CIPPM Centre for Intellectual Property Policy & Management

Jean Monnet Centre of Excellence 2018-2021 for European Intellectual Property and Information Rights

CIPPM / Jean Monnet Working Papers

No. 07-2020

Vehicle data controls:

Balancing interests under the Trade Secrets Directive

Freyja van den Boom

November 2020

Bournemouth University

Co-funded by the Erasmus+ Programme of the European Union

The Centre for Intellectual Property Policy and Management of Bournemouth University is a Jean Monnet Centre of Excellence for European Intellectual Property and Information Rights (2018-2021), co-funded by the Erasmus+ Programme of the European Union.

This Working Paper Series is peer reviewed by an Editorial Board led by prof. Ruth Towse and prof. Roger Brownsword.

Vehicle data controls -

Balancing interests under The Trade Secrets Directive.

Freyja van den Boom

PhD Candidate, Bournemouth University

_____

Email: fvandenboom@bournemouth.ac.uk

Abstract: As vehicles are becoming more connected and increasingly autonomous, new opportunities emerge to use the data vehicles generate. Telematics is an example of how data generated through vehicle use, enables insurers to develop more accurate risk profiles and adequate premiums. Having access to vehicle data provides those who hold the data with a competitive advantage which in addition to increased concerns over privacy, have led to initiatives to control vehicle data access. The European Parliament has called upon the Commission to publish a legislative proposal that ensures a level playing field on access to in-vehicle data and resources, protecting consumer rights and promoting innovation and fair competition. To contribute to the discussion, this paper analyses the potential for vehicle manufacturers to control vehicle data through trade secret protection. Neither the Trade Secrets Directive nor the General Data Protection Regulation provides clear guidance on how to decide in cases of conflicting interests. As such this paper concludes by arguing that holders of trade secrets should allow access to data subjects to personal data, however they may impose measures on data recipients to make sure their secrecy is kept.

Keywords: Trade secrets; Vehicle data; Telematics; GDPR; Data portability; Data access rights

Introduction

As vehicles become more and more advanced through built in sensors and communication technology they can collect and communicate large amounts of data. This data not only includes information about the functioning of the vehicle, which is necessary for the after-service repair market, but can also be analyzed to reveal how, when and where the vehicle is driven. Some examples of what information can be obtained from the data collected through the use of modern vehicles include:

- Driver profile information *(driving mode, use of seatbelts,number of trips taken, the number of kilometers travelled and in what conditions, how and where the car was charged)*
- Vehicle location *(latest destinations entered into the navigation system, GPS, last parking locations)*
- Maintenance information *(engine revolutions, mileage, status of vehicle lights, fuel consumption and level, tyre pressure)* [1]

Not surprisingly motor vehicle insurance companies have shown an interest in obtaining this data as research shows its use can help improve their risk assessment of drivers and subsequently determine premiums more accurately.[2] To provide for 'fairer' insurance, improving driving and road safety are just some of the benefits considered when access to vehicle data is provided to parties other than the vehicle manufacturer. However, concerns about the risks of (uncontrolled) access for privacy, competition and security have led to a debate on who should have access and control over the data vehicles generate.[3] Vehicle manufacturers on the one hand consider themselves best positioned to control the data, whereas after-market service providers, consumer representatives and insurers argue this leads to data monopolies, unfair competition and would not respect the rights of consumers over personal data. [4]

Where previously the discussion on vehicle data access focused on who 'owns' the data generated through the use of connected vehicles, several reports have led to a general consensus on the absence of a property right for data.[5] As a result the attention has shifted towards data access and control.

There are several lawful means that in practice may have the same results for protecting the data from uncontrolled access by those who hold the data. In the case of connected vehicles the vehicle manufacturers could limit physical access by design, reducing what data is available through the On-Board Diagnostics (OBD) port to only what is minimally required to comply with legal obligations.[6] Another way would be for them to rely on trade secret protection. To what extent trade secret protection can and will be used to control access and use of vehicle data in practice remains to be seen, especially given that most processing of vehicle data falls under the scope of the General Data Protection Regulation (GDPR).[7]

As both the Trade Secrets Directive and the GDPR only came into force recently there is legal uncertainty to what extent access to vehicle data can be controlled through trade secrets protection.[8] The purpose of this paper is to contribute to the discussion with an analysis and conclusion that *vehicle manufacturers can rely on trade secrets protection to control access and use of vehicle data,* This paper is organized as follows: on the assumption that vehicle data qualifies as personal data and the data can be processed lawfully either based on the driver´s consent or contract, the following section provides a critical analysis of the EU Trade Secrets Directive, looking at the scope and main conditions for trade secrets protection in relation to access rights to personal data. This paper concludes by proposing that trade secrets protection can play a role for vehicle manufacturers to control who can have access to vehicle data, and under what conditions.[9]

The EU Trade Secrets Directive

On 8 June 2016, the European Parliament and the Council adopted the Trade Secret Directive (Directive). [10] Stronger protection was considered necessary given the importance of trade secrets for innovation, competition and research.[11] Despite criticism on the Directive, the EU harmonization of trade secrets protection has generally been welcomed. [12]

The Trade Secrets Directive harmonizes the definition of trade secrets in accordance with the existing internationally binding standards.[13] Article 2(1) of the Directive states that: 'Trade Secret' means information which meets all of the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret;
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

The Directive does not create an exclusive right to know-how or information, meaning that independent discovery of the information under trade secret protection is lawful. [14]

Vehicle data under the scope of protection

The first element states that a trade secret applies *to information*. Recital 14 further clarifies the need for a homogeneous definition of a trade secret without it being restrictive in that it can cover know how, business information and technological information. [15] What is not covered is *trivial information* and the *experience and skills gained by employees in the normal course of their employment*.[16] Important to note here is that neither technical data nor personal data is excluded from trade secret protection.[17]

Most vehicle data is considered *technical information* which according to the recitals fall

under the trade secrets definition. Much of the data that vehicle manufacturers would want to protect is data generated and communicated from the sensors, cameras and microprocessors in the vehicle. Manufacturers will be hesitant to share this data as it can be used by their competitors to gain insights into the functioning and design of the vehicle. [18] Furthermore, *customer information*, is mentioned, which can be obtained from vehicle data.

