

IAP the road forward // Protecting Information and Privacy

This fact sheet answers commonly asked questions about protecting information and privacy within the Intelligent Access Program.

Introduction

The Intelligent Access Program (IAP) is a voluntary program which provides heavy vehicles with access, or improved access, to the Australian road network in return for monitoring of compliance with specific access conditions by vehicle telematics solutions.

This fact sheet outlines the strict conditions that apply to the collection, use and disclosure of information under the IAP.

LEGISLATION AND GUIDING PRINCIPLES //

The conditions that apply to the collection, use and disclosure of information under the IAP are designed to provide the highest order protection of information privacy. They are set out in each jurisdiction's IAP legislation and are founded on the Information Privacy Principles set out in the Commonwealth Privacy Act 1988.

WHAT INFORMATION IS COLLECTED UNDER THE IAP? //

Joining an IAP Application

Transport operators applying to join an IAP Application need to provide the following information to the road authority:

- operator's name, ABN or ACN, postal address, and contact details;
- name, title/position, and contact details of the operator's nominated officer;
- details of the vehicle to be monitored (including make, model, registration number and VIN number) and garaging address, and,
- details of any trailer or trailers required to be separately identified (if required by the IAP Application).

Transport operators must also provide this information to the IAP Service Provider they engage to provide IAP services.

Operating under an IAP Application

Transport operators joining the IAP agree that the IAP Service Provider must monitor the participating vehicle's movements in accordance with IAP service requirements, maintain accurate data, records and information regarding these movements and, in the event of non-compliance with an applicable IAP Condition, issue a Non-Compliance Report to the relevant road authority.

Each vehicle operating under the IAP is fitted with an in-vehicle unit. The in-vehicle unit is specific to the vehicle (ie. rigid vehicle or prime mover) and will monitor and store the necessary IAP information about the vehicle.

Electronic records will also be made of any interference with the in-vehicle unit – such as removal of any sensors or GPS equipment.

Non-Compliance Reports

A Non-Compliance Report is the report sent to the road authority by the IAP Service Provider when it identifies any non-compliance with the IAP Conditions (ie. agreed conditions of access associated with the IAP Application) issued by the road authority to the transport operator for the participating vehicle.

A Non-Compliance Report does not necessarily mean a traffic offence. All non-compliance reports are treated on a case-by-case basis, and it will be up to the relevant road authority to decide what action to take.

WHO CAN ACCESS IAP INFORMATION? //

Who owns the information collected?

Each transport operator owns any information collected about the movement of its own vehicles.

However, a transport operator in the program also permits its IAP Service Provider to collect, monitor and store the information, and issue Non-Compliance Reports to the relevant road authority.

Can a transport operator access the information?

A transport operator may inspect the IAP data, records and information maintained by the IAP Service Provider in respect of their vehicle, provided they give the IAP Service Provider reasonable notice. A transport operator may also receive and use this data as part of its commercial or fleet management activities.

A transport operator may also ask to be supplied with the information contained in any Non-Compliance Report issued in respect of their vehicle. However, the information provided by the IAP Service Provider will be in a different format to the Non-Compliance Report sent to the road authority.

Who else has access to information?

There are strict restrictions upon when, why and how an IAP Service Provider may disclose IAP information to other parties. In brief, the IAP Service Provider can make IAP information available to:

- road authorities if a Non-Compliance Report is issued, or the IAP Service Provider suspects any tampering;
- TCA and IAP auditors, to confirm that the IAP Service Provider is meeting its certification requirements, and,
- police officers or authorised road authority officers, for law-enforcement purposes if authorised by a warrant issued by a court.

IAP Service Providers will have to keep records of any information released – including who the information was released to, in what form, and why – for at least two years.

HOW LONG IS IAP INFORMATION STORED? //

Compliant information will be stored by the IAP Service Provider for a maximum of 12 months, to allow time for an audit to be done. After 12 months, the information will be destroyed. As owner of the data, the transport operator may of course elect to keep the data for its own purposes, for a longer period.

Non-compliant information must be stored by the IAP Service Provider for at least four years after a Non-Compliance Report has been sent to the road authority.

PROTECTION OF PRIVACY AND PERSONAL INFORMATION //

What personal information is collected through the IAP?

No information, personal or otherwise, about drivers is collected through the IAP. IAP information is collected for the purpose of monitoring vehicle compliance with access conditions, not drivers' movements. As a result, the identity of the driver is not required and is not recorded.

Where personal information is collected about individuals (eg. owner operators' details or details of nominated officers) the person collecting that information must take reasonable steps to ensure that the collection of that information does not intrude to an unreasonable extent on the personal privacy of the individual to whom the information relates.

What if an individual believes the information held about him or her is wrong?

If an individual believes that information held about him or her by an IAP Service Provider or by TCA is inaccurate, the individual can request that the information be corrected.

The IAP Service Provider or TCA must then either make appropriate alterations to the personal information, or if it considers the information is not inaccurate, provide a written explanation of the reasons for not altering the information.