# DATA CREATED BY THE INTERNET OF THINGS: THE NEW GOLD WITHOUT OWNERSHIP?

THOMAS J. FARKAS*

## Introduction

Today, data[1] is more important than ever. It has become an asset with a big financial impact.[2] The way people handle their data and their scepticism towards the use has also seen some significant changes. Back in 1983, the German government has planned a census. Government officials were supposed to visit the public to collect their data. Amongst others, the data relevant for the census included information about their religious beliefs and their employment. After several constitutional complaints, the German Federal Constitutional Court held that the collection, the use and the transfer of the data was violating several fundamental rights, inter alia the right of informational self-determination.[3] This can be seen as an example where the public successfully defended the use of their data. This attitude has somewhat changed. Especially on internet platforms and social media, people share their lunches, holiday locations, family pictures, their employment details as well as political and religious beliefs. With the extensive use of the internet, where people can perform almost any transaction and which "never forgets", society has become more transparent than ever. Also, there is more data being created than

* Dr. Thomas. J. Farkas, LL.M. (London), Visiting Industry Senior Lecturer, Queen Mary University of London. Private Practice at Eversheds Sutherland, Senior Lecturer at Queen Mary University of London (Londres, Reino Unido). email: thomasfarkas@eversheds-sutherland.com Fecha de recepción: 2 de marzo de 2017. Fecha de aceptación: 4 de abril de 2017. Para citar el artículo: Farkas, Th. J. "Data created by the Internet of Things: The new gold without ownership?", *Revista La Propiedad Inmaterial* n.º 23, Universidad Externado de Colombia, enero-junio 2017, pp. 5-17. DOI: https://doi.org/10.18601/16571959.n23.01

1 According to the standard ISO/IEC 2382:2015(en) - Information technology, "data" is defined as "reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing", available on: https://www.iso.org/obp/ui/#iso:std:63598:en, lastly visited on 4 January 2017.

2 See e.g. H. Baldwin in Forbes magazine, "Drilling into the value of Data", available at http://www.forbes.com/sites/howardbaldwin/2015/03/23/drilling-into-the-value-of-data/#edc79a287223, lastly visited 27 January 2017.

3 German Federal Constitutional Court BVerfG, judgment of 15 December 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

ever. It is said that due to our extensive use of the internet, 90% of the world's data has been created in the last years. Allegedly, we create 2.5 quintillion bytes of data.[4]

The increase of data creation is further catalysed by new technologies and connected devices; it is often referred to as the "internet of things" (hereinafter "IoT" and "IoT-devices"). Wearables connected to a smartphone create data to people's physical activity. Data related to heart rates, steps taken in a certain time frame, etc., are created Smart thermostats in our homes use sensors, real-time weather forecasts, and the actual activity homes during the day to reduce energy usage. Networked cars[5] have multiple sensors, steering devices and technology that can communicate with other devices outside the car. A networked car might communicate details about traffic, favourite routes and road conditions to the car owner, manufacturer, navigation service providers, insurers, construction authorities and other companies. This data can be used to avoid traffic jams, driving behaviour relevant for insurers, improve road conditions, plan advertising on roads and service stations and to plan road reconstructions. Household devices such as refrigerators may be able to order food products when scanning that we run low of our milk supply. In an industrial environment, production lines may be optimised when they only produce certain parts or products according to incoming orders or when electricity prices are particularly low. The use of the data is sheer endless.

While this could be seen as a positive progress – this article does not take position in this regard – it begs the question who owns this data created by IoT-devices. Who owns the data collected by the networked car related to traffic information, road conditions, driving behaviour etc.? The owner of the car, the actual user of the car, the car manufacturer, the manufacturer of the sensor or communicating

4 See e.g. the statement on the homepage of IBM, available at https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html, lastly visited on 27 January 2017.