The second requirement is that the information *has value* because it is kept secret.[19]
The value for a vehicle manufacturer in not sharing vehicle data lies in the fact that it gives them a competitive and strategic advantage when they can keep their competitors from obtaining the information without having to invest themselves resources for example in developing the technology to obtain the information. By monetizing (access to) vehicle data they can obtain a return on their investment. [20] The proliferation of data marketplaces where through contractual agreements with data providers and users the data is shared illustrates the value of (access to) data especially when this constitutes personal data.[21]

Thirdly the information must not *be 'generally known among or readily accessible within the circles that normally deal with the kind of information in question".* [22] In line with the purpose of trade secret protection to enable people to derive profit from their creation or innovation the relevant circle includes who could use the information to gain a competitive advantage from its disclosure or use.[23] For vehicle data, this would include other vehicle manufacturers and aftermarket product and service providers such as repair and insurance companies. One could argue that the vehicle owner/driver is excluded from the relevant circle because they normally don't use vehicle data in a commercial context. [24] As secrecy is not absolute it depends on the circumstances whether information has become generally known or readily accessible. [25]

Data as Trade Secrets are not obtained just by looking at the vehicle. One must either have permission to access the vehicle, vehicle communications and/or data storage.[26] The fact that the driver knows or would have access to the same information the vehicle manufacturer seeks to protect, does not lead to a loss of trade secret protection for other trade secret holders who have lawfully obtained the data and kept it secret. If however a competitor wants to obtain (access to) the vehicle data by having the driver submit an access request one could argue that now the data has become readily available and secrecy is lost. Until the European Court of Justice (ECJ) provides guidance, it is uncertain whether the process of obtaining information through a data subject access request falls under the scope of ´readily accessible'.

The fourth element for vehicle data to fall under trade secret protection is that the holder of the secret must take *reasonable steps* to protect its secrecy.[27] Whether this is an objective assessment looking at industry standards of practice or subjective assessment based on circumstances is not clear from the Directive. [28] In general steps include establishing internal policies on how to manage and disclose trade secrets making sure that IT security systems and technology are kept up-to-date.

Obtaining a trade secret is considered unlawful through unauthorized access to or copying of files which contain trade secrets, or through dishonest commercial practices.[29] Article 4 of the Directive states that a trade secret holder can take (preventive) measures to protect their trade secrets.[30] Vehicle manufacturers could prevent data from being accessible by closing off the vehicle access points and/or minimizing what data is communicated outside of the vehicle, and by using encryption technology.

To conclude vehicle data could fall under the requirements for Trade Secrets protection and be protected against access by vehicle manufacturers.[31] In the next section we will look at whether this is indeed possible when vehicle data to be protected includes personal data.

Limits to the rights of the trade secret holder

Notwithstanding the legitimate interests of the vehicle manufacturer in protecting vehicle data against unlawful acquisition, use and disclosure their right to protect data from being accessed is not absolute.[32] The Directive specifically limits the right of the trade secret holder in specific cases for revealing misconduct, wrongdoing or illegal activity (…). Recent scandals in the car industry about car emissions,[33] unethical testing on animals,[34] employee monitoring and surveillance[35] and price discrimination[36] illustrate this need for exceptions.[37]

Recital 34 specifically mentions that the Directive *respects* fundamental rights and *observes* the principles including the right to respect for private life, and the right to protection of personal data.*'* [38] Recital 35 goes on to state that that the rights of the data subject apply when their personal data is being processed *´when taking steps to protect a trade secret'*[39]. Note that it does not refer to the situation where the personal data *is* the trade secret. The recital furthermore mentions that the directive *should not affect* the rights and obligations, in particular, the rights of the data subject *to access* their personal data but not data portability. This may be of significance as argued for below.[40]

Despite these references prevalence of the right to privacy in case of a conflict of interest between the data subject and the trade secrets holder are not obvious.[41] To contribute to a better understanding of the scope of trade secret protection the next section looks at consequences for trade secret protection for vehicle data when the data doubles as personal data.

The General Data Protection Regulation

To the extent, trade secrets qualify as personal data processing must be compliant with the General Data Protection Regulation including that processing must have a lawful ground.[42]

Art 4 GDPR defines personal data as *"any information relating to an identified or identifiable natural person".* The GDPR makes a further distinction between personal data and personal data with a sensitive nature.[43]

Relevant for the assessment of vehicle data are the following considerations:
The article 29 Data Protection Working Party (WP29) in its opinion on personal data states that the definition must be interpreted broadly in that it covers all *information* regardless of its technical nature as long as it *relates to an identified or identifiable natural person*.[44] Information *relates to* an identifiable person if it is information about that person which is something that has to be answered for each specific data item separately.[45]

The WP29 has proposed a three-step model to analyze whether this is the case taking into consideration a) the content of the data. b) the purpose of the processing and c) the result. These elements are not cumulative. The content element is present when the information is given about a particular person.[46] Second, data can relate to a person based on the *purpose* of processing the data for example for evaluation, treatment or to influence the status or behavior of an individual. Third, when the consequence or *the result* of the use of this data has an impact on the rights and interests of a person. This impact does not have to be major as long as the person is treated differently from other people because of the processing of the data.

For data to fall under the scope of personal data is that it must not only relate to a natural person, but this person must be an identified or identifiable as a minimum threshold condition. [47]

Art 4(1) GDPR defines an identifiable natural person as *'one who can be identified, directly or indirectly, in particular by reference to an, see identifier*[48] *[...] or to one or more factors specific to the [...]identity of that natural person;'* Identifiers are pieces of information which hold a *'particularly privileged and close relationship with the particular individual*'. [49]

It depends on the context whether a specific identifier is sufficient to achieve identification.[50] Although a person's name is the most common identifier this information is not necessary as a person's identity can also be disclosed using socio-economic, psychological, philosophical and other criteria based on which a person can be categorized and attributed with decisions in a way that identifies them.[51] It is also not necessary for the required information to be held by the data controller as long as the information can be obtained using *all the means reasonably likely to be used* [..] not only by the controller but also by any other person to identify the natural person directly or indirectly. [52]

The WP29 specifically states that where the purpose of the processing implies the identification of individuals, this assumes that the controller or any other person involved has or will have the means "likely reasonably to be used" to identify the data subject.[53] When however the purpose is not identification, objective factors such as the costs of and time required for identification, and the appropriate technical and organizational measures taken to prevent identification become important to decide whether persons indeed are not identifiable through the data.[54] The test to determine ´reasonable means´ is dynamic in the way that it not only considers what the state of the art in technology is at the time of the processing but also

what future developments may bring in terms of possibilities for identification during the period for which the data will be processed.[55] The WP29 clarifies that a hypothetical possibility for identification, however is not enough for data to be considered as personal data.[56]

Only when identification is no longer possible and/or information does not relate to an identified or identifiable natural person data is not personal data and the principles of data protection do not apply. [57]

The right to access vehicle data

Vehicle data is personal data considering that in most cases the driver can be identified through the unique vehicle identification number or contracts for connected vehicle services.[58] As a consequence of vehicle data falling under the scope of the GDPR the vehicle manufacturer (as a data controller) must comply with data protection principles including respecting data subjects rights.[59] These rights include the right to access (art 15) and the right to portability of data (art 20).

