumers interact with the products and services offered by FCAI members. A proportion of these individuals have a direct relationship with a particular brand through interactions with their websites, consumer promotions, customer support centres and authorised dealers, which enables the required notifications to be provided to them in a practical and effective way. As connected vehicle features, and subsequently autonomous vehicles, are launched in Australia, the range of individuals potentially sharing personal information with FCAI members via their connected vehicles may grow and may include categories such as:

- second and subsequent owners of vehicles whose contact details are not known
- drivers or passengers who share use of a connected vehicle owned by another person and interact with the connected features of the vehicle with their personal devices
- users of connected and autonomous vehicles used in ride-share or shared ownership models who interact with the connected features of the vehicle with their personal devices

In this context, acceptance of the changes recommended to notification requirements in the DPI Report without an overlay of practicability and reasonableness could:

- prevent the rollout of new technology to entire vehicle car parcs if it was not possible to avoid situations where unknown individuals were interacting with vehicle features that rely on data collection to operate; or
- require detailed privacy related notifications to be made available in-vehicle in a prominent way (potentially each time the vehicle was switched on), in case the current user of the vehicle had not already received the relevant disclosures via one of the relevant member's other sources of information.

This would clearly be untenable, not only from a user experience perspective but if unique notifications were designed to be programmed into vehicles for Australian use, the costs and lead times required may make development of an Australian version unviable.

FCAI fully supports the recognition in the Issues Paper that "any consideration of increasing notification requirements needs to be accompanied by a discussion of how best to communicate

notice to individuals in a way that will promote engagement, reduce information overload and reduce the risk of consent fatigue.[8]"

In this context, FCAI would welcome consultation about the introduction of consistent, practical guidelines (whether in regulation or OIAC guidance) that would assist organisations to fully inform their customers about how their data is used provided that it was not unnecessarily onerous or prescriptive. This could include the use of standardized terminology, formats and icons that would improve customer familiarity with privacy related concepts.

We note, however, that these strategies may be insufficient alone to convey to consumers sufficient information to enable them to be fully informed about the complex interactions between the products and services they wish to use, and the types of information required to deliver them.

By way of example, when a customer purchases a connected vehicle, they may have the ability to tailor which categories of vehicle-generated data are shared with the vehicle's manufacturer or other authorised parties. These categories could include diagnostic/maintenance data, driving data, location data, live traffic data and data required to activate remote control operations (remote start, remote lock/un-lock, remote start of climate control system).

The connected features of the vehicle that are available to the customer will depend on the choices the customer has made about which categories of data they wish to enable the vehicle to share. If they do not enable the vehicle to share location data for example, they may not be able to access the vehicle's real time traffic alert or "find my car" features.

The complexity of these scenarios, and their specific application to a particular user, mean that meaningful information about the particular treatment of vehicle-generated and user-introduced data in a particular case will not be able to be reduced to simple icons and common phrases. As a result, it is essential that any changes proposed to the notification requirements in the Act continue to provide businesses with the flexibility needed to appropriately and clearly disclose all relevant information to their customers.

[8] Issues Paper page 39.

CONSENT TO COLLECTION AND USE AND DISCLOSURE OF PERSONAL INFORMATION

Consent to collection, use and disclosure of personal information

Questions to Stakeholders:

26. **Is consent an effective way for people to manage their personal information?**
27. **What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?**
28. **Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?**
29. **Are the existing protections effective to stop the unnecessary collection of personal information?**
    a. **If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?**
30. **What requirements should be considered to manage 'consent fatigue' of individuals?**

FCAI supports the current requirement to obtain consent, either express or implied, to the collection and use of personal information (as currently defined) from an individual in particular circumstances, including:

- the collection of sensitive information
- the use or disclosure of personal information for a secondary purpose not directly linked to the primary purpose of collection and where the use or disclosure would not reasonably be expected
- the use or disclosure of personal information or sensitive information for direct marketing purposes
- the disclosure of personal information to an overseas recipient
- the use or disclosure for a secondary purpose falling within a "permitted general situation" (including lessening or preventing a serious threat to life, health or safety of an individual or to public health or safety);

unless a specific legislative exception applies (including law enforcement and legal proceedings).

FCAI believes that the current requirements strike a fair and reasonable balance between the requirement to ensure that consumers are informed of the use to which their personal information would be put (via the notification requirements referred to above), ensuring particular information and uses are provided with additional safeguards and enabling businesses to offer the products and services that consumers want without unnecessary administrative or regulatory burden.

