



Memo

To	FIGIEFA/AFCAR	From	Dr. Johannes Graf Ballestrem, LL.M. johannes.ballestrem@osborneclarke.com
Cc	Ms Sylvia Gotzen	Office	Innere Kanalstr. 15 D-50823 Köln
Matter Nr.	0857182/G2529133	Date	1 st July 2016

FIGIEFA/AFCAR Position on RMI

This memo is about to enquire AFCAR's proposals and position on the access to Repair and Maintenance Information (**RMI**) and the draft Vehicle Type Approval Framework Regulation in connection with IP rights.

In our discussion about the requirements for freedom to operate as independent operators in the aftermarket we i.a. covered the question of Intellectual Property (IP). We understood that the Vehicle Manufacturers (**VM/OEM**) raise concerns that their IP is "eroded" by too far reaching access rights of the Independent Operators (**IOs**). This is an understandable concern but considered in detail we indeed see rather limited effects on the IP of the vehicle manufacturers, if at all. We therefore would like to warn of a too broad and very general use of the "IP argument" as a sledgehammer against our proposals as submitted with the draft AFCAR Position Paper of 2 June 2016.

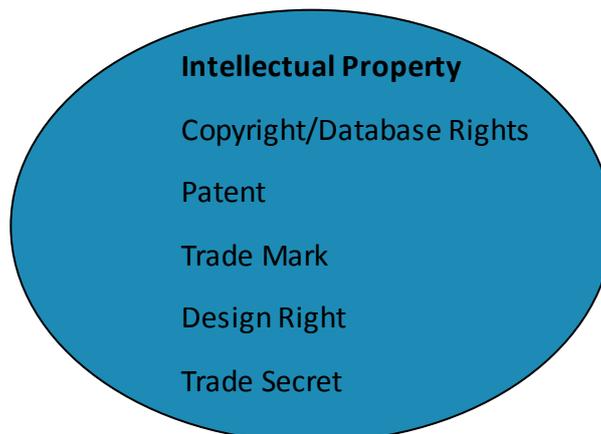
We would like to take the opportunity to briefly follow up on the main IP aspects with the below memo. Starting with a summary of our general remarks (A) we map exemplary provisions of our proposal against their alleged IP impact (B).

A. General remarks

1 IP and IP Rights

First of all, we would like to highlight that there is clearly a difference between IP in a broad sense and the defined IP rights. IP rights are the rights given to persons for the creations of their minds. They usually give the creator an exclusive right to use his/her creation for a certain period of time. They are deemed to honour distinct human and industrial achievements and require that the respective legal and/or administrative preconditions for obtaining the specific IP

right are met in the individual case. For example a patent is granted for a technical solution which is new and inventive while software as such is not protectable by a patent.¹ Software algorithms may be protected by copyright but only if the software reaches a certain level of original creation. The copyright law can neither capture the cooperation between machines and software nor the technical problem-solving strategy as such. It protects the source code as well as the object code of the software that is used. The programming code and functionalities on the other hand are not protected by copyright.² Data as such is as a rule not protectable by IP rights. It has to be noted that by far most of the vehicle generated measurement data is either raw data or information (information = processed raw data) which is required for repair and maintenance purposes of the Independent Operators is not protected by any IP rights.³ IP rights aim to protect the results from creative or inventive efforts, but they have a limited scope of application. When relying on claims from IP rights the owner of the IP right has to show that the respective requirements of the right are fulfilled, e.g. by filing a patent or by evidencing the creativity of a copyrightable works. The below drawing provides an overview on Intellectual Property including Know-How.⁴



If any arguments on IP rights were raised, it should therefore be carefully analysed for each object whether it is indeed protected by a specific IP right or not. For example a technical drawing or picture comprised in RMI can be copyright protected as human creation. Consequently the user requires a license if he wants to use the drawing one by one. By contrast machine generated data from the car being a result of interaction of software and car hardware is not

¹ Cf. Art 52 (2) c) EPC.

² Cf. ECJ, judgment of 2 May 2012 – C-406/10 SAS Institute Inc. / World Programming Ltd.