The right to access

Article 15 of the GDPR states that a person has the right to obtain from a data controller access to personal data concerning him or her. Access must be provided even when this means giving access to trade secrets. At first glance, this seems to be in conflict with the requirement for trade secrets to be kept secret. [60] However, it can be argued that trade secret protection is not lost given the following considerations: As mentioned the driver is not part of the relevant circle for whom vehicle data has economic relevance. [61] Second, even if this was the case trade secrecy is not absolute. This means that information can be held by multiple people as long as it has not become *generally known or readily accessible* within the

relevant circle. Furthermore, an access request may not require access to all the vehicle data in real-time if the purpose is only to inform the driver what (type and granular level of) data is collected. [62]

As access can be given for example without the driver having the option to download a copy of the dataset in a computer readable format without being able to analyze the data the information obtained may not be ??is not sufficient to give away trade secrets.[63]

The right to obtain a copy of trade secrets

Although based on article 15 (3) a copy of the personal data under processing can be requested article 15(4) makes clear that this right (to obtain a copy) ´shall not adversely affect the rights and freedoms others´. Recital 63 mentions trade secret protection to be taken into account?? while making it clear that the consideration should not be a refusal to provide any information to the data subject.[64] Neither the Regulation nor the relevant Recitals provide further guidance, which has led to uncertainty to what extent the right to access under article 15 can be refused or restricted.[65]

In a case predating the GDPR the ECJ ruled that access could be denied, however this decision has been met with criticism.[66] If business interests prevail over the data subjects right to access and know whether their personal data is being processed this would contradict the purpose of empowering citizens. [67] There is currently another case where the ECJ is asked to consider whether access to personal data can be refused because it would 'adversely affect trade secrets or intellectual property. [68] The outcome may provide the necessary clarity on how to interpret the exception to the right to access and obtain a copy of personal data.

If the purpose of the right to access their personal data, is for the data subject to become aware and verify the lawfulness of processing one could argue that it is sufficient to show (an example of) what data is collected and for what purpose. Under art 15 GDPR, this would not require them to obtain a copy of all of the data collected (in real time) which would amount to a large volume of mostly raw sensor data that may not be of much relevance to the data subject for the purpose of knowing.[69] Article 20 of the GDPR, on the other hand gives the data subject the right to obtain a copy of the subset of personal data as well as a right to have it transmitted to another data controller.[70]

The right to data portability of trade secrets

Subject to conditions article 20 on data portability gives the data subject the right to receive a subset of personal data in a structured, commonly used and machine-readable format, and to have the data transmitted to another controller without hindrance from the controller to which the personal data have been provided. [71]

With respect to data portability the data controller is not allowed to place *"any legal, technical or financial obstacles to refrain or slow down access, transmission or re-use"*[72] Examples include fees, lack of interoperability, excessive delays or complexity, deliberate obfuscation or undue accreditation demands.[73] Furthermore, the data must be transmitted directly where technically feasible. [74] It is up to the receiving data controller to make sure data is not used without a legitimate purpose.

Data portability is not a general right, but it is limited to personal data which concerns the data subject and which they have provided to the controller based on the lawful ground of consent or on a contract and the processing was carried out by automated means.[75]

According to the WP29 the right to data portability covers the following personal data:

- data actively and knowingly provided by the data subject, such as contact information, comments and uploaded material, and
- data indirectly related to the data subject's activity or result from the observation of their behavior including data from the conduct or use of a device or service such as telematics devices.[76]

Data portability will allow the driver to request vehicle data including real-time raw data, to be transmitted from one vehicle manufacturer to another or in case of insurance from one insurer to another.[77] What is not covered is derived or inferred data, resulting from the analysis of that behavior by the data controller.[78]

Despite some discussion most agree with the extensive interpretation of what data falls under the right to data portability.[79] The European Data Protection Supervisor (EDPS) confirms that in order to be effective, the right to data portability should have a wide scope of application (…).[80] The right to data portability allows data subjects to better understand and choose what data he or she is willing to provide to get a service, and be aware of the extent to which his or her right to privacy is respected.[81] Criticism on the broad interpretation mostly considers its effect on competition and privacy. [82]

The right to refuse access

To what extent the rights of access and data portability can be limited or refused depends on the interpretation given to the scope of the exception mentioned in Article 15 (4) and Article 20 (4) GDPR stating that the respective right to access and data portability *[…] shall not adversely affect the rights and freedoms of others.* [83]

Trade secret protection is specifically mentioned in recital 63 of the GDPR as a right to take into consideration. [84]

The exception refers to the *rights and freedoms of others* which includes other data subjects as well as the data subject who is requesting access. Although argued by some, it would seem unlikely that the rights of the data controller are excluded from consideration.[85] But even if this is the case there can be third parties who have lawfully obtained vehicle data and who have an interest in protecting secrecy of this data. When (access) to vehicle data is sold to third parties they, as subsequent trade secret holders, can be considered to have a vested commercial interest in keeping the data from becoming publicly known and available to all.

To qualify as an *adverse effect* granting a request would have to create unjustified damage or illegitimate limitations.[86] The Trade Secrets Directive acknowledges that the loss of trade secret protection *´could have devastating effects on the legitimate trade secret holder, as once publicly disclosed, it would be impossible for that holder to revert to the situation prior to the loss of the trade secret´*. [87] The Directive provides useful factors to take into consideration when deciding how to balance the decision on how to respond to a request, looking at the value of a trade secret, the impact of granting access and the interests of third parties including, where appropriate, consumers.[88.]

Since the GDPR does not state what the outcome of the consideration should be, it leaves the judgement about what the right response would have been ultimately open for the courts to decide on a case-to-case basis.[89]

Looking at the GDPR in the context of the Trade Secrets Directive, Recital 18 of the Directive states that*´ the treatment of the acquisition of a trade secret as lawful should be*

without prejudice to any obligation of confidentiality as regards the trade secret or any limitation as to its use that Union or national law imposes on the recipient or acquirer of the information.´ One could argue that the trade secret holder could pose additional measures upon the receiver of the trade secret through its terms of use or via agreement. Such a measure would benefit both vehicle manufacturers to be compliant with the GDPR and provide a service to their customers while still being able to protect trade secrecy and/or monetize the data. The driver will still obtain access and control over who they choose to share their data with for legitimate purposes.

