Max Planck Institute for Innovation and Competition

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

Josef Drexl[*], Reto M. Hilty[*], Luc Desaunettes[**], Franziska Greiner[**], Daria Kim[**], Heiko Richter[**], Gintarė Surblytė[***] and Klaus Wiedemann[**]

I. Introduction

1. Digitalisation is increasingly shaping the economy. Buzzwords such as "Industry 4.0" and the "Internet of Things" symbolise the **data-driven economy**. Data-based business models do not represent an isolated industrial sector. Instead, data-driven operations permeate nearly all sectors of economic life today.

2. The European Commission has declared its Digital Single Market Strategy in Europe (COM(2015) 192 final) to be one of ten priority projects. One of the three pillars of this strategy statement is the aim of "maximising the growth potential of the digital economy". This is to be reached through **the European *Free Flow of Data Initiative***, which is scheduled to be released in November 2016. In this context, the Commission has announced that it will also address "the emerging issues of ownership, interoperability, usability and access to data" in certain situations. However, the Commission does not use a clear definition of the term "data".

3. This Position Statement of the Max Planck Institute for Innovation and Competition has been released in view of this announcement and against the backdrop of the ongoing debate in the political, economic and academic fields on the question of whether or not **exclusive rights or access rights in digital data**

[*] Prof. Dr., Director.
[**] Doctoral Student supported by the MPI/Junior Research Fellow at the MPI.
[***] Dr., Senior Research Fellow at the MPI.

should be introduced. It refers to both personal and non-personal data, focusing on the latter.

II. No need for exclusive rights in data

4. At present, the Max Planck Institute for Innovation and Competition **can see neither a justification nor a necessity to create exclusive rights in data**.

5. There is **no legal principle** that rights in data must be allocated to a specific legal subject from the outset. The law on the protection of personal data does not legitimise the control (ultimately, for economic motives) over the use of data either as such or on downstream data markets. Nor should exclusive data use rights be allocated to the owners of objects that generate data by sensors (e.g. machines or everyday appliances such as vehicles or heaters).

6. Based on the current state of knowledge, there are also **no economic reasons** for recognising exclusive rights in data. On the contrary, this would entail the risk of interference with the freedom to conduct a business and the freedom to compete, the risk of impeding business operations of other market players who depend on access to data, and generate negative effects on the development of downstream data markets. Of critical concern would be the strengthening of existing data power and the creation of new market power derived from data, which would foster anti-competitive market entry barriers. The general principle of a public domain of free information must prevail over the imminent creation of "information monopolies". In light of the apparent dynamic development of the digital economy, no general market failure can be observed or expected. Thus, no legislative incentives for the collection or creation of data are necessary: data will be produced anyway, often as a by-product.

7. Today, even without actual exclusive rights, data is already the **object** of daily **transactions**. The firms in question usually have the technical means to shield from third parties the data produced in the course of their business operations that they deem worthy of protection. In practice, this factual exclusivity is suf-

ficient to grant access to data on a contractual basis. It affords effective protection *inter partes* and guarantees the availability of feasible courses of action for market players. In particular, each firm can retain control over "its" data and determine who is authorised to access it. Compliance with contractual obligations can be secured, for instance, by imposing a contractual penalty in the case of unauthorised disclosure of data. This way, new markets can develop without statutory exclusive rights (comparable with markets for transmission rights for sporting events). Interfering with this well-established and functioning system by means of the statutory allocation of rights in data to individuals does not promise to improve market conditions from an economic standpoint. Instead, it would pose the risk of disturbing the already functioning markets.

8. Apart from economic arguments, the enactment of exclusive rights in data would lead to a number of **practical problems**, which could hardly be solved adequately in the short term. First of all, it would be necessary to determine the subject-matter and the scope of protection, thus raising such complex questions as how to define the term "data". Furthermore, the legislature would have to define the entitlements and specific rights of the right holders. This would pose quite a challenge, especially, when diverse stakeholders may qualify as potential right holders. Due to the interconnected and collaborative value chain in the data-driven economy, the creation of new rights in data is likely to yield legal uncertainty. Finally, it would be difficult to balance the interests of all parties affected by such rights and delineate the scope of protection.

III. No need to adjust the sui-generis protection for databases

9. As the allocation of exclusive rights in individual data is neither necessary nor justified, the **sui-generis protection of databases** laid down in Art. 7 *et seq*. of Directive 96/9/EC of 11 March 1996 on the legal protection of databases should not be expanded or reinterpreted to this effect.