³ So called “data license agreements” which can be seen in the sector are often not what they pretend to be (an IP right-license) but a mere factual allowance providing factual access to the proprietary good “data” in the hands of the OEM. The term “license” is often misunderstood in this context.

⁴ Excerpt from: Bright Idea Scotland, c/o Targeting Innovation Ltd, <http://www.slideshare.net/hpicinnovation/ken-marr-targeting-innovation-ip-presentation>.



protected by any (software) copyright.⁵ Consequently there cannot be a general claim that IP rights stand against the Independent Operators access neither to vehicle generated measurement data nor to RMI. Moreover and more importantly, an IP right (e.g. a patent) is not consumed by its use. Usage of the IP right does not mean that the IP right as such is denied. The question is rather due to which justification the IP right is used (voluntary or compulsory license). For example: Assuming that above interaction between software and car hardware could be protected by a process patent and assuming further that the processed data stemming from that calculation could be protected as a “process result”, the usage of this information for diagnosis of the car condition would by no means put into question the patent protection of the process as such. Same as in other constellations of “essential patents” the only question would be whether the OEM needs to tolerate usage of its patent for free or against payment of a reasonable royalty under FRAND terms.⁶

2 IP in a wider sense

When understanding IP in a wider sense such as covering general business secrets and internal know-how, it is understandable that the OEM invoke interests to protect their internal know-how from disclosure to the public. This argument is at first glance valid for veritable trade secrets. However, it is not an argument based on IP rights and also not based on the principle of rewarding innovation. The threshold for Know-How protection is significantly different from IP right protection. Most importantly, Know-How protection does not cover any information which is not confidential, e.g. when this information is available to third parties anyway.⁷ For example: The data and information which is made accessible to a large number of authorized dealers in the network of the Vehicle Manufacturer (such as the RMI) is no business secret already for the reason that it is not kept confidential. The same applies to data and information which can be acquired independently by reverse engineering, e.g. by dismantling the product. For example, data and information (= machine processed data) which can be acquired by monitoring the functioning of an OEM diagnosis tool is consequently not protected as a trade secret.

3 Reverse engineering is a lawful business practice

Article 4 of the EU trade secrets directive re the “Lawful acquisition, use and disclosure of trade secrets” further explicitly confirms the legality of reverse engineering performed by the Independent Operators. Article 4 expressly clarifies that independent discovery and reverse engineering are legitimate means of acquiring information.

Art 4 (1) (b) reads:

⁵ Cf above fn 2.

⁶ Cf the ECJ ruling of 16 July 2015 C-170/13 in re Huawei vs ZTE. See below section C.

⁷ Art 2 (1) a) Directive 2013/0402/COD of the European Parliament and of the Council (trade secrets directive) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.



1. *The acquisition of trade secrets shall be considered lawful when obtained by any of the following means:*

(b) "observation, study, disassembly or test of a product or object that has been made available to the public or that it is lawfully in the possession of the acquirer of the information;"

Recital 10 explicitly addresses the need to avoid any exclusive effects from the know-how protection. In other words: The Know-How shall not become an exclusive IP right.

"In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right on the know-how or information protected as trade secrets. Thus, independent discovery of the same know-how and information remains possible and competitors of the trade secret holder are also free to reverse engineer any lawfully acquired product."

However, some OEM seem to block the use of the OEM tool stating that the OE tool may only be used in a workshop environment/workshop level and then prevent (blocked access or online link) the use of the OE tool by independent tool producers for comparative purposes.

As confirmed by the trade secrets directive, reverse engineering cannot be perceived as an "illegal practice" of Independent Operators if they use data and the Original Equipment Manufacturer's tools in the course of reverse engineering in order to check the functionalities and create with their own know-how their own diagnosis tools. To this end, it is allowed to use OEM diagnosis tools in course of the reverse engineering process. The deviating practice of OEM to bloc Independent Operators from such activity must accordingly be perceived as anticompetitive and without justification in itself.