If the vehicle manufacturer can successfully argue that providing a copy would result in the loss of Trade Secret protection of the data this can be considered a valid ground to refuse a request based on Art 20 GDPR for Data Portability. [90] A more proportionate response could be to allow the manufacturer to request for reasonable steps to be taken to keep the data secret by the recipients and/or to limit further use when this would result in a loss of trade secret protection. This interpretation of the GDPR would still empower the data subject by providing them with information in a way that does not destroy secrecy therefore finding a balance between sharing of knowledge, protecting privacy and enabling innovation.

To conclude and consider

Car manufacturers have been collecting vehicle data for years using it to understand their (potential) consumers and to optimize and develop new products and services and business relations. The value of vehicle data is evident not only for the car manufacturer but third parties who increasingly rely on data. To contribute to the discussion this paper considers the role of Trade Secrets protection for Vehicle manufacturers to control vehicle data access. Trade secrets could play an important role in EU innovation policy providing incentives to invest in research and development and to share knowledge. [91] Based on the analysis

presented in this paper, it is proposed that vehicle manufacturers who hold vehicle data as a trade secret must respond to a data subject access request by providing access to personal data under processing. Access rights can only be refused when granting a copy and/or have a copy transmitted to another controller would adversely affect the right of the trade holder and there is no alternative.[92] In absence of clear prevalence of the GDPR over the Trade Secrets Directive we argue that if granting access to a copy or data portability of personal data would have such an adverse effect on trade secret protection, it justifies the trade secret holder to take measures to maintain trade secret protection.[93] A full refusal to provide access however is not considered a proportionate response when other measures can be taken to maintain trade secret protection. Whether this interpretation of scope and requirements under the trade secret directive and the GDPR presented is correct remains to be seen, what is clear is that there is a need for more legal certainty how to balance between competing interests with respect to protection of and access to in-vehicle data and resources. With the call for a regulatory proposal the European Commission now has an opportunity to do so to provide all stakeholders involved with the necessary guidance to allow for beneficial use of vehicle data.[94]

References

Almeling, DS. *Seven reasons why trade secrets are increasingly important*. Berkeley Tech Law, 2012, J 27:1091

Aplin, T. *Reverse engineering and commercial secrets*. 2013 Curr Leg Probl 66(1):341

Aplin, T. *Right to property and trade secrets*.2014 I: Geiger C (ed) Human rights and intellectual property: from concepts to practice. Edward Elgar, Northampton, p 421

Article 29 Data Protection Working Party, on the concept of personal data, Opinion 04/2007

Article 29 Data Protection Working Party, on Anonymization Techniques, Opinion 05/2014

Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01 5 April 2017

Article 29 Data Protection Working Party, on legitimate interests, Opinion 6/2014.

Ayuso, M., Guillen, M., and P´erez-Mar´ın, A. M. *Telematics and gender discrimination: Some usage-based evidence on whether men's risk of accidents differs from women's*. Risks, 2016, 4(2):10.

Bapat, A. *The new right to data portability*, 2013, 13(3) P & DP 3.

Wilkoff, N. Basheer, S. (eds.) *Overlapping Intellectual Property Rights* 2012, OUP Oxford, 57

Bordoff, J. E. and Noel, P. J. *Pay-as-you-drive auto insurance: A simple way to reduce driving-related harms and increase equity.* 2008. The Brookings Institution. Discussion Paper.

Brown, I. Marsden, C. *Regulating code: Good governance and better regulation in the information age*, 2013, MIT Press, Cambridge, MA,

Centre for Information Policy Leadership. Comments on the Article 29 Data Protection Working Party. 2017.

C-ITS Platform Working Group 6, *Access to in-vehicle resources and data*, Report December 2015, >https://tinyurl.com/yblsemml< Accessed June 2018

Determann, L *No One Owns Dat*a, 2018. UC Hastings Research Paper No. 265.

Desyllas, P. and Sako, M. *Profiting from business model innovation: Evidence from pay-as-you-drive auto insurance*. 2013 Research Policy, 42(1):101–116

Drexl, J. *Designing Competitive Markets for Industrial Data - Between Propertization and Access*, 2016 Max Planck Institute for Innovation and Competition, Munich

Dreyfuss R and Strandburg K (eds.), *The Law and Theory of Trade Secrecy* , 2010, A Handbook of Contemporary Research, Edward Elgar Publishing

European Commission, Staff working paper*, Impact Assessment report*, SEC(2012) 72 final.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

European Commission, A Digital Single Market Strategy for Europe, Communication, COM, 2015, 192 final, 6 May 2015,

European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market*, MARKT/2011/128/D (April 2013), pp.12 f., 23

European Commission, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, (COM(2016)0766)

European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* 2014 (Preliminary Opinion) 6

European Data Protection Supervisor, Opinion on the proposal for a directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Opinion) 2014

European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final 2013/0402

Falce, V. *Trade Secrets - Looking for (Full) Harmonization in the Innovation Union*, 2015 Max Planck Institute for Innovation and Competition, Munich

Filipova-Neumann, L. and Welzel, P. *Reducing asymmetric information in insurance markets: Cars with black boxes.* Telematics and Informatics 2010, 27(4):394–403

Friedman, D. et al. *Some economics of trade secret law*, 1991. J Econ Perspect 5(1):61

Geradin, D., & Kuschewsky, M. *Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue* 2013. SSRN Working Paper.

De Graef, I. Verschakelen, J. Valcke, P. *Putting the right to data portability into a competition law perspective*, 2013, Annual review, The Journal of the Higher School of Economics 53, 58

Graves, C. Diboise, J. *Do strict trade secret and non-competition laws obstruct innovation* ?

Halligan, R.M. Weyand, R.F. '*The Economic Valuation of Trade Secret Assets'* (2006) J Internet L 19, 21.

Hoeren, T. *The EU Directive on the Protection of Trade Secrets and its Relation to Current Provisions in Germany*, 9 (2018) JIPITEC 138 para 1.

Hogan Lovells International LLP *Report on trade secrets for the European Commission* (2012)

Husnjak, S., Perakovi´c, D., Forenbacher, I., and Mumdziev, M. *Telematics system in usage-based motor insurance.* 2015 Procedia Engineering, 100:816–825.

Janal, R. *Data Portability - A Tale of Two Concepts*, 8, 2017 JIPITEC 59 para 1.