FCAI has significant concern that the adoption in the Act of the ACCC's recommendations in the DPI Report[9] that:

- consent should be required to be obtained in relation to any collection, use or disclosure *unless the personal information is necessary for the performance of a contract to which the individual is party*, is required by law, or an overriding public interest reason applies [emphasis added]; and
- valid consent should require a clear affirmative act and cannot be bundled with other consents

when applied to all organisations (not just the digital platform operators to which it is appeared to be addressed) would be impractical and onerous and would lead to consumers being swamped by an unmanageable deluge of consent requests.

We consider that this would overwhelm any desired increase in the transparency of information processing or any desired adjustment to the bargaining power of individuals and the organisations with whom they share their personal information, and would be inconsistent with a common-sense understanding of how consumers expect their chosen products and services to operate.

We would particularly like to highlight the following practical issues that are raised by the ACCC recommendation:

- the majority of instances where FCAI members collect personal information from individuals are not governed by a contract between the parties (unless that term is defined very broadly). This is because (with some limited exceptions) vehicles are initially purchased from the appointed authorised dealers of FCAI members and then on-sold to multiple subsequent owners, none of whom are obliged to enter a contract with the vehicle's manufacturer (or their local subsidiary or distributor).
- for the reasons dealt with earlier in this submission, in many cases FCAI members will not have contact details for the individuals whose information they may be collecting through the use of connected, and subsequently autonomous, vehicles. This issue will be exacerbated if the definition of personal information is expanded to include "technical information" without careful regard to the practical concerns identified above.
- if the definition of "personal information" is amended to inadvertently include the types of vehicle-generated data described above, an obligation to obtain separate consent for each use of a vehicle's data outside a contract between a user and the manufacturer could easily become completely unworkable. For example, it would require a vehicle manufacturer to obtain the consent of multiple vehicle owners each time it wished to share vehicle-generated data from a group of vehicles with a component supplier in order to investigate a potential quality or safety issue in that group of vehicles.

[9] ACCC DPI Report page 464.

- the collection of personal information is a fundamental requirement for many connected and autonomous vehicle features to operate. For example, in order for an emergency assistance feature in a vehicle to notify emergency services that the vehicle has been involved in an accident if the user is unable to do so, it needs to collect and send specific location data linked to the driver via a paired mobile device or connected vehicle modem in real time.

FCAI recognises that some consumers are already overwhelmed by the amount of information they need to absorb to be properly informed about whether to consent to the use of their personal information in any particular case. We strongly support the concern raised in the Issues Paper that further tightening consent requirements would place an even larger burden on individuals in this regard[10].

While some of the options suggested in the DPI Report to address this (consent only required where collection falls outside a contract, use of standardized icons or phrases) may be effective when applied to digital platform operators, for the reasons identified above they would not assist to reduce the substantial burden on users and manufacturers of connected or autonomous vehicles in most circumstances.

FCAI therefore strongly requests that should any changes to the regulation of consent in the Act be required to address identified shortcomings in connection with digital platform operators, that this be dealt with by industry specific requirements rather than by a change to the Act that would have universal application.

Exceptions to the requirement to obtain consent

Question to Stakeholders:

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any other situations be included?

FCAI supports the existing general permitted situations and general health situations as appropriate and fit for purpose.

In particular, it recognises the value to the community of the general permitted situation which permits an entity to "use or disclose personal information for a secondary purpose where it reasonably believes the use or disclosure is necessary to prevent a serious threat to the life, health or safety of an individual or to public health or safety"[11]

It would, however, be useful if further guidance could be issued to confirm a standing approval, without need for individual consent, of the use of vehicle-generated information (which may include personal information) of the kind collected in connected and autonomous vehicles where such

[10] Issues Paper page 44.
[11] See Australian Privacy Principle 6, paragraph 6.34.

information was necessary for automotive product or service development or to further the community benefits of vehicle safety, road safety and vehicle emission reduction.

Pro-consumer defaults

Question to Stakeholders:

32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

FCAI notes that the matters raised in the Issues Paper in relation to the potential for the introduction of pro-consumer defaults apply specifically to concerns raised in the DPI Report that digital platform operators should only collect information needed to provide their products and services and that default settings enabling data processing for a purpose other than for the performance of a contract should be switched to off[12].