10. On conceptual grounds alone, the sui-generis protection of databases is **unsuitable** for the protection of individual data. It is contingent upon the investment made by the maker of the database in the obtaining, verification or presentation of the database contents. When interpreting the Database Directive, the CJEU emphasises its goal of providing incentives for the creation of databases based on the already existing information, and not for the creation of new elements which can then be assembled into a database (established case law, first CJEU judgment in Case C-203/02, *BHB Horseracing* [2004] ECR I-10415 para 31 *et seq*.). Therefore, the protection of investments in obtaining database contents does not cover the investments made by the maker of the database to create its individual elements.

11. In the course of adopting the Database Directive, it was agreed that individual database contents should not be protected. Rather, the protection of the database as such should exist regardless of the intellectual property status of individual database contents (Art. 3(2)). Nevertheless, there were legitimate concerns that the de facto protection of database elements – especially in the case of **single-source information** – would, in effect, amount to the protection of database contents by exclusive rights. To prevent this risk, the legislature included a threshold of substantiality for extraction (Art. 7(1)), a reporting duty for the Commission (Art. 16(3)) and a reminder concerning the applicability of the general competition rules (cf. recital 47).

IV. No need for the special protection of algorithms

12. The Max Planck Institute for Innovation and Competition does not see any need to create special legal protection of **algorithms** used in data processing (e.g. in the context of big-data analysis).

13. To a great extent, technological challenges in the digital economy concern the development of tools to process collected raw data, in particular for filtering

and analysis. The algorithms that underlie such data-processing programs are *de lege lata* **not specifically protected**.

14. In contrast, **concrete computer programs** for processing data are already protected by copyright law of the Member States implementing Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs. Nevertheless, this protection covers neither the functionality of a computer program (judgement in *SAS Institute Inc.*, Case C-406/10, ECLI:EU:C:2012:259, paras 39-41) nor the underlying general algorithm (which is understood here as a set of rules to solve a problem step by step, independent of its expression and representation, e.g. the description of the steps to be made for analysing or filtering data and the criteria to be applied). This is already implied by Recital 11 of the Directive, which clarifies that copyright protection for computer programs should not extend to the "ideas and principles which underlie any element of a program".

15. A computer program as such also cannot be **protected by a patent** (Art. 52(2)(c) and (3) EPC). The underlying task of the program, i.e. the processing of data by means of an algorithm, is considered as non-technical in nature.

16. Likewise, **blanket protection of a computer program's functionality, abstract problems and underlying general algorithms** *de lege ferenda* must be **rejected**. In effect, such protection would extend to general ideas and business models. Protection of this type would lower the requirements for the grant of exclusive rights to a level that would contradict the fundamental conception of intellectual property rights, according to which abstract methods, ideas and theories should remain free.

17. Furthermore, protection would pose a risk of two **negative effects**: first, protection of abstract subject-matter would cause needless – and, in the case of algorithms, unreasonable – restraints on competition that, according to current knowledge, would not be economically justified. In particular, the resulting monopolisation of ideas would hinder technical progress and industrial devel-

opment (judgement in *SAS Institute Inc.*, C-406/10, ECLI:EU:C:2012:259, para 40). Second, it is barely foreseeable what markets and sectors would be affected. This makes finding suitable approaches to a regulation seem unrealistic.

V. Tortious conduct as a reference point for regulation?

18. The existing legal framework already prohibits particular forms of tortious conduct that are relevant for the data-driven economy. Such rules are known, for instance, as "regulation of fair dealing" or "regulation against unfair competition". Without creating exclusive *erga omnes* rights, they prohibit certain practices of market players and penalise violation through tort liability, administrative or criminal sanctions.

19. Such regulatory approach presents many **advantages** for a data-driven economy. In particular, the flexibility of its application makes it possible to keep abreast of rapid economic changes. Furthermore, it refrains from creating exclusive rights in the particular subject-matter, e.g. data, leaving access to such subject-matter, in principle, open. Moreover, regulation that is based on protection against tortious conduct and strongly influenced by legal practice is easier to adjust if it turns out to be dysfunctional.

20. Nevertheless, a regulation based on protection against tortious conduct would still constitute an intervention in the competitive process. Therefore, its adoption would require **justification** as well as a detailed analysis of the regulatory and economic framework. The starting point should be the stock-taking and evaluation of the existing regulations, both at EU and Member State level.