Kaushik, A. Franzoni, L.A. *The optimal scope of trade secrets law,* 2014, Quaderni - Working Paper DSE N°1020, ISSN 2282-6483

Kerber, W. *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 2018. Forthcoming in: JIPITEC

Kellezi, P. et al. (eds.), *Abuse of Dominant Position and Globalization Protection and Disclosure of Trade Secrets and Know-How*, 2017 LIDC Contributions on Antitrust Law ,Intellectual Property and Unfair Competition, Springer International Publishing AG 2017 p 291-311

Lemley, M. *The surprising virtues of treating trade secrets as IP rights*. 2008 John M. Oil Program in Law and Economics, Stanford Law School, Working Paper No. 358

Malgieri, G. *Trade Secrets v Personal Data: a possible solution for balancing rights International Data Privacy Law,* 2016 Volume 6, Issue 2, Pages 102–116,

Malgieri, G. Custers, B. *Pricing privacy – the right to know the value of your personal data*, 2017 Elsevier p 302

McCarthy, M. et al. *Access to In-vehicle Data and Resources.* 2017, Study commissioned by European Commission CPR2419. Brussels.

Moura, P. '*The sticky Case of Sticky Data: An examination of the Rationale, Legality, and Implementation of a Right to Data Portability Under European Competition* Law' 2014, Media@LSE Electronic MSc Dissertation Series

Ohm, P. '*Broken promises of privacy: Responding to the surprising failure of anonymization',* 2010, UCLA Law Review, Vol. 57, No. 6, pp. 1701–1777

Petit, J. Shladover, S. *Potential Cyberattacks on Automated Vehicles. Intelligent Transportation Systems*, 2014 IEEE Transactions on. PP. 1-11.

Pooley, J. *'Trade Secrets The Other IP Right'* (2013) 3 WIPO Magazine 2.

Reichman, J.H. Samuelson, P. *Intellectual property rights in data?* 1997, Vanderbilt Law Rev 50:51

Reddix-Smalls, B. *Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market* 2011, 12 U.C. DAVIS BUS. L.J. 87, 117-18

Samuelson, P. Scotchmer, S. *The law and economics of reverse engineering.* 2002 Yale Law J 111:1575

Schwartz, A. '*The Corporate Preference for Trade Secret'* 2013, 74 Ohio State LJ 623

Schultz MF, Lippoldt DC, ''Approaches to Protection of Undisclosed Information (Trade Secrets) – Background Paper'' 2014, OECD Trade Policy Paper No. 162, 5,

Sousa, E. *What exactly is a trade secret under the proposed directive?* , 2014, Journal of Intellectual Property Law & Practice, Vol. 9, No. 11

Simpson, M. *The Future of Innovation: Trade Secrets, Property Rights, and Protectionism—An Age-Old Tale* 2005, 70 Brooklyn Law Review 1121

Smethurst, G. *Access to the vehicle and vehicle-generated data - "NEVADA Share and Secure Concept"** Verband Der Automobilindustry (VDA) online >https://tinyurl.com/yd4m8rwy< accessed August 2018

Stuyck, J. et al *Confidence through fairness? The new Directive on unfair business-to-consumer commercial practices in the internal market.* 2006 Common Mark Law Rev 43:107–152

Surblyte_ G *Liability for the infringement of trade secrets in Lithuania* , 2008. Justitia 69(3):41–52

Swire P, Lagos Y, *'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique'* 2013, 72(2) Maryland Law Review 335 360.

Toledo, T. Musicant, O. Lotan, T. *In-vehicle data recorders for monitoring and feedback on drivers'behaviour.* 2008Transportation Research Part C: Emerging Technologies, 16(3):320 – 331.

Tselentis, D. I., Yannis, G., and Vlahogianni, E. I. *Innovative insurance schemes: Pay as/how you drive.* 2016. Transportation Research Procedia, 14:362 – 371.

Van Caenegem, W. *Trade secrets and intellectual property: breach of confidence, misappropriation and unfair competition*. 2014 Wolters Kluwer, The Hague

Van der Auwermeulen, B. *How to attribute the right to data portability in Europe: A comparative analysis of legislations,* 2017 Computer Law & Security Review, Volume 33, Issue 1, 2017, pp. 57-72

Wachter, S. Mittelstadt, B. *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,* 2018. Columbia Business Law Review, Forthcoming.

Weiss, S. *Privacy threat model for data portability in social network applications* 2009 International Journal of Information Management, 29 (4) pp. 249-254

Yoo, C.S. *When antitrust met Facebook,* 2012 George Mason Law Review, 19 (5) pp. 1147-1162

Zanfir, G. *The right to Data portability in the context of the EU data protection reform,* 2012 International Data Privacy Law, 2 (3) pp. 149-162

Zech, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data* 2016, JIPLP, 460,

.

Notes

[1] FIA technical study [online] http://www.mycarmydata.eu/# (Accessed December 2018)
[2] For a detailed description of telematics insurance [online] https://www.insurethebox.com/telematics (Accessed April 2019)
[3] Verband der Automobilindustrie (VDA) Position Paper, Access to the vehicle. [online] https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html (Accessed December 2018) See for security concerns: Jonathan Petit and Steven Shladover. (2014). *Potential Cyberattacks on Automated Vehicles. Intelligent Transportation Systems,* IEEE Transactions on. PP. 1-11. 10.1109/TITS.2014.2342271.
4 See VDA Position Access to the vehicle and European Automobile Manufacturers' Association [online] https://www.acea.be/publications/article/position-paper-access-to-vehicle-data-for-third-party-services< (Accessed December 2018)
[5] McCarthy M, et al. Access to In-vehicle Data and Resources. 2017, Study commissioned by European Commission CPR2419. Brussels; and Determann, L. *No One Owns Data,* 2018. UC Hastings Research Paper No. 265.
[6] Victor Barreto, Paul Ciolek *What is OBD II? History of On-Board Diagnostics* [online] https://www.geotab.com/blog/obd-ii/ (Accessed August, 2018)
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[8] Member States had to implement Directive (EU) 2016/943 into national law by June, 2018; and the Regulation (EU) 2016/679 came into force in May 2018.
[9] Henrik Bengtsson, *International report* in P. Kellezi et al. (eds.), *Abuse of Dominant Position and Globalization, Protection and Disclosure of Trade Secrets and Know-How,* LIDC Contributions on Antitrust Law, Intellectual Property and Unfair Competition, Springer International Publishing AG 2017 p 291-311
[10] Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
[11] Recital 1 of the Directive states that a lack of adequate protection for trade secrets compromises the legitimate trade secret holders' ability to obtain first-mover returns from their innovation-related efforts. See for an overview of the different views on trade secrets: Charles T. Graves*, Trade Secrets as Property: Theory and Consequences,* 15 J. Intell. Prop. L. 39 (2007) citing Pamela Samuelson.
[12] Opinion of the European Economic and Social Committee on the Proposal for the Trade Secrets Directive describes why a Directive was needed. For a more critical analysis of the proposed directive see Tanya Aplin, *A critical evaluation of the proposed EU trade secrets Directive,* 2014 King's college Legal Studies Research paper Series Paper no 2014-25
[13] The Paris Convention, states that its members must assure protection against acts of unfair competition and specifically against any act of competition contrary to honest practices in industrial or commercial matters that constitutes an act of unfair competition (Article 10bis (2)) See Valeria Falce, *Trade Secrets - Looking for (Full) Harmonization in the Innovation Union,* 2015 Max Planck Institute for Innovation and Competition, Munich.
[14] Article 3 Trade Secrets Directive. Independent discovery of the same know-how or information should remain possible. Mars UK Ltd v Teknowledge Ltd, [2000] FSR 138 (Ch D) 14
[15] Recital 1 of the proposal COM(2013) 813 final. Stating that business information extends 'beyond technological knowledge to commercial data'. What constitutes as a business secret is further defined in case law: ECJ judgment of 18 September 1996, CaseT-353/94 (Postbank v Commission), paragraph 87; ECJ judgment of 30 May 2006, Case T-198/03 (Bank Austria Credit anstalt v Commission), paragraph 71. SWD (2013) 471 final, Annex 4, Section A4.2, p.112. See for a critical analysis further Sandra Wachter and Brent Mittelstadt *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2018. Columbia Business Law Review.

