March 17, 2021

Automated Vehicles Team

Law Commission, 1st Floor

Tower, 52 Queen Anne's Gate

London, SW1H 9AG.

Re: Automated Vehicles: Consultation Paper 3 – A regulatory framework for automated vehicles.

BlackBerry Corporation respectfully submits these comments in response to consultation of the Law Commission of England and Wales and the Scottish Law Commission on the future Regulatory framework for automated vehicles (framework). BlackBerry is grateful for the opportunity to contribute to an important UK government effort to enable safe and effective deployment of automated vehicles on Britain's roads.

BlackBerry is a global leader in vehicle cybersecurity. Our secure software is embedded in more than 175 million vehicles. 9 of the top 10 automotive OEMs, and 7 of the top 7 automotive Tier 1s use BlackBerry to secure their digital instrument clusters, connectivity modules, handsfree systems, and infotainment systems.

About BlackBerry's work in intelligent mobility sector.

BlackBerry offers a broad range of safety-certified and secure embedded software, development tools, cybersecurity products and services to safeguard vehicle and road infrastructure from cyber threats. These include:

- The most secure microkernel-based operating system (OS) and hypervisor for the automotive market (BlackBerry QNX). Both are safety-certified to the highest level (i.e., ISO 26262 ASIL D).
- A cloud-based static binary code scanner to identify and evaluate software vulnerabilities and produce a software bill of materials for vehicles (BlackBerry Jarvis).
- Over-the-air software update management services.
- Security credential management systems for V2X communication, code signing and other applied cryptography and key management solutions (BlackBerry Certicom).

BlackBerry's Advanced Technology Development Labs (BlackBerry Labs) investigates, incubates, and facilitates technologies specifically designed to safeguard vehicle and road infrastructure from cyber threats and related vulnerabilities. BlackBerry's cybersecurity consulting practice provides automotive OEMS, supply chain manufacturers and backend infrastructure providers for connected vehicles with threat intelligence & modelling, cyber risk governance strategies and advice, software and hardware reverse engineering, training, security assessments, penetration tests, and incident response services. BlackBerry also offers UNECE WP.29 regulation readiness assessment services for OEMs and Tier 1s. BlackBerry provides subject matter expertise to advance standards and regulation development. BlackBerry actively participates in international standards development through the Standards Council of Canada, ISO, SAE, NIST, ETSI Cyber, UNECE and other regulatory and standards bodies. BlackBerry is actively engaged in the development of new products and services to secure the next generation of vehicles and road infrastructure such as AI-based endpoint protection and endpoint detection and response technologies that protect vehicle software (BlackBerry Cylance).

We are pro-actively incorporating state-of-the-art security technologies and practices into our solutions to match (and exceed) emerging cybersecurity standards (i.e., ISO/SAE 21434, ISO 24089 etc.). BlackBerry team is actively involved in providing subject matter expertise to inform industry-wide cybersecurity legislative, standards and regulatory development in Canada and internationally.

Based on BlackBerry's experience and expertise we are answering in the below remarks the following consultation questions:

Question 5.120 - We welcome observations on how automated vehicles can be made as safe as reasonably practicable.

1. **Ensure highest safety practices through software certification.**

There has been an explosive increase in software-dependent features coming to cars. While true for any modern car, software is even more fundamental for automated vehicles where software predominates and will be the main enabler of automated decisions.

An autonomous system requires software that is reliable and safe. Yet a car's self-driving system uses different software technologies than normal automotive embedded software. For instance, machine learning algorithms often use the Python programming language and machine vision systems usually need graphics processing unit (GPU) programming.

Automakers traditionally outsourced vehicle hardware and software development to others. This model however failed as soon as software became a defining and differentiating feature. Since then, automakers have decided to design and own the car's software so it can be built, fixed, extended, and maintained over the life of a car and across different product lines. Now that automakers are responsible for software, they're carefully selecting components, designing how it should interact, and planning for its adaptation and evolution

It's important to note that these new developments mirror a software-first strategy and companies use software to solve old problems in car design, manufacturing, and customer appeal. However, traditional automakers have not cultivated the software expertise needed to support this new direction. And while new automakers may have software competency, they are lacking automotive-specific domain expertise.

