Submission by VOICE Australia to the
Parliamentary Joint Committee on Intelligence and Security's
Review of the Cyber Security Legislative Package 2024

For National Security, Regulate the Cybersecurity of Connected Private Vehicles

15 October 2024

Our Submission focusses on the cybersecurity of connected private vehicles (for definition, see Footnote)[1]. We submit that connected private vehicles

- Are relevant to national security;
- Are not the focus of the current cybersecurity legislation package;
- Should be brought into national security discussions.

Why are connected private vehicles relevant to national security?

Consider these scenarios, none of which is theoretical:

- **Tracking**: Some vehicles have built-in GPS which cannot readily be turned off. Currently, nothing stops a nation state adversary, such as China through made-in-China vehicles, to access their location, thereby knowing from the aggregate level (eg. traffic flowing away from the site of a bombing) to the individual vehicle level (current and past locations).
- **Intelligence**: An adversary can do more if it is able to link a vehicle to a person. This is possible because a civil-military-fusion nation such as China can mandate access to car dealers' data. Thus, it can, for example, blackmail the person if some of their trips are personally embarrassing. Or, it can know which officials are driving to a national security meeting and where. Vehicles with built-in microphones can also be listened into.
- **Physical actions**: Using the above intelligence, an adversary can do much to damage Australia. For example, it can cause traffic chaos to delay critical road-based transport of military materials during wartime; It can even assassinate selected Parliamentarians or mid-level officials who play important roles but are not provided personal protection.

[1] By "**connected private vehicles**", we mean those which use public roads, carry only a few people at a time (ie. private cars, taxis, motorhomes, motorcycles,..), and send or receive signals (via GPS, Bluetooth, mobile network, satellite,..), whether driven manually or by algorithms. Our Submission does not deal with, eg. watercraft, or vehicles used solely on farm land

- **Hacking**: Cybersecurity researchers have demonstrated that they could remotely hack connected vehicles then, for example, brake it hard, or steer it, or just listen in. This cyber-to-physical threat is huge and is no longer theoretical. This has been demonstrated in real-life attacks from nuclear facilities down to pager devices.

Why does VOICE Australia believe that connected private vehicles are not currently the focus of cybersecurity legislation?

- **The Cyber Security Bill 2024** in the Cyber Security Legislative Package 2024 covers "devices". The Bill does not define this term, but based on the stated Object of the Bill, it seems unclear to us whether devices in private connected vehicles are within scope;
- **The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024** in that package does cover transport infrastructure, but does not seem to cover connected private vehicles;
- **The Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024** in that package also does not mention them;
- **What about government agencies**? It is possible that some are taking executive action on this space, but we are not aware of any.

VOICE Australia submits that if connected private vehicles are not regulated now, then they should be:

1. **Reporting:** Include vehicle-related industries in the current security package's scope – eg. they should report cybersecurity incidents;
2. **Data:** Examine vehicle companies' collection of data. Security researchers have discovered, for example, that some companies receive real-time data about how many people are currently in a vehicle;
3. **Bugs:** Require vehicle manufacturers to continually work on their vehicles' cybersecurity issues: promptly discover them, resolve them, and certify that their vehicles are cybersecure;
4. **China:** Give increased scrutiny to Chinese and other vehicles made in or have components from China. This is because of China's civil-military fusion. The US is proposing a ban on Chinese software and hardware for smart vehicles. Australia should consider this as a starting point.

-End-