[16] Recital 14, Falce 2015, p. 959 n.12

[17] As confirmed by the EDPS referring to the relevance of the protection of personal data as trade secrets may include personal data. For a more narrow view Aplin 2014 n.11 and What constitutes as a business secret is further defined in case law: ECJ judgment of 18 September 1996, CaseT-353/94 (Postbank v Commission), paragraph 87; ECJ judgment of 30 May 2006, Case T-198/03 (Bank Austria Credit anstalt v Commission), paragraph 71. SWD (2013) 471 final, Annex 4, Section A4.2, p.112. See for a critical analysis further Sandra Wachter and Brent Mittelstadt *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2018. Columbia Business Law Review

[18] PTOLEMUS, Global Usage-based Insurance Study January 2016, Free abstract [Online] https://www.ptolemus.com/ubi-study (Accessed December 2018)

[19] Art 4 Directive. Value is considered proven when the information has been misappropriated by a third party On value see Aplin, 2014 n.11 p.10

[20] Christian Scheiblich, Thomas Raith *The extended vehicle*, The ExVe *ISO 20078*, Daimler AG, GSP/O–CLEPA Aftermarket Conference–Brussels, November 2014

[21] Some examples of platforms [online] https://otonomo.io/ (Accessed December 2018) and [online] https://aos.bmwgroup.com/web/oss/apps/otp-public (Accessed December 2018) On the value of personal data see G. Malgieri and B. Custers, *Pricing privacy the right to know the value of your personal data*, 2017 Elsevier p. 302

[22] The data can still fall under protection when it is part of a protected data collection..

[23] Recital 1 Directive. This interpretation is proposed by Aplin 2014, n.11 p.9 and p.14. On the importance of trade secrets for businesses in the digital economy. 'Protect and Preserve: The Rising Importance of Trade Secrets' [Online] www.bakermckenzie.com/ (accessed January 2019)

[24] The driver knows detailed information about their own driving and may have access to some of their vehicle's data. See for example the client portal for BMW [online] www.bmw-connecteddrive.com. (accessed December 2018)

[25] The scope and level of protection this offers is unclear. Relevant in this regard is the case of Douglas v Hello! Ltd [2005] EWCA Civ 595, see Aplin who argues for a case when the vehicle owner has a commercial interest in their personal data 2014.n. 11

[26] Reverse engineering can be understood as ' the process of ascertaining knowledge from a product or artefact and a lawful means of acquiring trade secret information except when otherwise contractually agreed.' If the information can only be obtained through reverse engineering and not further communicated the data should not be considered as readily accessible. Aplin 2014, p 11. Samuelson and Scotchmer consider ''reverse engineering as an important factor in maintaining balance in intellectual property law. Pamela Samuelson and Suzanne Scotchmer, '*The Law and Economics of Reverse Engineering'* (2002) 111 Yale Law Journal 1

[27] Valeria Falce, *Trade Secrets - Looking for (Full) Harmonization in the Innovation Union,* 2015 Max Planck Institute for Innovation and Competition, Munich

[28] Given the uncertainty over the interpretation of the Directive, this could lead to a situation where member states differ between what information qualifies for trade secret protection. Aplin 2014

[29] TRIPS provides some examples of what is considered contrary to honest commercial practices including a breach of confidence and an inducement to breach. Article 39(2) TRIPS See also Këllezi, Kilpatrick and Kobel, *Abuse of Dominant Position and Globalization & Protection and Disclosure of Trade Secrets and Know-How.* 2017 Cham: Springer International Publishing.

[30] Article 4 Directive

[31] Opinion of the European Automobile Manufacturers' Association, representing car makers who argue for control. [Online] http://cardatafacts.eu/safest-secure-way-share-car-data (Accessed December 2018)

[32] Trade secrets do not grant the holder exclusive rights. For an analysis of the optimal model: Kaushik A, Franzoni LA *The optimal scope of trade secrets law,* 2014, Quaderni - Working Paper DSE N°1020, ISSN 2282-6483

[33] On access needs: Gregory J. Thompson ea. In-Use Emissions Testing of Light-Duty Diesel Vehicles in the United States, Final Report, Center for Alternative Fuels, Engines & Emissions West Virginia University [Online] www.theicct.org and Zeynep Tufekci, *Opinion Volkswagen and the Era of Cheating Software*, Sept. 23, 2015, The New York Times [Online] https://nyti.ms/1L5wnHN and Jack

Ewing, Researchers Who Exposed VW Gain Little Reward From Success, July 24, 2016, [Online] https://nyti.ms/2a8HWxB< (Both Accessed December 2018

[39] Monkeys and a Beetle: Inside VW's Campaign for 'Clean Diesel', New York Times, [Online] >https://nyti.ms/2Fh7wjd< (Accessed December 2018)

[35] Lee Rainie and Maeve Duggan *The state of privacy* January 14, 2016 [Online] http://pewrsr.ch/1Ok0R7A (Accessed December 2018)

[36] BBC News, [Online] *Admiral and M&S insurance firms deny 'racism' claims by The Sun{Online}* https://www.bbc.co.uk/news/uk-wales-42795981 (Accessed , 23 January 2018)

[37] Various examples of vehicle data being used to improve urban life can be found in the context of smart city developments.

