

Remarks to the Standing Committee on Industry & Technology

Bill C-244 An Act to Amend the Copyright Act



Canadian Vehicle Manufacturers' Association (CVMA)

Brian Kingston, President & CEO

November 14, 2022

Canadian Vehicle Manufacturers' Association (CVMA)
116 Albert Street, Suite 300
Ottawa, ON K1P 5G3
416-364-9333 bkingston@cvma.ca

Mr. Chair, Honourable Members, thank you for the invitation to appear today as part of the committee's study of Bill C-244 An Act to Amend the Copyright Act.

The Canadian Vehicle Manufacturers' Association (CVMA) is the industry association representing Canada's leading manufacturers of light and heavy-duty motor vehicles. Membership includes Ford Motor Company of Canada, Limited; General Motors of Canada Company and Stellantis (FCA Canada Inc.).

Canada's automotive industry is responsible for over \$13 billion in annual economic activity, 117,000 direct jobs, and an additional 371,400 jobs in aftermarket services and dealership networks in 2020. The industry is Canada's second-largest export sector with \$36.5 billion in exports in 2021.

The CVMA has been a strong supporter of the Canadian Automotive Service Information Standard (CASIS) since its inception twelve years ago. CVMA members are industry leaders providing vehicle repair information and tools to the aftermarket at a level equivalent to their respective independent authorized dealers to ensure Canadians' vehicles are repaired to OEM specification, to the benefit/protection of the consumer.

Over the past few months our members have reviewed and submitted recommended updates to the CASIS website to ensure technicians have up-to-date links to our member's respective technical information portals. Regular CASIS task force meetings provide an opportunity to bring forward details about any issues being encountered by the aftermarket for further study and to collaborate on solutions.

Safety is automakers' number one priority and OEMs are responsible to ensure vehicle safety systems comply with the Motor Vehicle Safety Act (MVSA). Vehicle safety technologies provide societal benefit – they may save lives - including that of the driver, other passengers, and the surrounding environment including other motorists or pedestrians, for example.

Vehicle emissions systems must also comply with federal regulations under the Canadian Environment Protection Act (CEPA). Modification to a vehicle's emission system may put a sensor out of alignment resulting in a compliance issue due to increased emissions and may also affect fuel consumption.

Allowing unrestricted access to vehicle safety and emissions system software that is not required to complete a repair introduces significant compliance and safety risk in the event a modification results in a system not operating as originally designed. CASIS ensures that repairs are done safely and in compliance with MVSA and CEPA, among other regulatory frameworks applicable to OEMs.

Cybersecurity is another top priority for industry and data protection and data privacy are embedded from the earliest stages of product development. OEMs invest and include security measures beginning at the design process and throughout the automotive ecosystem and abide by rules that govern cybersecurity management.

Circumvention of a vehicle technology protection measure (TPM) and the modification of vehicle system firmware may undermine cybersecurity protections making vehicles more vulnerable to hacking. Automated vehicle and connected vehicle technologies, driver assist systems and the transition to an electric fleet and charging infrastructure require an increasingly vigilant approach to cybersecurity.

As noted in the 2020 Transport Canada report, "*Canada's Vehicle Cybersecurity Guidance*", "a cyber security breach, whether deliberate or accidental – could have adverse consequences such as compromising vehicle safety, unauthorised access of confidential information, and vehicle theft among others."

Context is critical. The consequences of allowing unrestricted modification of motor vehicle firmware and certain software are more serious than compared to other consumer goods, which we understand are the intended focus of this bill.

As the committee continues its' study of C-244, the '*right to repair*' Bill, we strongly recommend the committee hear from a **cybersecurity expert**, such as a CSIS or CSE representative, to receive a briefing about cybersecurity threats as related to vehicle security safeguards, including measures to protect the integrity of vehicle systems.

We also recommend inviting an appropriate **Transport Canada** official who could provide input to the committee from a road safety and motor vehicle regulation perspective as well as an **Environment and Climate Change Canada (ECCC)** official who could speak to the importance of vehicle system integrity related to fuel consumption and emissions compliance.

In closing, the CVMA remains committed to the CASIS model which has been working for over a decade and that may serve as a model for other industries to adopt. We urge

¹ Page 8: https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

the committee to continue its detailed review, hear from vehicle cybersecurity and safety experts and continue to connect with the CVMA as the study moves forward.

I would be pleased to address your questions.