5 Networked cars are cars that e.g. automatically place the car in a parking spot or communicate with other cars. In the future, "*cars will be fully connected and automated. Intelligent 360- degree sensors ensure that the car moves forward at walking speed when in a traffic jam, removes the risk of an accident before it occurs, detects other vehicles and pedestrians in good time and understands traffic signs. Cars pick out the gaps in the traffic right away. Chips incorporated into the pavement record the flow of traffic and send the data to the vehicles. Autonomous mobility and fully connected traffic reduce both accidents and fuel consumption. Autopiloted cars turn drivers into passengers, giving them time to do other things while on the road like watching TV, reading or checking emails. Voice controlled Internet and social media as well as the control of comfort functions, such as regulating the air conditioning in the car via mobile devices, have already found their way into the cockpit*." It is said that "Nokia's Here brings maps and information on traffic and surroundings into the car and combines the services in the car with those available on: smartphones and on the web; BMW uses ConnectedDrive to offer navigation with current traffic information in real time, Internet services and a butler for the driver; Google plans to have robot taxis on the road by 2017; Toyota's Autopilot is equipped in similar fashion, but with improved sensors; The Nissan Leaf has a 360-degree laser scanner that monitors the surroundings while the car is moving. It even assumes control of the car independently." See the article "Mobility Has A New Dimension", TÜV Rheinland (German technical inspection association Rheinland), dated March 2015, available on: http://www.tuv.com/en/corporate/up_to_date/archives/knowledge_magazine_3_13/information_sercurity/networked_car/autonomous_mobility.html, lastly visited 5. January 2016.

devices built in the networked car, companies like navigation service providers or the road construction authorities?[6]

On the one hand, this data can be turned into a significant knowledge and into significant revenue. On the other hand, involved parties, e.g. the car owner/user, may have an interest on keeping information like their driving behaviour and location secret and might regard it as an intrusion to their privacy.[7]

This article intends to analyse the question if the status quo of the (German/European) law is sufficient to govern the ownership of data arising from new technologies and, if the question is to be answered in the negative, whether or not there is a need for "new industrial data rights".

## 1. Conflict of interests in the ownership of new data

When taking the example of the "networked car", and in order to allocate the problems arising with such new forms of data, the conflicting interests of the parties must be observed. As mentioned above, there are several parties[8] which have an interest in the ownership of the data:[9]

The owner or the user of a company or rental networked car may has an interest that the data of his location and driving behaviour is not revealed.

Navigation and Telecommunication service providers have an obvious interest to improve their services. Only with new data about driving behaviour and current locations, a navigation service provider could e.g. direct its users to other route options in case of increased traffic, bad road conditions or accidents.

In order to judge questions of liability, insurers have a clear interest on information related to driving capability and behaviour.

6 The European Commissioner for the Digital Economy and Society, Günther Hermann Oettinger, is in his personae in charge of the Commission's department for communications networks, content and technology. In 2015 he commented that the EU would lack a data strategy and that a virtual and digital law of property that includes data is necessary, see the article in the German journal *Wirtschaftswoche*, dated 14 April 2015, available on: http://www.wiwo.de/unternehmen/industrie/datenschutz-in-der-industrie-4-0-die-lange-nacht-der-forderungen-/11632398.html, lastly visited on 5 January 2017.

7 A rather dark forecast of the implications of new technologies on mankind is the theme of the TV show "Black Mirror". Its creator, Charlie Booker, explains the show as follows: "*If technology is a drug – and it does feel like a drug – then what, precisely, are the side effects? This area – between delight and discomfort – is where Black Mirror, my new drama series, is set.*" While reviews of this dark TV show have been overwhelmingly positive, this article does not intend to judge on the positive or negative aspects of new technologies. However, tech enthusiast will find some interesting aspects here, it should be briefly mentioned.

8 This is an exemplary, non-exhaustive list.

9 Furthermore, there is an obvious issue related to automated driving and liability in case of accidents. However, this article does not cover these issues. For further reading see e.g. *Duffy/Hopkins* , "Sit, Stay, Drive: The future of Autonomous Car Liability", 16 *SMU Sci. & Tech. Law Rev*. 101 (Winter 2013), available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379697, lastly visited on 4 January 2017.

The interest of the government in obtaining this information could relate to their activities in optimising traffic control, toll systems and maybe even crime prevention.

Internet service providers could use the data of networked cars to optimise their advertising on certain routes and service stations.

These interests beg the questions if e.g. any of these parties (i) may be able prohibit the collection and transfer of data being created by the networked car (here most likely the car owner or user)?; and (ii) who will decide on granting or denying access to this data to third parties (even if said handling of the data would be against the will of other parties)?

As the use of this data may involve significant revenue, the crucial question is, who owns this data, and, which area of law is governing this ownership?

## 2. Current legal framework for data ownership

The protection of intellectual property has significantly increased in the recent decades. Especially in Europe, new laws have significantly changed the IP framework and – at least to some extent – led to a harmonisation of the law governing intellectual creations[10]. But is the current legal framework[11] ready to face the challenges of the IoT, connected devices and the enormous amount of newly created data?