[38] The EDPS recommended that measures against unlawful practices should not restrict the rights of the data subject (…)in particular his or her right to access the data being processed and to obtain rectification, erasure or blocking of the data where it is incomplete or inaccurate. Proposed amendment of the article on lawful acquisition, use and disclosure of trade secrets. Opinion of the European Data Protection Supervisor, 2014

[39] 'The rights to respect for private and family life and to protection of personal data of any person whose personal data may be processed by the trade secret holder when taking steps to protect a trade secret, […]be respected. […] Thus, this Directive should not affect the rights and obligations laid down in Directive 95/46/EC, in particular, the rights of the data subject to access his or her personal data being processed [...]. furthermore, Article 9(4) of the Trade Secrets Directive concerning confidentiality during legal proceedings explicitly requires that any data pursuant to that article should be carried out in accordance with Directive 95/46/EC.

[40] Previous research confirms the rights to privacy and protection of personal data of data subjects. See EDPS Opinion 2014. On the conflict of rights: Malgieri, G. *Trade Secrets v Personal Data: a possible solution for balancing rights International Data Privacy Law*, 2016 Volume 6, Issue 2, Pages 102–116

[41] Malgieri, 2016, n.47

[42] Malgieri, 2016, n 47

[43] Sensitive data is referred to in Art 9(1) as special categories and include *'personal data revealing (...) political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'* Processing is prohibited unless any of the exceptions apply. Art 9(2)-(4) GDPR. Considering the revealing nature of location data as well as the improvements and sensor innovations this is something that should be closely monitored.

[44] WP29 Opinion 4/2007 on the concept of personal data, p. 4 Also the European Court of Justice (ECJ) supports a broad approach see Case C-101/01 Lindqvist [2003] ECR I-12971, paragraph 24; Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989, paragraph 64; Case C-524/06 Huber [2008] ECR I-9705, paragraph 43; and Case C-553/07 Rijkeboer [2009] ECR I-3889, paragraph 62. Y and S and M, N44

[45] According to the WP29 whether data 'relates to' a certain person is something that has to be answered for each specific data item separately. WP29 Opinion 4/2007 p.12;

[46] For example medical analysis.

[47] Data protection rules may (indirectly) still apply to information relating to dead people, business or legal persons. WP29 Opinion 4/2007 p22-24 and C-92/09 Volker und Markus Schecke GBR v Land Hessen.

[48] Identifiers include a name and location data. Art 4 GDPR

[49] "a person may be identified directly by name or indirectly by [..]a car registration number, [..]" The WP 29 considers a person identifiable when there is a possibility that he or she can be distinguished from all other members of the group. WP29 Opinion 4/2007, p.12

[50] WP29 Opinion 4/2007 p.13

[51] European Court of Justice C-101/2001of 06.11.2003 (Lindqvist), § 27 See further WP29 opinion p13 T37: Privacy on the Internet, An integrated EU Approach to On-line Data Protection, adopted on 21.11.2000

[52] Recital 26 GDPR

[53] Whereas some data controllers have argued differently, it would 'not make sense otherwise' WP29 Opinion 4/2007 p 16.
[54] WP29 Opinion 4/2007 p. 15
[55] The potential for identifiability depends on how long data is stored. WP29 Opinion 4/2007
[56] WP29 Opinion 4/2007
[57] This is the case when personal data can no longer be attributed to a specific data subject without the use of additional information. Recital 23(1); Art. 30(1)(a); Art. 83(1); Recital 60(a); Recital 61; Recital 67; Recital 125 GDPR; Art29 WP Opinion 05/2014 P3 See further Art 4(5) GDPR and Recital 26 Pseudonymized data is still personal data. Art 3 GDPR. See also WP29 Opinion 05/2014 p4 on the challenges for anonymization in the context of Big Data: Paul Ohm, P. *'Broken promises of privacy: Responding to the surprising failure of anonymization',* UCLA Law Review, Vol. 57, No. 6, pp. 1701–1777; and WP29 Opinion 05/2014 p5
[58] For telematics insurers the data would otherwise be useless for a person's risk assessment. Research has shown that telematics improves the accuracy of risk assessments. See for example Anales del Instituto de Actuarios Espanoles, Pay-as-you-drive insurance: the effect of the kilometres on the risk of an accident, 3a Epocaa, 19:135–154. On the limits what data can be used for insurance see Ayuso, et.al. Telematics and gender discrimination: Transportation Research Part A: Policy and Practice, Volume 113, July 2018, Pages 243-258
[59] This includes compliance with data processing principles (lawful ground, transparency and driver´s data subject rights) Art 5 GDPR.
[60] The Directive (art 2) requires trade secret holders maintain the secrecy of the information while the GDPR requires them to give access to the data subject whose data it concerns. Art 15 GDPR
[61] Recital 63 GDPR
[62] In this regard Recital 63 GDPR notes that the controller can ask to be more specific about what information or processing activities.
[63] Compare this with article 20(1) GDPR where the data must be provided ´in a structured, commonly used and machine-readable format´.
[64] Recital 6 GDPR, however, is somewhat confusing when it refers to ´ That right´ should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. That right could be the right to know and obtain communication or specifically the right to direct access to his or her personal data
[65] Some argue that the right to access can be restricted but never totally denied. Malgieri 2016 p.105 For a different opinion see IAB Europe's GDPR Implementation Working Group, Working Paper 4 – Data Subject Requests, [online] https://www.iabeurope.eu and Robert Madge, *Five loopholes in the GDPR 2017 Medium [online] https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b*< (Both accessed August 2018)
[66] Arguments for refusing a copy could be found in the 2014 "YS" judgment C-141/12, YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S. Also, Madge, 2017
[67] In several UK cases the court has decided that a blanket refusal to comply with an access request is not proportionate. An access request having an alternative purpose (fishing) is allowed for legitimate reasons. Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74; This may however limit what is required from the controller. Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd and Others [2017] EWCA Civ 121, 3 March 2017
[68] In an ongoing case between social media site Facebook and Max Schrems, the latter was denied some access to data requested based on trade secrecy. [Online] .http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf *(accessed December 2018)*
[69] Several Car brands now provide drivers with the opportunity to log inn to a website where they can access their driving data and obtain feedback about their driving based on actual driving data. [online] https://www.bmw-connecteddrive.com/ (accessed December 2018)
[70] Art 20 GDPR complements art 15 GDPR access with the right to dataportability. Anita Bapat ' The new right to data portability' (2013) 13(3) P & DP 3. The preamble of the GDPR confirms that the right is also applicable to other automated data processing systems and sectors including insurance. See Gabriela Zanfir, *'The Right to Data Portability in the Context of Data Protection Reform'* (2012) 2(3) International Data Privacy Law 149; Aysem Diker Vanberg, Mehmet Bilal Ünver *The right to data*

portability in the GDPR and EU competition law: odd couple or dynamic duo? 2017 in European Journal of Law and Technology, Vol 8, No 1,