21. In this regard, the scope of the new Directive 2016/943/EU of 8 June 2016 on the protection of trade secrets should be examined. When technical measures enable factual exclusivity of data, the **protection of trade secrets** gains high practical relevance for undertakings. The Directive lays down rules "on the protection against the unlawful acquisition, use and disclosure of trade secrets" (Art. 1(1)); it is therefore a decisive issue whether the factual exclusivity of da-

ta falls under its scope. In light of these uncertainties and in view of the transposition of the Directive by the national legislatures, it is of utmost importance that the European Commission promptly take a position on these issues.

22. Art. 2(1) of the Directive defines a **trade secret** as "information which meets all of the following requirements: a) 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; b) it has commercial value because it is secret; c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".

23. **Individual data** can hardly qualify as a trade secret, especially due to the requirements of "secrecy" and "commercial value". Gathered or obtained data is often publicly available. If, for instance, potholes are automatically detected by passing cars, the same opportunity – to know where the potholes are – is available for everyone; the data generated are not absolutely "secret" to begin with. This also raises questions regarding the commercial value of such data. Despite the impossibility of keeping a piece of data secret, the information encompassed therein could still present some value if the generation of that data entails substantial costs.

24. In general, one should also take into account that the Directive **does not aim specifically at regulating the data-driven economy**. Although the second recital mentions "commercial data such as information on customers and suppliers", it is doubtful whether the broad interpretation of such passages could classify *all kinds* of data as trade secrets in the sense of the Directive.

25. Alternatively, the regulation could focus not on individual data but on **data sets**. To qualify as a "secret" in the sense of the Directive, trade secrets do not have to be created *ex nihilo*. Freely accessible information can also constitute a part of a trade secret. For instance, some information about customers might be publicly available; however, the aggregated customer data as a whole may well

qualify as a trade secret. Art. 2(1) of the Directive provides explicitly that information must be secret "in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known".

26. Translating this into the context of data, one can conclude that even if individual data might not constitute a trade secret, the **combination of data or information** (that as such is not publicly available) might well do so. The same argument also applies with regard to the requirement of commercial value: Even if the publicly available data as such might not possess commercial value, their combination can, nonetheless, acquire a certain value, conferring on the data holder a competitive advantage.

27. Even though the Directive does not specifically aim to regulate the data-driven economy, the legislature at any rate intended to create **flexible legal protection** and to ensure that the Directive remains adaptable to technical and economic developments. Pursuant to Recital 14, "[i]t is important to establish a homogeneous definition of a 'trade secret' without restricting the subject matter to be protected against misappropriation".

28. Should the Directive on the protection of trade secrets be inapplicable, it would be worth considering whether specific forms of protection against tortious conduct should be adopted in order to prevent interference into the entrepreneurial sphere of market players by third parties. Undertakings can remain competitive only if they possess a certain degree of autonomy in business operations. Although some Member States already provide for protection against third-party interference in undertakings' sphere of confidentiality, it might be worth considering a **specific legal regime** under EU law if there is no other way to achieve legal harmonisation in the internal market. Such protection should be designed so as to avoid creating disincentives for potential investors. In particular, the legal protection of undertakings' entrepreneurial sphere should neither result in exclusive rights in data as such, nor hamper legitimate access to data.

VI. The need to ensure access to data

a) The relevance of access to data

29. In the digital economy, more important may become situations, when particular market participants (such as start-up companies, suppliers etc.) **do not have access to the data** that they need to develop new or improve the existing products or services while also lacking the possibility to produce or gather such data themselves. At the same time, the companies that produce or collect data are as a rule unmotivated to grant (potential) competitors access to their data.

30. From an economic perspective, a **regulation of access** is necessary when, absent intervention, competitive markets would be hindered, or the development of new markets precluded. In particular, a regulation mandating access under certain conditions can countervail the accumulation of market power.

31. However, competition law, in principle, **is not a suitable instrument** to solve the problem of access in a systematic way (under b). If problems of access should accumulate and raise competition and innovation-related concerns, it would then be irresponsible to deny the need for a special regulation of access with reference to competition law. If an access regulation should be necessary, its implementation would, in turn, raise further questions regarding the interoperability and standardisation of data (under c).

b) The inadequacy of competition law

32. Access to data under competition law can be obtained only exceptionally, as a remedy in cases of **abuse of market dominance** (Art. 102 TFEU). First and foremost, one should take into account that competition law is enforced by reactive *ex post* instruments; its stringent – yet to be clarified – standard of intervention cannot provide a systematic solution to the problem of access that would create legal certainty upfront.