### 2.1. Copyright

Current Copyright Law provides the author protection in their work. Despite not yet being harmonised in the EU[12], Copyright Law "only" protects an author's own intellectual creation, see e.g. Sec. 2 para. 2 of the German Copyright Act. Moreover, an author must be a natural person[13]; the law does not apply to creations which are solely composed by a technological device. A device does not fall under the definition of an "author".

10 In the past decades, new laws that may protect intellectual property, inter alia the EU design law framework (Community Design Law as governed by the Council Regulation (EC) No 6/2002 on Community designs), the "sui generis" Database Right (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases) and, most recently, the EU framework on the protection of trade secrets (Directive EU 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure).

11 European Competition Law is not part of this article's assessment.

12 The "*Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market*" intends to harmonise EU copyright law, but must advance through the EU's legislative process. This may not be as early as 2018 (for further reading see the homepage of the EU, https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules, lastly visited 5. January 2017.

13 See e.g. Sec. 7 of the German Copyright Act ("The author is the creator of the work").

Hence, Copyright Law does not protect data generated by connected devices. Said data is not "original" and not created by an "author". The protection offered by Copyright Law and the long term of protection[14] also seems to be too extensive to protect data automatically generated IoT-devices.

### 2.2. Database right

The Database Directive[15] governs the protection of databases. Pursuant to Art. 1 (2) of the Database Directive, a database is defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means." Hence, in order to obtain protection for data generated by IoT-devices, said data must be arranged in a systematic or methodical manner. Moreover, it must be individually accessible. In case of the networked car, the data generated by virtue of the sensors must rather be regarded as raw data. E.g., the data regarding location and driving behaviour is rather not in a systematic or methodical order. Only when the data regarding the traffic status of more vehicles is combined, there is a strong value for e.g. a navigation service provider. Combining this data of more data objects may lead to a database which is protected by Art. 7 et seq. of the Database Directive. Hence, on conceptual grounds alone, the sui-generis protection of databases seems not suitable for the protection of individual, raw data[16]. Moreover, the established European case law emphasises the intention of the Database Directive to provide incentives for the creation of databases based on already available data, not for the creation of new information which can made into a database[17]. Therefore, the protection of investments in obtaining the contents of a database does not cover the investments made by the database creator in the creation of individual elements implemented in said database. When adopting the Database Directive, it was agreed that individual data contained in a database should not be protected[18] in order not to hinder free access to information. Also, the legislator implemented

14 "Copyright expires 70 years after the author's death", see Sec. 64 of the German Copyright Act.

15 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

16 See also the statement of the Max-Planck-Institute for Innovation and Competition, "Data Ownership and Access to Data", available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, page 4, para. 10, lastly visited on 5 January 2017.

17 See Judgment of the Court of 9 November 2004, ECLI:EU:C:2004:695, para 31. - British Horseracing Board Ltd.: *"The purpose of the protection by the sui generis right provided for by the directive is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database."*

18 See the statement of the Max-Planck-Institute for Innovation and Competition, "Data Ownership and Access to Data", available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, page 4, para. 11, lastly visited on 5 January 2017.

a threshold of substantiality[19] in Art. 7(1) of the Database Directive to prevent the risk of single-source information being monopolised.

### 2.3. Know-how and trade secrets

The eagerly awaited harmonised protection of trade secrets and Know-how has become a reality when the Trade Secrets Directive[20] came into force on 5 July 2016. According to Art. 2(1) of the Trade Secrets Directive, a trade secret is defined as any information which (i) is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (ii) (b) it has commercial value because it is secret; and (iii) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. As can be seen from this definition, the Trade Secrets Directive limits the protection of information to factual secrecy. When considering the protection of single-source data in light of this definition, said data can hardly qualify as a trade secret. Information automatically gathered by networked devices may not be secret, especially when considering that many interested parties could have access to it. Even if this information is kept secret by the means of technical measures against misappropriation, certain information remains available to others. For instance, information related to traffic jams obtained by networked cars is still available to other traffic participants passing by. Moreover, single-source information is not likely to have commercial value. Only the collection and combination of more data will the lead to commercially exploitable value. Another aspect worth considering is that the Trade Secrets Directive did not intend to specifically govern the data-driven economy. While the second recital mentions "commercial data such as information on customers and suppliers"[21],

19 A database right is only infringed if a substantial part of the database is extracted, see Art 7 no. 1 of the Database Directive: *"Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."*