BlackBerry respectfully suggests that to help ensure safety in self-driving systems, the Law Commission proposes that the upcoming regulatory framework contains guidance that will enable the automotive industry to meet highly rigorous software safety requirements.

We recommend requiring the use of tools that enable automakers to streamline their safety certification processes and meet aggressive start of production dates with a combination of pre-certified software and unique safety expertise by utilizing market leading safety assured operating systems.

Additionally, building today's autonomous car is not just about embedded development experience, it's also about the knowledge of certification processes, safety requirements, and preeminent safety expertise. Most automakers' in-house engineering staff may not have the necessary experience with the difficult process of certification.

BlackBerry respectfully suggests that one of the ways to enhance safety of automated vehicles is to use regulatory authority to encourage focus on safety through creation of a safety framework. Such framework should contain a variety of approaches and mechanisms, including a robust safety assurance and functional safety programs and engineering measures. **A particular area of focus should be to ensure that automotive industry uses market leading safety assured operating systems and safety-certified software through engineer training, safety assessments,**

development methodologies, as well as custom software components that meet special safety and security requirements in automated vehicles.

2. **Secure automated vehicles' cloud connection.**

With any connected vehicle, and even more so for automated vehicles, securing cloud communications is paramount. However, the interactions with cloud-based servers and their effects on the vehicle need to be considered from both a cybersecurity and safety perspective. With automated vehicles for instance, the regular updating of maps on the vehicle to ensure continued safe driving in an ever-changing road landscape is of utmost importance. Furthermore, updates to vehicle software code (usually referred to as "software updates") are just as equally important e.g. to ensure vehicles have the most up to date remediations to remain secure in an ever-evolving cybersecurity landscape. Predominantly, software updates are delivered to vehicles from cloud-based servers via "over-the-air" (OTA) mechanisms (e.g., cellular networks), but they can also be delivered to vehicles via wired connections e.g., Ethernet, OBD-II port, USB interface, etc.

BlackBerry would like to highlight one area of software updates and recommend that the Commission considers this in its recommendations for the upcoming regulatory regime. The reasoning for this is explained below.

Today, people generally rely on software updates for their phones, laptops, and other connected devices. These updates allow the fixing of bugs, patch security vulnerabilities, add new features, and improve customer experience to keep products running optimally. Software update expectations have also carried over to the vehicle. Furthermore, vehicle software updates can enable an increase in perceived value after their purchase, for example by offering more functionality than when they were first sold to the vehicle owner, as well as generate brand loyalty. Therefore, vehicle manufacturers are already increasingly reliant on software updates to help differentiate their products in a crowded and competitive market.

However, unlike phones and laptops, vehicles can present a significant safety hazard to their users and others (e.g. other road users) if software updates are incorrectly applied and/or mismanaged. Such a safety concern is further exacerbated for those vehicles that have automated driving functionality.

In all vehicles, software updates must be performed safely and securely, and be sufficiently tailored to the vehicle to which they are to be applied.

Whilst most software updates can be applied seamlessly without the vehicle owner being aware, other software updates are impossible to be done in a seamless manner, and as such, those updates must be prevented from being carried out whilst the vehicle is being used and the vehicle prevented from being used until the updates have completed.

Furthermore, some updates to a vehicle require re-calibration to vehicle systems after an update has been applied e.g., an update to a vehicle's braking system may need the brakes to be recalibrated. As such, those types of updates must be restricted to being carried out only by skilled individuals (e.g., mechanics).

Finally, it must be ensured that updates that have failed to be applied to a vehicle do not "brick" the vehicle. That is, a vehicle needs to be able to be put back to its original state before the failed update was attempted, or at the very least, into a safe state to allow for trouble shooting and fixing (e.g., by a skilled individual). Such a "bricked" state is not only an inconvenience for a vehicle user but could also be a safety hazard if the state of vehicle systems is left in an unpredictable and/or erroneous state.

BlackBerry respectfully suggest that the Commission recommends mandating in the upcoming framework the use of tools and services enabling software updates that are automotive-specific and enable safe and secure updates.

Question 19 - (2) "Should the scheme also deal with cybersecurity?"

Based on BlackBerry's experience, it is fundamentally almost impossible to separate safety and security in automated vehicles. **In BlackBerry's position, the upcoming scheme should also deal with cybersecurity because cybersecurity has significant impacts to AV safety as explained below.**

Automobiles have evolved into sophisticated, multi-layered digital software systems that contain over 100 million lines of code and connect to thousands of devices and external networks via a variety of communication technologies (e.g. cellular, V2X, Wi-Fi, Bluetooth, USB, OBD-II, EV chargers).