33. In situations other than the elimination of competition by providing access on discriminatory terms or exclusive dealing, the duty to grant access under com-

petition law is contingent on **quite narrow requirements** under Art. 102 TFEU. It is difficult to even prove that market dominance arises out of control over data. Moreover, it is by no means clear how the relevant market for data should be defined when access concerns not individual data, but large data sets for data-mining purposes, and under what conditions different data sets can be considered as substitutable. Furthermore, it can be difficult to prove abuse in cases of refusal to grant access to data.

34. In the cases *Magill* (joined Cases C-241/91 and C-242/91 [1995] ECR I-743), *IMS Health* (Case C-418/01 [2004] ECR I-5039), and *Microsoft* (Case T-201/04 [2007] ECR II-3601), the CJEU formulated **case-specific criteria** of infringement: The petitioner for access needs to prove that the data/information at issue is essential for the appearance of a new product or service, and that there is no other way to create or otherwise obtain it. Furthermore, the CJEU acknowledged that there might be an objective justification for the refusal to grant access. Yet the criteria and the scope of the specific requirements involved remain uncertain. In addition, it should be noted that these judgements were issued under the assumption of IP protection for the subject matter at issue; whether and how these findings can be applied to situations involving unprotected raw data is yet to be clarified. In this regard, one can assume that, in the context of a dynamic, data-driven economy, a duty to grant access under competition law could only be enforced in exceptional circumstances.

35. Indeed, the diversity and dynamic development of business models in the digital economy stand in stark contrast to the **case-by-case assessment** required under competition law. The fast pace of the data-driven economy pushes the applicability of competition law to its limits.

36. Data can be a source of **market power**, especially when (potential) market players lack the capacity to gather data themselves or otherwise gain access to them. This market power is not as such sufficient to establish abuse of market dominance, though. Moreover, the possession of market power can be easily

contested due to the fast pace and dynamics of the technology-intensive markets. So far, the Commission has been quite reluctant to intervene in such markets by competition law, as evidenced in the *Microsoft/Skype* and *Facebook/Whatsapp* cases.

37. Furthermore, in the relevant case law (*Magill*, *IMS Health*, *Microsoft*), access concerned particular, clearly identifiable and delineable information or data. In situations involving 'big data', access concerns data that are much **larger in volume** and of **unknown or unspecified** contents. The products or services that might be developed on the basis of such data cannot be readily ascertained at the time when access is granted. Therefore, it is not (yet) possible to adequately evaluate the dynamic effects on competition of the refusal to grant access in such cases. This applies all the more to situations when real-time data are provided by advanced technological means such as an application programming interface (API). To date, competition law has not dealt with such cases.

38. Not least the duration of proceedings makes the instrument of competition law particularly unsuitable to enforce interests in access (in *Magill* the proceedings went on for 10 years, in *Microsoft*, over 14 years). Furthermore, claims to access under competition law entail follow-up problems. In particular, commitments and conditions imposed in closing a case can intervene in the dynamic development of markets. Moreover, remedies necessitate monitoring of compliance.

c) The principles and modalities of special access regulation

39. A special **regulation of access to raw data** might, for one thing, aim to prevent potential market failure by protecting the proper functioning of competition and thus enabling innovation. A pertinent example of this is the regulation of data portability under Art. 20 of EU Regulation 2016/679 on the protection of personal data. A need for regulation can exist specific to a particular sector or context. For another thing, regulation of access can be justified by public-interest

considerations. In any case, there is a considerable need for further research with regard to the overall framework, the justifications and the concepts of regulation that are capable of realising an effective regime of access.

40. There is also a need for clarification with regard to **the modalities of access**, in particular the formats in which the data at issue should be made accessible. The value of data is likely to be enhanced through the interoperability of data formats and standardisation. Here, self-regulation by the involved industry players is one possibility. The Commission should encourage such self-regulation by establishing an appropriate regulatory framework. In this regard, the competition-law principles for assessing standard-setting agreements set out in the EU Guidelines on Horizontal Cooperation Agreements can serve as a starting point.