20 Directive EU 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

21 The second recital reads as follows: "*Businesses, irrespective of their size, value trade secrets as much as patents and other forms of intellectual property right. They use confidentiality as a business competitiveness and research innovation management tool, and in relation to a diverse range of information that extends beyond technological knowledge to commercial data such as information on customers and suppliers, business plans, and market research and strategies. Small and medium-sized enterprises (SMEs) value and rely on trade secrets even more. By protecting such a wide range of know-how and business information, whether as a complement or as an alternative to intellectual property rights, trade secrets allow creators and innovators to derive profit from their creation or innovation and, therefore, are particularly important for business competitiveness as well as for research and development, and innovation-related performance."*

it is at least doubtful whether a broad interpretation of said wording will classify all kinds of data as trade secrets pursuant to the Trade Secrets Directive[22]. Finally, and when reconsidering an important question of data created by IoT-devices, the Trade Secrets Directive does not help to clarify who shall own the relevant information in this scenario.

### 2.4. Data protection

Generally, Data Protection laws intend to protect the right to privacy of individuals being impaired through the handling of his/her personal data[23]. This limits the scope of protection to only certain data, namely personal and sensitive data. With respect to many other forms of data, such as those mainly collected by IoT-devices, it is not applicable. Moreover, Data Protection laws are rather relative rights offering a very limited set of remedies where the interests have to be weighed. Hence, data protection laws have a different quality compared to exclusive rights[24]. Despite discussions among legal scholars to extend this right to tradeable aspects of data, the personality aspect of data protection seems to stifle such a progress[25]. Therefore, Data Protection laws also do not comprehensively govern data as created by IoT-devices.

### 2.5. Other relevant legal tools

Indirect protection could be afforded by simply taking governing that the data created by IoT devices follows the ownership of the relevant data carrier. However, this concept would not take into account the interests of other participants apart from those of the owner. Also, the ownership of a networked car would then lead to ownership of the data created by it. Hence, the ownership of data created by a networked rental/business car would be treated differently than that of a car personally owned. This aspect is likely to lead to further issues.

### 2.6. Conclusion

The current laws do not comprehensively govern the ownership and other issues related to data created by IoT-devices. This begs the further question whether or not a new law needs to be implemented.

22 See also the statement of the Max-Planck-Institute for Innovation and Competition, "Data Ownership and Access to Data", available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, page 7, para. 27, lastly visited on 5 January 2017.

23 See e.g. Sec 1 para. 1 of the German Federal Data Protection Act.

24 See Wiebe in GRUR Int. 2016, 877, 880.

25 See Kerber in GRUR Int. 2016, 639 et seq.

## 3. Demand for a new right regulating data ownership?

### 3.1. Preliminary considerations

One basic principle of IP rights must be stressed: IP rights shall in no way monopolise rights on information. Moreover, when comparing data to other protectable subject matter within the framework of IP law, there is arguably non-rivalry in the use of data. The use of data by one person does not (necessarily) distort the use of said data by other market participants. Furthermore, there is also a valid argument for data being a public good. Only when there is open access to data to some extent, then every market participant has the same chances in order to advance. Additionally, most of the data privately produced is excludable. The data holder may choose whether or not there shall be access to certain data. For example, technological protection measures may exclude certain employees of a company to access certain records. This notion is somewhat analogous to a trade secret. As mentioned above, the worldwide creation and storage of seems to increase exponentially. In contrast to the pre stages of the implementation of other IP rights, there is hardly any claim concerning market failure due to the lack of an "appropriate" protection.

In a nutshell, excludability and the requirement of public access prove that the protection of data created by IoT-devices is somewhat different than the other IP rights.

### 3.2. New right?

However, legal scholars discuss whether or not there is a need to govern the enormous amount of data being created or to be created in the future by IoT devices in respect of their ownership and therefore, to determine their economic significance. But could a new law help to solve the issues related to data generated by IoT-devices? Moreover, can it strike the right balance between protection of the investment in the creation of data and free access to it? How should a new law be designed?

#### *3.2.1. Subject matter*

As a starting point, and analogous to any law governing IP protection, a new law must have a specific subject matter. The concept of data as such does not seem to be an appropriate subject matter[26]. Especially in light of the various types of data emerging, the mere subject matter of data would be too broad as a protection

26 The definition of data according to Wiebe, see GRUR Int. 2016, 877, 883.

requirement. At least there should an additional requirement, e.g. "added value" or "novelty"[27].