B. IP Impact of proposed clarifications and amendments

1 "Normal RMI"

AFCAR's minimum demand is that the current regulation on access to RMI is maintained. It is safe to say that the normal RMI, although some of it might be copyrighted, does not raise new concerns. The current EU legislation already provides for a "compulsory licensing" against payment of a reasonable royalty for the RMI. Since the RMI is made available to the authorized dealers, the OEM can also not raise any new concerns about alleged confidentiality of this information.

2 Access to in-vehicle raw data in combination with RMI:

As a further minimum requirement for competition on the aftermarket access to the in-vehicle data, either through the current standardised OBD interface or via wireless communication



technologies is necessary to allow Independent Operators to provide repair and maintenance services to consumers.

a) OBD interface

Presently the OBD interface (16-pin connector in the car) is the standardised access to the electronic systems and components. However, in future data will be increasingly exchanged through direct access by wireless communication technologies instead of the OBD. It is therefore important to note that this access must be kept open for the Independent Operators. For example: If the OEM decides to reduce the data available or to renounce access the OBD connector and only allow communication with the car through wireless communication technologies the Independent Operators should be equipped with sufficient means (e.g. the Wireless communication technologies password and other settings if necessary) to still access the in car data, free of charge and without competitive monitoring This usage is not qualitatively different from accessing the car via the OBD connector and therefore should not raise new concerns in terms of IP rights and Know-How or introduce new barriers or costs. A wireless communication technology access code is not protected by copyright or other IP right. Moreover, the access code should be at the disposition of the car user anyway to support their freedom of choice for competitive repair and maintenance services.

b) Interpretation of the car data

In order to understand the in-vehicle raw data it must be combined with the Vehicle Manufacturer-specific RMI in order to allow a correct interpretation of the raw data (such as is a value "good or bad"). Raw data are the messages that are exchanged between the vehicle ECU (Electronic Control Unit) and the diagnostic tool through the OBD connector. They exist in form of bytes and bits. By making specific requests using the diagnostic tool for example a specific parameter or diagnostic trouble code, the data can be analysed and compared with RMI. The data can be in a range of formats, electrical values i.e. volts/resistance, or specific values i.e. temperature/pressure. With this raw data the development of an aftermarket tool for the purpose of repair and maintenance can be accomplished.

c) processed data from the car

To our knowledge, the machine generated data and the machine processed data (information) from the car are not protected by any IP rights. In Europe patent protection is usually not available for data as such since patent protection requires the solution of a technical problem with technical means, i.e. usually a hardware steering or improving functionality.⁸ Only in exceptional cases one may consider protection for information which is generated by the invention of an innovative process patent. The data as such can also not be protected by copyright since copy-

⁸ In this the European approach significantly differs from the US where patents for business methods and software implemented inventions are granted more extensively.

right always requires a human creation. Machine generated information is therefore not protectable. The measured values from the electronic control units of the car (ECUs) are also not aggregated and stored. If the data is stored at all (usually in a short time memory) it is stored in hardware of the customer since the customer acquired ownership in all components of the car, including the ECUs and the memories.⁹ An individual property right in data does not exist. The proprietary attribution of data is yet governed only by factual access to the data not by a legal allocation. Therefore, the OEM can also not claim that it is “their data” which is generated and processed in the car.

d) Increasing use of software and on-board diagnosis

In the future more software will be applied in the car as the trend is to process and evaluate data from the ECUs already inside the car before its transmission to external display devices such as diagnosis tools or mobile apps. However, the legal assessment remains identical. There is no claim that the processed data (information) is covered by any software or other copyright. The information is a product result of the use of the software but not software in itself. Software protection does also not extend to the process result created by application of the software. The software copyright only protects against a one by one copying of the software (source code) onto another device or against not permitted use. The use in the car happens entirely within its purpose designation. The rights of the OEM into this software are exhausted after the first sale of the software together with the car and subsequently exhaust with every update to the customer.¹⁰ The customer is therefore entitled to use the software accordingly. By contrast the Independent Operators do not need and do not copy the OEM software onto their own testing and diagnosis devices. They simply need the result of the data which is processed by the OEM software.

