The Autonomous Vehicle technology is still emerging at a very fast pace and is very dynamic, hence the Automated Vehicle Safety Law need to be reviewed and upgraded accordingly.

**ADSE duties and enforcement framework**

The AV’s are meant to take away the driving from the driver sitting inside the vehicle, which then makes the ADSE liable for upholding the law and owing up to the responsibilities of safe driving. The definition of ADSE in AVSL must clearly state the entities responsible for safe functioning of an AV and must also define their specific tasks. Their responsibilities must include, but not limit to; safety of the occupants and that of others on the road, integrity of ADSE’s software that it cannot get hacked into, the liability of software breach need to lie with the ADSE, and their capability in dealing successfully with the trolley problem.

The executives of ADSE must also declare their dependence on other entities involved in the safe operation of their ADS and should be covered under legislation. For safe and successful deployment of Autonomous Vehicles on Australian roads, it is important that each entity involved in safe and successful operation of ADS must have their specific tasks, which they are responsible for, well documented and covered under legislation. This will provide lucidity to the executives while decision making.

**Transfer of ADSE responsibilities**

If the new ADSE takes the ownership of the existing ADSE, then the responsibilities must be transferred in full or as mutually agreed upon by both the parties but only after the legislative approval from concerned authority as described in AVSL. The regulator must enlist all the responsibilities to be taken over by the new entity and must also audit the new entity for its capabilities in safely and successfully carrying out the new responsibilities which they are about to take. If the new entity fails the audit; the regulator must not approve the transfer.

In case when the ADSE is exiting the market, they would need to transfer their IP and technology to the regulator. The regulator may appoint an interim ADSE to keep the ADS operational. The regulator can also transfer the IP and the technology to the new ADSE, subjected to legislation.

**In-service modifications and after-market installations**

NTC’s proposal that any modification or upgrade; can only be performed by an approved and accredited entity is idyllic. These are still early days for automated vehicles, hence aftermarket ADS kits or any such installations which would convert in-service vehicles into automated vehicles, should be prohibited. Once the automated driving technology has proven itself safely on our roads, then only AVSL should be revised and provisions for such installations and modifications be allowed for.

**Functions and powers of the in-service safety regulator**

NTC has hit the right note again by identifying the additional functions need to be undertaken by the regulator to ensure in-service safety. Reporting, Crash investigations, Accreditation and Regulatory approvals were already mentioned by NTC, driving data collection and analysis would be additional too. The responsibilities and regulatory authorities will grow correspondingly in a phased manner with the growth in automated vehicle market and automated vehicle technology.

**Roadside interaction and enforcement**

The Law enforcement authorities need to be briefed about the new laws and regulation brought upon by the emergence of new technologies in the field of Automated Vehicles. They need to be given time to comprehend these new laws so that they could enforce them on with all fairness.

For a national AVSL to be enforced, the regulatory authority needs to develop a law enforcement interaction protocol on behalf of in-service regulator and/or roadside enforcement agencies and advise the ADSEs of the same. By doing so different ADSEs will follow the same enforcement protocols nationwide.

If a road traffic law is breached by the vehicle while ADS was engaged, the incident should be treated as a breach of the general safety duty and not handled through the infringement system for human drivers. It is the foremost responsibility of ADSE to ensure their ADS is safe to be deployed on our roads. Whereas, at the time of breach, if a remote driver was in control then the infringement need to be booked against the entity providing remoting driving services, but if remote driving was part of ADS then the liability would fall on ADSE.

In the situations, where it is unclear that which entity was in control of the vehicle at the time of breach, the infringement notice should be issued to the registered owner / operator. But they should also be given time and a chance to corroborate that which entity was in control, along with data to support their claim.

NTC must also consider the cases where road traffic or road safety law was breached or not breached on ethical grounds, for instance, to give way to an Ambulance, a Red Traffic Light signal should be crossed or not crossed. Such breaches will happen on numerous occasions as the scenarios could be multiple. The ADS can only make a humane decision when its decision make is running on Ethical AI (Artificial Intelligence). Hi IoT proposes that until the ADS have Ethical AI as their integral part, remote operation (tele-operation) should be made an integral part of ADS; Human taking ethical decisions, to counter trolley problem.

However, if any ADS are found to be breaching the road safety rules, they should be taken off our roads as, the whole point of having Automated Vehicles on our road is to avoid human errs. They should only be allowed back on once they’ve demonstrated that the error or breach has been rectified permanently.

**Access and exchange of information by the in-service regulator**

The ADSE should be in charge of data and information collected by ADS. The ADSE should also be made responsible for its preservation and should bear the responsibility of reproducing that data to Commonwealth as and when required. In doing so, the privacy of the individuals involved should be protected or as directed by the Commonwealth. The sharing of data among the entities can only be done by the consent of the regulatory authority.