As stated above, the information collected by connected (and soon) autonomous vehicles is required for the operation of their particular features. The inapplicability of a "contract" based nexus in a connected and autonomous vehicle framework has also been addressed earlier in this submission.

Any amendments made to the Act in this regard should therefore be limited to addressing the concerns raised in respect of digital platform operators, and should not have universal application to all entities governed by the Act.

The role of consent for IoT devices and emerging technologies

Question to Stakeholders:

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

FCAI recognises the difficulties associated with applying the existing privacy law to Internet of Things (IoT) devices which collect a broad range of personal information, including from multiple people, some of whom may not have consented to, or even realise, that their information is being collected[13].

Connected and autonomous vehicles share some of the challenges faced by IoT devices, including the difficulty of identifying individuals who may be using the vehicle at any particular time, however

[12] Issues Paper page 43.
[13] Issues Paper page 45.

generally the information collected is being used to enable the particular features of the vehicle that the user is operating to function and does not include sensitive information such as health data.

FCAI members would be willing to participate in consultation in regard to this area, as it is critical that any regulation deemed necessary to ensure universal application of privacy principles to IoT devices does not have unintended and potentially significant implications for the ongoing roll out of connected and autonomous vehicle technology, and the broader community benefits they will bring.

Ensuring that any revised definition of “personal information” does not inadvertently capture vehicle-generated data that does not fall within the community expectation of data requiring privacy protection (as identified above) will be one factor that is key to a constructive resolution of this issue.

CONTROL AND SECURITY OF PERSONAL INFORMATION

Security and retention

Questions to Stakeholders:

43. **Are the security requirements under the Act reasonable and appropriate to protect the personal information of individuals?**
44. **Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?**

FCAI strongly supports the need for strict security requirements for the protection of personal information and believes that the existing security requirements under the Act are reasonable and appropriate to protect the personal information of individuals.

The maintenance of appropriate and ongoing physical, technical, security, access controls and organizational measures to protect customers' personal information are a key component of the "We Maintain Data Security" principle in the FCAI Voluntary Code.

In particular, FCAI members commit to protecting the safety of drivers and the integrity of their vehicles (particularly from cyber security threats) before any vehicle-generated data is made available to third parties or received from third parties to be transferred to a vehicle. This will include taking reasonable steps to secure the data transmission, which may include the requirement that data be sent and received through a secure off-board facility.

Access, quality and correction

Questions to Stakeholders:

45. **Should amendments be made to the Act to enhance:**
    a. **transparency to individuals about what personal information is being collected and used by entities?**
    b. **the ability for personal information to be kept up to date or corrected?**

A clear, practical definition of personal information (see comments above) is critical to ensuring:

- transparency to individuals about what personal information is being collected and used by entities; and
- individuals are able to keep their information correct and up to date.

Any changes to the existing definition that inadvertently include vehicle-generated information from connected cars (outside the kinds of information the community would expect to be protected) will also cause flow on difficulties for the meaningful application of an individual's right to review and correct or update any personal information which has been collected from them.

Not only could FCAI members be required to isolate and extract technical information associated with a particular individual from within global systems containing massive amounts of technical data, once the information was identified the affected individual could have to wade through a mountain of highly technical data to find the type of "real" personal information they were expecting to find and check.

Such a situation would be untenable from the perspective of both consumers and FCAI members and their parent organisations.

Right to erasure

Questions to Stakeholders:

46. **Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?**
47. **What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?**

Similar to our comments above in relation to an individual's right to update and correct personal information collected by an organisation, a clear, practical definition of "personal information" will be critical to ensure that any right to erasure which was included in the Act was able to operate without significant unintended consequences.

Once again, if the definition was not drafted carefully and included vehicle-generated information from connected cars (outside the kinds of information the community would expect to be protected), it would be extremely difficult, if not practically impossible, to identify and erase the personal information of a particular individual from aggregated data in vehicle manufacturers' global technical databases.

Any right to erasure would also need to include exceptions necessary to ensure that information which was required to be retained for compliance with laws or public benefit reasons was not destroyed (in a similar way to general permitted situations being an exception to the requirement to obtain consent to the collection of personal information in some circumstances). In an automotive context, exceptions should also include information required to be retained for vehicle safety (including product recall), road safety and emission reduction reasons.

