National Motor Vehicle Theft Reduction Council

28 January 2021

Competition and Consumer Amendment (Motor Vehicle Service and Repair Information Sharing Scheme) Bill 2020

Submission by the National Motor Vehicle Theft Reduction Council (NMVTRC)

Introduction

This document is a formal submission by the National Motor Vehicle Theft Reduction Council (NMVTRC) to the Australian Government s Bill for an Act to amend the *Competition and Consumer Act 2010* (the Bill) to establish a motor vehicle service and repair information sharing scheme.

The NMVTRC is Australia s expert body on vehicle crime. A joint initiative of Australian state and territory governments and the insurance industry, its purpose is to develop and facilitate the implementation of strategic national responses to combat vehicle crime.

The NMVTRC maintains world-leading analysis systems on vehicle crime which integrate theft incident and vehicle data sourced from more than 40 organisations nationally including every police service, registration agency and the nation s major insurers. From those combined sources we can compile more than 140 bits of information about every reported theft, including circumstances of the theft and the standard of an individual vehicle s security features.

This submission concentrates on the potential impacts of wider access to vehicle security information in respect to its potential to facilitate profit-motivated vehicle crime by allowing the overriding or rewriting of a vehicle s critical electronic security features.

For the purposes of this submission the NMVTRC defines vehicle security information as data, protocols or processes associated with the—

- effective operation of vehicle immobiliser systems; and
- coding of replacement keys (and immobiliser transponders).

We note that the Bill envisages that much of the administrative detail about how an approved scheme operates, including defining the characteristics of a fit and proper person (FPP) test, will be dealt with in development of the Scheme Rules determined by the Minister. We look forward to further consultation in that respect but make some general observations herein about related processes, and the challenges of applying FPP standards within a *distributed* assessment model that assumes a multitude of decision makers will apply the same (or at least consistent) judgment in determining an application for access.

Vehicle Crime in Australia

Motor vehicle theft in Australia has decreased significantly over the past two decades since its peak in 2001. However, the theft landscape continues to change and presents significant new challenges that simply were not present as recently as five years ago.

Increasingly, vehicle theft is not just a single crime; it is now often at the centre of a more complex mix of high-harm, high-impact offending that may involve significant road safety risks, other crimes against a person, subsequent property crimes and a wide variety of fraudulent activity in respect of personal identity, finance, and staged collisions.

In the 12 months to September 2020 a total of 52,638 vehicles were stolen across Australia—the lowest annualised volume since 2015.

However, we believe this represents a temporary distortion in the trend of the nation s theft trajectory, which in March 2020 we were predicting would breach 60,000 thefts for the first time since the Global Financial Crisis of 2007-2009. There is no question that the nation s COVID-19 related social and work restrictions helped to contain theft levels. However, with the established correlation between the performance of the economy and crime generally, there is a significant risk that volumes will grow in the next several quarters as social conditions normalise, and temporary income support programs wind up. We anticipate a challenging theft outlook for 2021-22.

In 2020 some 9,200 passenger and light commercial (PLC) vehicles vanished altogether—the surrogate indicator of the level of organised criminal activity seeking to convert stolen vehicles into cash.

The NMVTRC estimates the total annual cost of PLC vehicle theft to be $939 million, excluding the very large community costs associated with police investigations, courts, and corrections.[1]

Security of the Australian Fleet and Modes of Theft

The increasing penetration of electronic immobilisers across the Australian fleet has made a major contribution to improving the nation s theft performance. Nationally 9 in 10 vehicles are protected by an engine immobiliser.

By law all new vehicles sold in Australia since 2001 are fitted with a factory fitted immobiliser that complies with regulated Australian and European security standards. The introduction of the mandatory fitting of engine immobilisers has rendered modern cars almost impossible to steal today without the thief gaining access to the keys.

The relative security of immobiliser technology has seen a distinct shift in offenders tactics, with residential burglaries to access the keys of secure vehicles now recognised as the most common mode of theft. Despite media reports, incidents of electronic hacking in Australia are very rare events.

The NMVTRC conducts an annual threat assessment of current and emerging risks based its own data analysis and intelligence from its Vehicle Crime Managers Network. The network comprises senior officers of all state and territory police services, the Australian Criminal Intelligence Commission, and the Australian Border Force.

Along with advice from this Network, studies conducted by the NMVTRC and international theft bodies still indicate that the majority of late model thefts have been facilitated by access to the key and transponder via a burglary.

Across Europe, the estimated impact of electronic hacking may range from 1 in 20 thefts in the United Kingdom up to 1 in 5 in Russia via combination of specialised ‘defeat or programming tools and insider technical knowledge. Australia s exposure is estimated to be in the very low range at less than 1 in 100.