[71] Recital 55, Recital 68 GDPR and Article 29 WP, Guidelines on the right to data portability, WP 242 rev.01 p. 4. Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10.1.2017, SWD (2017) 2, p. 11 and p. 47,

[72] WP29, Guidelines on the right to data portability, p. 4. Commission Staff Working Document on the free flow of data and emerging issues of the European data economy of 10.1.2017, SWD (2017) 2, p. 11 and p. 47

[73] WP29, Guidelines on the right to data portability. Note that this could include requiring the data subject and subsequent data controllers to agree to a confidentiality agreement based on trade secret protection.

[74] Art 20(2) GDPR. The WP29 specified that a direct transfer is "technically feasible" when "*communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data*". Thus, there is no obligation on the first controller to create or adopt compatible processing systems. WP29, Guidelines on the right to data portability 2017. That this could be problematic see Ruth Janal, *Data Portability - A Tale of Two Concepts,* 8 (2017) JIPITEC 59 para 1; Vanberg and Unver, 2017 n. 76; Inge Graef, Jeroen Verschalken, Peggy Valcke, *'Putting the right to data portability into a competition law perspective'* 2013 Law: The Journal of the Higher School of Economics, Annual Review 4.

[75] Article 20(3) and Recital 68. WP29 Opinion 6/2014 on legitimate interests (WP217); WP29 *Guidelines on the right to "data portability" 2*017, p5

[76] Raw data processed by connected objects fall under the right. WP29 *Guidelines on the right to "data portability" 2*017. Which is considered needed to achieve empowerment and market competition.' Janal 2017 n.51

[77] Allowing for data portability would avoid consumer lock-in in with a service provider.

[78] Including all data observed about the data subject and collected through the tracking and recording of the data subject WP29 *Guidelines on the right to "data portability" 2*017. Risk profiles developed based on telematics data would not be included. See Graef et.al 2013 n.51

[79] See De Hert, et.al 2018. In contrast the restrictive interpretation includes only personal data that the subject has *actively provided* in an explicit form See Malgieri 2016; Peter Swire, and Yianni Lagos. *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy* 2013, Critique Public Law and Legal Theory Working, Paper Series No. 204, 347

[80] EDPS Recommendations on the EU's Options for Data Protection Reform (2015/C 301/01). De Hert et.al 2018

[81] 'Article 20 does not limit portable data to those which are necessary or useful for switching services. WP29 Guidelines *on the right to "data portability" 2*017 p.5

[82] On the need for a broad interpretation for IoT See Ruth Boardman, Ariane Mole and Gabe Maldof: '*The Article 29 Working Party Issues Final Guidelines on the right to data portability.* For an economic analysis: Vanberg and Unver, 2017 n.76

[83] Important to note here that the right to obtain a copy under article 15 includes all personal data concerning the data subject where the right under article 20 is limited to personal data provided by based on contract or consent.

[84] Art 20(4) GDPR and Recital 68

[85] Instead of referring to third-party defined in Article 4(10) which excludes the data subject, controller, processor (...) both article 15 and 20 refer to the rights and freedoms of *other*s which is a term not further defined in the GDPR. Recital 68 mentions specifically the right of the data subject to obtain the erasure of personal data and emphasis that a request for data portability does not imply ´the erasure of personal data provided for the performance of a contract [..]. ´

[86] De Hert, et.al 2018; Barbara Van der Auwermeulen, *How to attribute the right to data portability in Europe: A comparative analysis of legislations* Computer Law & Security Review, Volume 33, Issue 1, 2017, pp. 57-7

[87] The Directive also acknowledges that trade secret protection could be used to pursue illegitimate intents including to unfairly delay or restricting access to the market, which would undermine the smooth functioning of the internall market. See Recital 22 Directive in reference to empowering judicial

authorities to adopt appropriate measures when a trade secret holder would act abusively or in bad faith and submit manifestly unfounded infringement applications

[88] Recital 21 Trade Secrets Directive referring to the principle of proportionality, when taking measures, procedures and remedies to protect trade secrets.

[89]A possible reason why the GDPR does not provide further guidance on when this requirement is fulfilled may be due to uncertainty about the impact of this newly proposed right. De Hert, et.al 2018; Van der Auwermeulen, 2017 n.86

[90] Judgment of the Court (Third Chamber) of 25 January 2018 Maximilian Schrems v Facebook Ireland Limited and for case updates [online] https://www.fbclaim.com/ui/register (accessed August 2018)

[91] Michael Risch, "*Trade Secret Law and Information Development Incentives,"* in The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research (Rochelle C. Dreyfuss, Katherine J. Strandburg, eds., Edward Elgar Publishing, 2010). Michael P. Simpson, *The Future of Innovation: Trade Secrets, Property Rights, and Protectionism, An Age-Old Tale*," 2005, 70 Brooklyn Law Review (2005), 1121. As the benefits of trade secrets include unlimited protection and being able to keep the information secret it may compete with patent protection. See further Charles Tait Graves, James A Diboise, *Do strict trade secret and non-competition laws obstruct innovation?*

[92] One could argue that by making the data only accessible but not available to copy, the data subject is informed about the (detail of personal data for) processing without the risk for the vehicle manufacturer that this data is copied and shared for analysis to reveal sensitive business information. Whether this is permitted remains to be seen.

[93] EC impact assessment on the Directive and Malgieri 2016, for an in-depth analysis why there is no clear prevalence between the GDPR and the Trade Secrets Directive.

[94] Amendment No 20 The EC is urged to establish an adequate legal framework. European Parliament resolution of 13 March 2018 on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI))

Acknowledgements

This Working Paper is part of the research undertaken by the Jean Monnet Centre of Excellence on 'European Intellectual Property and Information Rights' at Bournemouth University (European Commission's Erasmus+ Programme).
The funding of the European Commission to produce this publication does not constitute an endorsement of the contents, which only reflects the views of the author.