As the complexity and scale of software in road transportation and infrastructure grow, so does the attack surface. A cybersecurity attack that intervenes with the functional safety of a vehicle could have fatal consequences. The issues of safety and security must be considered in tandem as cybersecurity is the most important building block in ensuring safety of automated vehicles.

These vehicles will face a complex network of internal and external interactions, which will include things like roadside traffic management and wider infrastructure. These dependencies present a wide attack landscape which could have a direct impact on the safety of the vehicles, its passengers, and its surroundings.

New vulnerabilities to vehicle cybersecurity are discovered daily. There are multiple entry points for cyber actors to attack road transportation, and many attractive targets for threat actors. These include:

- remote attacks that take over critical vehicle control functions threatening passenger safety,
- direct access attacks that exploit cybersecurity vulnerabilities in on-board diagnostics, connected alarm systems, infotainment systems, telematics, and electronic control units; and
- cyber exploits that steal personal information flowing between connected cars, infrastructure, and the cloud.

The threat landscape contains the following subset of issues that can impact cybersecurity and in turn, safety of vehicles and individuals:

- **Endpoint vulnerabilities for autonomous vehicles and connected infrastructure**

Autonomous vehicles and road infrastructure are equipped with a range of connected sensors that help vehicles navigate roads, detect other vehicles on the road, stop for pedestrians, and react to unexpected developments. These sensors, while essential to the functioning of vehicles, also represent additional attack surfaces against which malware can be deployed. Exploits can occur through remote access (e.g., internet, cellular), local wireless (e.g., Wi-Fi, Bluetooth) and physical connectors (e.g., Ethernet, OBD-II, USB).

- **Cybersecurity and privacy**

As vehicles become hyperconnected, they will collect and analyze vast amounts of personal data (including real-time location data), which can be exploited, raising important privacy concerns. To protect personally identifiable information, the vehicle as an endpoint must be secured. Mass privacy breaches have occurred in many industry sectors and are inevitable in the automotive sector in the absence of preventive measures and standards. The protection of personally identifiable information should be a key consideration for public policy related to vehicle cybersecurity.

- **Software and supply chain vulnerabilities**

The increasing complexity of the vehicle software supply chain makes it difficult to gain insight into vehicle software composition (Software Bill of Materials – SBOM). In the absence of regular software updates (e.g. via OTA mechanisms) and SBOM checks, software with existing vulnerabilities could be exploited leading to critical failures.

- **Mobile application security vulnerabilities**

Mobile applications regularly fail basic security tests (Gartner). Malicious actors could exploit these flaws to manipulate vehicle control functions. This risk was demonstrated on a Nissan Leaf in 2016 when security testers gained unauthorized remote access to the heated steering wheel, seats, fans and air conditioning.

There are additional considerations that BlackBerry would like to offer to support the argument that cybersecurity should be included within the proposed scheme.

There is a trend in the automotive industry (mainly due to the skills shortfall) of involvement of safety experts in cybersecurity related areas of work such as assessing the cyber security risks of the vehicles, including its software and infrastructure. If the proposed scheme keeps the two areas aligned and considered in tandem, experts can maximize the impact of their work, by ensuring efforts are aligned, prioritized, and address the interconnected nature of safety and security risks to vehicles.

Equally, new regulations such as those passed by UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) will empower vehicle certification agencies to opportunity to reinforce focus on safety in vehicles. If safety and cyber security and included under the proposed regulatory scheme in the UK, agency experts will be enabled to comprehensively consider safety and security as both areas of focus aim to achieve some of the same objectives; particularly understanding of areas like the supply chain risk, software vulnerabilities, and interaction of individual components of vehicles.

Based on these considerations BlackBerry respectfully suggest that the upcoming scheme should also deal with cybersecurity because cybersecurity has significant impacts to AV safety.

We remain at your disposal for any questions you may have about our response or our work. BlackBerry is looking forward to working with the UK government on ensuring safety and security of automated vehicles.

Respectfully,

Klara T. Jordan
Director, UK Government Affairs & Public Policy
Mobile: [redacted]