OVERSEAS DATA FLOWS AND THIRD PARTY CERTIFICATION

Questions to Stakeholders:

48. **What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?**
    a. **Are APP 8 and section 16C still appropriately framed?**
49. **Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?**
50. **What (if any) are the challenges of implementing the CBPR system in Australia?**
51. **What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?**
52. **What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?**

FCAI does not have any concerns with the current accountability approach to cross-border disclosures of personal information, and recognises the responsibility of members to take reasonable steps to ensure that any overseas recipient of Australian personal information does not breach Australian Privacy Principles. FCAI members would, however, value a government approved list of jurisdictions with substantially similar privacy protection schemes and a list of approved standard clauses for use with overseas trading partners to streamline business assessment of the appropriateness or otherwise of potential cross-border disclosures.

ENFORCEMENT POWERS UNDER THE PRIVACY ACT AND THE ROLE OF THE OAIC

Questions to Stakeholders:

53. Is the current enforcement framework for interferences with privacy working effectively?
54. Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?
55. Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?
    a. If so, what should these enforcement mechanisms look like?

FCAI members support consumers' rights to have their personal information protected and encourage regulatory mechanisms that assist them to raise any concerns they have at the earliest opportunity so these can be addressed to the consumer's satisfaction in a quick, practical and cost-effective way.

FCAI believes that the current enforcement framework for managing breaches of the Act assists members to achieve this goal and particularly values the constructive role that the OAIC plays in assisting members to resolve any privacy issues that are not able to be solved internally to the satisfaction of the customer. Having access to an independent privacy expert to assist in the dispute resolution process is also very valuable in ensuring customer confidence in an appropriate resolution of their concern.

FCAI believes that the current enforcement mechanisms available to the OAIC are working effectively for both the resolution of individual complaints and escalation to a formal investigation where systemic issues are identified (potentially leading to determinations and compensation orders which are enforceable by the Federal Court). Accordingly, it does not believe that expansion of those mechanisms is required.

DIRECT RIGHT OF ACTION

Questions to Stakeholders:

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

FCAI believes that the current enforcement mechanisms in the Act are working effectively for both the resolution of individual complaints and the escalation by the OAIC where required of any systemic issues identified. This success is in large part due to the direct involvement of the OAIC, which is respected as an independent and professional expert by both consumers and businesses.

FCAI is concerned that the inclusion of a direct right of action could undermine the operation of the current OAIC compulsory conciliation process and set up a "two-track" resolution process that could lead to an increase in frivolous complaints and add an unnecessary burden to the court system.

Should the inclusion of a direct right of action be considered appropriate, FCAI strongly recommend that it only be permitted after conciliation by the OAIC has been completed and then only if the OAIC certifies that the concern raised is one of substance.

STATUTORY TORT

Questions to Stakeholders:

57. **Is a statutory tort for invasion of privacy needed?**
58. **Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?**
59. **What types of invasions of privacy should be covered by a statutory tort?**
60. **Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?**
61. **How should a statutory tort for serious invasions of privacy be balanced with competing public interests?**
62. **If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?**

FCAI members recognise the rights or consumers to have their personal information appropriately protected and have invested, and will continue to invest, substantial resources in ensuring their ongoing compliance with their obligations under the Act. FCAI further recognises the significant and appropriate introduction of offences in both Commonwealth and State criminal law to prohibit particularly egregious breaches of an individual's privacy.

In this context, FCAI does not believe that adding a further level of complexity to privacy regulation through the introduction of a general statutory tort for invasion of privacy is necessary to encourage the desired compliance behaviours.

NOTIFIABLE DATA BREACHES SCHEME

Questions to Stakeholders:

63. **Have entities' practices, including data security practices, changed due to the commencement of the NDB Scheme?**
64. **Has the NDB Scheme raised awareness about the importance of effective data security?**
65. **Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB Scheme?**

FCAI members support the need for effective data security and have not experienced any challenges with the implementation or operation of the Notifiable Data Breaches Scheme either on its own or in parallel with other similar schemes in other jurisdictions.

INTERACTION BETWEEN THE ACT AND OTHER REGULATORY SCHEMES

Questions to Stakeholders:

66. **Should there continue to be separate privacy protections to address specific privacy risks and concerns?**
67. **Is there a need for greater harmonisation of privacy protections under Commonwealth law?**
    a. **If so, is this need specific to certain types of personal information?**
68. **Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?**

FCAI members have not experienced any issues with the application of overlapping privacy obligations under the Act and other Commonwealth or State legislation.