e) In car data is not protected as a trade secret

The data and information in the car are not protected as trade secrets either. First of all the information is accessible by using the designated interface irrespective whether this is the classical OBD or wireless communication technologies connection in the future. Secondly, it is not in the possession of the carmaker but in the possession of the car user. Thirdly, it is not created by the OEM but after sale by the user of the car. The trade secrets directive does not protect know-how which either belongs to no one or to another party than the party who claims the trade secret. It neither protects know-how which is created independently by a third person without any obligation to maintain this information confidential. The car user clearly does not undertake to keep the information in his car confidential since he has a vital interest to use it i.a. for instructing an independent repair shop or to get road assistance from the available local operators. By contrast the Independent Operators do not request disclosure of any confidential source code of

⁹ This could be potentially different if the customer only rents the car from the OEM but this is no relevant practice.

¹⁰ Judgment of the ECJ of 3 July 2012 - Case C-128/11 – Used Soft.



software which is running on the car components. The Independent Operators use their own software solutions on their diagnosis devices. The demand for interoperability of software is also addressed in article 6 No. 1 of the Computer Programs Directive¹¹ 2009/24/EC. We therefore do not see valid grounds on which the OEM can invoke trade secrets against access to the in car data.

3 Use of source code/algorithms for the purpose of development of specific test procedures

Independent test equipment manufacturers currently apply their own diagnostics know-how and do not need to know the Vehicle Manufacturer's software and the source code of software. However, the technical preconditions are becoming increasingly complex and already today some of the processes involved when wanting to develop specific test procedures/tests steps cannot be completed because the OEM algorithms are part of the specific test procedures/test steps, and are therefore needed. As vehicles become more connected in the future, specific routines will be carried out remotely. We therefore suggest that while the IP and/or trade secret protection for OEM software is respected the OEM shall make such software and source code/algorithms available against payment of a reasonable royalty and on basis of adequate license agreements which may include non-disclosure and other common provisions in order to safeguard their confidentiality interests.

C. Question of reasonable royalty

As pointed out the problem of determination of a reasonable royalty for RMI and diagnostic information is indeed an important issue which has not yet been resolved. Since in the particular field no suitable case law exists yet, a reference can perhaps be made to the determination of so called FRAND royalties in cases involving usage of standard essential patents. Also in these cases, courts acknowledged the hurdles to determine which royalty is market adequate and which is excessive. Nevertheless, they finally resolved this issue with guidance from the CJEU.¹² The major practical difference is, however, that in the FRAND cases the patent is already used and no further activity by the patent owner is needed. In this scenario the situation differs from the situation at hand. Despite the Euro 5/6 regulation the OEM still has the means to claim licence fees which are prohibitive and thereby factually exclude the Independent Operator from that information since the Independent Operator is dependant from the factual data provision of the OEM. This situation needs to be tackled in the future by an adequate mechanism for controlling the OEM's royalty requests. Our recommendation is that for the provision of RMI only an administrative fee should be owed to the OEM which compensates the administrative efforts of the data supply. The reason is that the OEM has to create and store this data in an ordered form anyhow as this is a mandatory prerequisite for selling his cars. There is no need to reward

¹¹ Directive 2009/24/EC of the European Parliament and of the Council.

¹² Cf the ECJ ruling of 16 July 2015 C-170/13 in re Huawei vs ZTE.



him for creation of such data. Innovative efforts of the OEM will not be influenced if he receives no additional remuneration for making the RMI available to the Independent Operators.

By contrast if the OEM makes IP protected software available to the Independent Operators a licence fee may be requested. However, the royalty should be proportional to the fees requested in the authorized network of the OEM. For example if software updates are provided to authorized dealers free of charge they should be also made available to the Independent Operators free of charge. If software is provided to an OEM tool manufacturer against a licence fee, the fee requested from the Independent Operators should be fair reasonable and non-discriminatory compared to the conditions of the contract between the OEM and the OEM tool manufacturer. In order to be non-discriminatory the royalty fee must be in any case taking into account the intended scope and intensity of use of the respective Operator. The burden of proof for proportionality of the requested licence fee should be with the OEM.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Dr. Ballestrem'.

Dr. Johannes Graf Ballestrem, LL.M.
Rechtsanwalt