With respect to a criterion of "added value" for data being created by IoT-devices, a subjective assessment would be necessary. When considering the various different types of data, when is data "adding value" and to what? Also, at what stage new data is adding value. Can single-source data "add value" or is this only the case when combined with further data? In the first case, when single-source data would suffice to "add value", this seems to restrict free access to information and not properly striking the right balance. In case the criterion of "adding value" would require single-source data to be combined with other data – which, from a factual viewpoint seems more likely – then this could come too close to the database right. This would lead to a risk of an overlap or dilution of both rights[28]. Hence, the criterion of "added value" does not seem to be an appropriate fit. It is too subjective to evaluate and it would endanger free access to information.

The discussed criterion of "novelty" with respect to data generated by IoT-devices seems – at first sight – more appropriate. However, what is "novelty" of data generated by IoT-devices? One could consider that this data is novel if it has not been created or stored before. However, this is rather difficult to assess. The data created by an IoT-device will in some aspects always be new since data e.g. related to a certain traffic jam are always related to a specific date, time and place. But if these new aspects shall suffice to regard data as novel, then virtually any data would be new. The balance of the protection of data and free access to information would be shifted towards the right holders. When defining "novelty" in types of data generated by an IoT-device according to their type, this could lead to a monopoly restricting competition. A "type" of data could be data about road conditions and accidents on a highway, or the data related to turning on the heaters in a house via smartphone. However, when the mere type of data is sufficient to determine "novelty", then this would create a factual monopoly for the owner of this type of data and could stifle competition[29]. Then, there is a clear need to further limit this new right, e.g. with regard to the term and the scope of protection to already existing data[30]. Further, creating a type of data again and creating new data should be free for all. A limitation to private use would also be appropriate (despite the fact that the delimitation of commercial and private use is not always an easy evaluation).

A criterion of "originality" or "creativity" is not appropriate: it is too close to copyright law.

27 See e.g. Zech, *Information und Schutzgegenstand*, Tübingen, p. 46 et seq.; Wiebe in GRUR Int. 2016, 877, 883.

28 It could also be considered to implement the criterion of "investment" made in the creation of data. Again, this criterion is already utilized in the protection of databases.

29 Therefore, there would be a need to further limit this new right.

30 Wiebe in GRUR Int. 2016, 877, 883.

In summary, it seems that the mere "first-mover advantage" is sufficient to exploit the interests of the creator of the business idea relating to the data created by IoT-devices. With respect to the business model, other IP laws are already in place offering appropriate protection. Moreover, the protection of this data could also lead to indirect protection of information[31], which should be avoided.

### *3.2.2. Ownership*

A main issue of a new right in data created by IoT-devices is ownership. Easily, any party involved in creating this new data can substantiate in either commercially exploiting this data or at least in keeping this information a secret or – for private persons such as the user of networked car – to himself. When evaluating who created the data and grant the right to the creator, also many parties[32] are involved to a more or lesser extent. All of the parties mentioned before are involved in the creation of this new data. One could argue, that ownership should fall to the party with the clear most interest or who could make the most value out of it[33]. The clear and simple argument against this proposal is that it will be difficult to determine the party with the most interest. When considering the party with the most benefit of owning the data, one could argue, that this will be also the party with the biggest financial possibilities unfairly favouring big enterprises and leaving behind start-ups. Moreover, this very subjective consideration does not match the basic idea of IP law as it is unprecise and would then be evaluated differently in every single case. From a factual point of view, it seems to be very difficult to assess who has the most interest in this data. The exclusion of the parties who have a lesser degree of interest could also result in less cooperation between the parties which all play a role in creating this data in the first place. Less interaction between these parties also contradicts the principle of IoT, where the cooperation is necessary to set up new business models and methods of doing business.

### *3.2.3. Summary*

The current discussion related to a new law governing data created by IoT-devices, which so far only few scholars got involved, proves that the creation of a new right is not easy. The subject matter and the ownership of such a new right are rather difficult to define. Moreover, it seems difficult to strike the right balance between protection and the right to free access to information.

31 See Heyman, "Der Schutz von Daten bei der Cloud-Verarbeitung", CR 2015 807, 810.

32 E.g. the manufacturer of the IoT-device, the manufacturer of products where said devices or the software are implemented, the provider of a service based on this data and the owner/user of the product.

33 Wiebe in GRUR Int. 2016, 877, 883.

## Conclusion

In favour of a new law it could be argued that new business models will only emerge when a new right adequately protects their newly created data[34]. However, currently an enormous amount of data is created despite a specific protection by the law.