Obviously, the release of security information beyond the vehicle distributors own networks carries an increased risk of that information falling into the wrong hands and therefore requires robust risk mitigation measures. In the NMVTRC s assessment there is currently insufficient detail on how it is envisaged the ‘fitness and propriety regime would operate.

Design of Approved Schemes

Treatment of Safety Information for Automated Driving Systems (ADS) Versus Security Information

We note with interest that the Bill expressly excludes safety information relating to ADS Level 3 (and above) vehicles. We assume that this is to maintain the primacy of the *ADS Entity's* universal obligation to assure the safety of an automated vehicle in all operating conditions without requiring the intervention of a human driver.

We would prima facie contend that security information should be exempt on a like basis, i.e., that widening access poses an unacceptable risk of manipulation by criminal networks that cannot, at least under the level of administrative detail currently available, be sufficiently mitigated.

With immobilisation rates approaching 100 per cent and the very low incidence of electronic hacking, modern vehicle security systems deployed in Australia remain almost impossible to defeat. The NMVTRC is committed to ensuring that this remains the case.

Any wider access to security information poses a number of threats that need to be managed to mitigate the risk of allowing ‘backdoor access for third parties to that information in order to facilitate crime.

[1] Based on an independen economic analysis conduc ed by Niskin En erprises or he NMVTRC (Sep ember 2020) which es ima ed vic ims cos s per inciden o be $17,300 or recovered vehicles and in he range o $7,980 o $20,370 or non-recoveries (depending on ac ors such as vehicle age, personal, injury and insurance adminis ra ion cos s).

Consistent Assessment of Applications

While it is noted that the Bill aims to restrict safety and security information to those who meet specified criteria, in the NMVTRC s view the onus on individual data providers to make an FPP assessment—with no experience in making such judgements—is problematic and leaves the system vulnerable to manipulation.

While a form of standardised criminal record check may be required, the system seems to rely on delegates of the data provider being able to make non-expert judgements as to what constitutes a relevant or disqualifying criminal offence. In most cases the delegate is likely to have a technical or engineering background with absolutely no experience in the application of FPP standards. The NMVTRC Executive has had considerable direct past experience in applying FPP standards in respect of a range of occupational licensing regimes and can attest that it is a task for specialists with appropriate professional experience and training in applying what is in effect a quasi-judicial assessment.

The task is made more difficult by the absence of any form of nationally consistent occupational competency or licensing regime with only New South Wales and Western Australia maintaining any form of related registration or licensing.

(The NMVTRC s understanding is that the equivalent United States (US) model—which it seems the Bill s primary objectives are based on—utilises a centralised processing bureau with appropriately trained, expert personnel.)

In the NMVTRC s assessment the above challenges call for a secure, centralised system (perhaps administered by the envisaged *Scheme Adviser* or other competent authority) to ensure all applications are subject to a consistent, meaningful appraisal of a candidate s—

1. Need for the information—based on a standardised form of documentation as to the nature of the repair or service proposed to be provided; and
2. Suitability as an FPP.

A centralised system would ensure all applications are filtered through a secure, consistent funnel, greatly mitigating the risk of criminal exploitation.

In the NMVTRC s view, extensive consultation is needed with industry and FPP subject matter experts as to how appropriate standards can be applied pragmatically and consistently.

Further guidance is also required as to whether an approval is enduring or subject to review, renewal and/or termination with appropriate sanctions to deal with misrepresentations by repairers as to the need for access or trading in related information.

While the Bill includes extensive financial penalties for data providers failing to provide service information, there does not appear to be any penalties contemplated for the misuse of supplied information by an applicant or repairer.

Summary

The NMVTRC appreciates the benefits of accessible diagnostic, repair and servicing information for repairers and consumers.

While the current Bill recognises the importance of restricting access to safety and security information, the NMVTRC would contend that further safeguards are necessary.

Security information is by its very nature different to the general service information because of its critical importance to safeguarding the vehicle from criminal attack. The current controls over the sharing of this information in Australia have helped deliver the nation low rates of electronic criminal manipulation by world standards.

It is the NMVTRC s view that the onus on individual data providers to determine a person s FPP status is unwieldy and leaves the system extremely vulnerable to manipulation. Similar to that seen in the US, the NMVTRC recommends the establishment of a central bureau (or monitor) to provide objective and expertly applied FPP assessments.

A repairer should be required to demonstrate a need for access to specific security information to conduct the proposed service or repair.

Extensive consultation with industry and appropriately qualified, experienced FPP subject matter experts to determine a workable set of rules for both the preceding elements is essential.

Finally, we recognise there is some consumer disquiet in respect of the cost of genuine replacement keys. However, we would argue this could be dealt with as a separate issue by, for example, the Australian Competition and Consumer Commission promoting the principle of transparent pricing that reflects the true replacement cost and any dealer mark-up.

For any issues of clarification in respect of these matters, please contact the NMVTRC s Chief Executive, Geoff Hughes.