Moreover, a new law could also set the tone for free access to information by virtue of specific limitations. As technological protection measures play a significant role, it is doubtful, that the use of such measures will be actually reduced to guarantee free access. Allocating the right and guaranteeing rules for the ownership of the data created by IoT-devices could bring order into a rather unregulated market. This could lead to data being collected and used more efficiently instead of grabbing all data available[35].

As shown above, the question of ownership is a difficult one. It is not clear who shall own the data created by IoT-devices and to which party it is allocated without interfering with the interests of the others. Moreover, the delimitation between granting a new right and safeguarding free access to information is even more difficult. In fact, free access to information seems to be endangered. Finally, a new right seems to be either not suitable or to interfere with the existing IP framework.

At the current stage, the question whether or not there is a need for a new law must be answered in the negative. The issues overweigh the positive aspects. The first mover advantage seems to suffice in order to protect new business models. The fact that many new business models already depend on utilizing said data and that – due to enormous amount data being collected – a market failure is not in sight[36], a new law also does not seem to solve any real issues. A new law offering protection for data generated by IoT-devices is more likely to create new monopolies stifling innovation than to regulate this wild market.

It remains to be seen whether or not the impact of the new Trade Secrets Directive will have on the protection of (secret) information. Before establishing another

34 This is the main argument for most newly created rights. For example the justification of the trade secrets Directive is – amongst others – laid down in recital: *"Innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage or the breach of confidentiality requirements, whether from within or from outside of the Union. Recent developments, such as globalisation, increased outsourcing, longer supply chains, and the increased use of information and communication technology contribute to increasing the risk of those practices. The unlawful acquisition, use or disclosure of a trade secret compromises legitimate trade secret holders' ability to obtain first-mover returns from their innovation-related efforts.* Without effective and comparable legal means for protecting trade secrets across the Union, incentives to engage in innovation-related cross-border activity within the internal market are undermined, and trade secrets are unable to fulfil their potential as drivers of economic growth and jobs. Thus, innovation and creativity are discouraged and investment diminishes, thereby affecting the smooth functioning of the internal market and undermining its growth-enhancing potential." (emphasis added).

35 Wiebe in GRUR Int. 2016, 877, 881.

36 Wiebe argues that a test for market failure should be made depending on the specific market and only if it is then necessary, further actions (by the legislator) should be taken, see Wiebe in GRUR int. 2016, 877, 884.

new right, the legislator should take into account the impact of the Directive and the issues related to it[37].

As for now, parties involved in a scenario with data generated by IoT-devices are well advised to rely on contractual arrangements with at least a license to use this data. Since the discussion on a new right has not been led in all jurisdictions and a discussed new right would only be a national or European right, contractual arrangements are even more important in an international context.

## References

### Literature

Drexl, J.; R. Hilty et al. "Data Ownership and Access to Data", Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165

Duffy and Hopkins. "Sit, Stay, Drive: The future of Autonomous Car Liability", 16 *SMU Sci. & Tech. Law Rev.* 101 (Winter 2013), available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379697

Heyman. "*Der Schutz von Daten bei der Cloud-Verarbeitung*", CR Computer und Recht, 2015 807, 810.

Kerber, W., in *GRUR Int. Gewerblicher Rechtsschutz und Urheberrecht* – Internationaler Teil 2016, 639 et seq.

Koch and Farkas. "The disclosure–fair trial dilemma when enforcing trade secrets in civil court proceedings", *JIPLP*, (2016) 11 (12).

Wiebe, A., in *GRUR Int. Gewerblicher Rechtsschutz und Urheberrecht* – Internationaler Teil 2016, 877, 880.

Zech, H. "*Information und Schutzgegenstand*", Tübingen, Mohr Siebeck, 2012, p. 46 et seq.

### Cases

Court of 9 November 2004, ecli:eu:c:2004:695, para 31. - British Horseracing Board Ltd.

German Federal Constitutional Court BVerfG, judgment of 15 December 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

37 For a commentary on the issue of enforcing trade secrets in civil court proceedings see Koch and Farkas, "The disclosure–fair trial dilemma when enforcing trade secrets in civil court proceedings", *JIPLP*, (2016) 11 (12).

## Statutes

Council Regulation (EC) n.º 6/2002 of 12 December 2001 on Community designs.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

Directive EU 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

German Copyright Act.

German Federal Data Protection Act.

Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market (see the homepage of the EU, https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules).