An access and transfer right to data—
from a competition law perspective†

Björn Lundqvist*

ABSTRACT
While business users face difficulties accessing and porting data on platforms, the
Digital Markets Act has been hailed as the legislative tool enabling business users ac-
cess and transfer the data they have generated on platforms controlled by gatekeepers.
The tool provided by the Digital Markets Act is discussed in this article and the author
argue that business users should have a more elaborated right to first access the data
they produce on platforms and in ecosystems, and secondly transfer such data from
platform to platform, cloud to cloud, thing to thing or in-house. A right to access and
transfer data could have several benefits; it benefits dissemination of data, creativity
and innovation in connected markets and it promotes competition between platforms,
clouds and ecosystem providers. Creativity will be enhanced because necessary data—
being the raw material for new innovations—will be more broadly disbursed. It will
also benefit consumers having a disbursed and disseminated data commons for the de-
velopment of ideas, innovations, and the exchange of knowledge.

KEYWORDS: access, DMA, portability, Digital Markets Act, access and transfer right,
intellectual property law

JEL CLASSIFICATIONS: K00, K20, K21, K31, K42, L11, L14, L22, L23, L24, L41, L42

I. INTRODUCTION
The world is creating more and more data, and the digital economy is built around
data-driven business strategies. New service-providing platforms have business mod-
els in which data collected from both business users and private users are essential.
However, these platforms do not share their data with their clients. The data are not
normally covered by property rights. This does not mean that the data collected are not valuable. The global flow of data is already worth more than the international trade of goods.1 Thus, access to data will be the key for creating wealth and success in the market for the future. Already, data are traded and not freely accessible, even though there is no proprietor of the data collected by everyday devices, distributed to the cloud and reused for other purposes. In fact, such data are hard to come by and only a few entities have the right to access the stream of data flowing on the internet.

So, if the data are generally free, non-exclusive and not subject to competition, why are they so difficult to access? The reason is that the infrastructure for collecting, storing and distributing data is normally embedded behind technology barriers; moreover, there are legal and behavioural barriers to access. The data are thus technically difficult to access, as well as being obscured behind a thicket of property rights, including intellectual property rights (IPRs)—or, in the case of personal data, they might be off-limits due to the General Data Protection Regulation (GDPR). The collection and storing of data on platforms or in clouds might also be done under restrictive agreements. The platform or cloud provider enters a contract with the platform or cloud user, and thus secures not only the right to store the data but also the rights to analyse and make use of them for its own benefits. Platform providers do not let the business users of their platforms access the data they themselves generate. Thus, the data, while not covered by any property rights, are generally accessible only to the intermediaries, the platforms. For the platforms, the data form the basis of their business models, and are vital for their business success. Data make it possible for platforms to provide personal ads or services, for example, or to nudge users to spend their attention on specific media messages and news items.2

The persons or processes that generated the data are not guaranteed access to them. Instead, the legal system around the data, as it is currently set up, seems to benefit the system leaders—the gatekeepers—in the virtual ecosystems being developed around e-platform ‘silos’. Amazon, Apple, Google, Facebook and the like are currently the most visible assemblers of data, since they not only monitor users through their own services but also control the clouds of their respective ecosystems. They are often the only platform service providers that firms can turn to for cloud space to store data and other connected services such as data analytics and predictive modelling. These firms are the most visible gatekeepers, but in the arena of the ‘industrial Internet’, where data will be transferred from thing to thing, T2T, other firms might become the large assemblers of data.

The platform providers can become the masters of their respective data ecosystems and hoard the data; generally, they do not trade or share data.3 Several

---

economists point to the fact that direct and indirect network effects have become relevant because of recent progress in data storage and data analytics technologies.4 The economists Prufer and Schottmüller have, in a recent and well-received paper,5 identified that data-driven markets tend to tip in the favour of one provider as a result of even slight differences in the amount and quality of data, and when such a market tips, it is difficult to re-establish competition other than granting access to data. Moreover, the economists have also shown that superiority in data on one market may be leveraged to create market dominance on neighbouring markets, should a data-driven business model be implemented.6

When a market has tipped due to data-driven indirect network effects, new firms are deterred from entry, and even if they have developed revolutionary technology or so-called disruptive innovations, they may not be able to alter the market structure. Indeed, when a firm holds a monopoly or quasi-monopoly position based on data-driven indirect network effects, it could be declared that the market is failing.7 The market itself cannot create competition.

The platform and cloud service agreements which a business user needs to sign are often skewed to the benefit of the provider, while the brick-and-mortar firm (business user) must provide data and is both contractually and technically locked-in with their platform provider. For example, the agreements do not include a right to access the data that the business user is generating on a platform, but they do include clauses regarding non-assertion and non-reverse engineering. There is moreover no coherent technical standard that facilitates the transfer of data between platforms or clouds. Indeed, porting data from one provider to another can be excessively difficult and expensive for a small firm.

The current probe by the EU Commission of Amazon Marketplace should also be mentioned as an example of the development of data use catering to the digital economy.8 In 2019, the European Commission opened a probe into Amazon’s use of data generated by its third-party merchants (business users) on its platform. The idea was to assess the dual role of Amazon, given that it hosts other merchants, but also competes with them. There were concerns that Amazon could be using data about its competitors’ products and customers to its own advantage.9 It seems that Amazon is using data it collects from its competitors’ business transactions on Amazon Marketplace to set up or intensify its own

6 ibid.
services or product lines, in competition with the business users, while not granting them access to said data.\footnote{Bjorn Lundqvist and others and the BRICS teams, ‘Chapter 7. Exclusionary and Unfair Unilateral Practices in Reference to Platforms’ in Ioannis Lianos and Alexey Ivanov (eds), Digital Era Competition: A BRICS View, <https://publications.hse.ru/en/books/321442247> accessed 12 September 2022.} Other large platforms, such as Google and Facebook, also collect large amounts of data from both business users of their intermediate services and third-party websites. They can then use these data in competition with their business users, for example publishers.\footnote{The CMA sector enquiry indicated that Google and Facebook collect data from several sites, both connected and not connected to their respective ecosystems. cf CMA (2020) Final Report ‘Online Platforms and Digital Advertising Market Study’, 49 et seq, <https://assets.publishing.service.gov.uk/media/5fa57668fa85f788db46efc/Final_report_Digital_ALT_TEXT.pdf> accessed 10 December 2021.}

If this continues, the platform providers will hold large amounts of data collected through their dominant platforms and soon perhaps also the data collected through IoT devices. This would enable them not only to succeed in their own core markets, based on what they do on the world wide web but also to integrate downstream, onto the markets of the brick-and-mortar firms. If they hold data for certain brick-and-mortar markets, they will be able to predict and nudge the consumers as regards what device to buy, what services to use or what news to read. For example, by knowing what news, refrigerator, car or kitchen an individual would prefer to consume, platforms can provide such personalized items before the media house, refrigerator, car and kitchen producer is able to do so. Indeed, the platforms could in such case leverage their control over the data to gain market power on regular brick-and-mortar markets, while nudge consumer to purchase their products.

The European Commission has identified this problem and that brick-and-mortar firms, especially small and medium-sized enterprises, face difficulties with accessing and porting data. Therefore, it has stated that firms should be given the possibility to access and port data—especially vis-à-vis the so-called gatekeepers. The newly enacted Digital Markets Act contains \textit{ex ante} rules that would apply to large platform providers that \textit{inter alia} stipulate a bilateral right for business users of gatekeepers’ platforms to access and port non-personal data.\footnote{The Data Free Flow Regulation contained a call for self-regulation of the right to port data (Art 6). European Commission, Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on the framework for the free flow of non-personal data in the European Union, SWD/2017/0304 final - 2017/0228 (COD), Brussels, 13.9.2017 (Impact Assessment); Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, COM (2017) 9 final, 10 January 2017.} The first part of the article will discuss and present the Digital Markets Act, while the second part will discuss that the rules in reference to access and transfer of data are difficult to reconcile with the intellectual property legal system, and the gatekeepers may have IPRs that could prevent such access. Moreover, the rules of data privacy under the GDPR prevent bilateral access and portability from being effectively and efficiently used in the digital economy. Competition law may possible in theory be applicable. But, as the author shows, business users face institutional and procedural problems gaining access to data under Competition law. To solve this conflict, the author proposes, at the end of the article, the creation of a new form of right for the digital economy: an
access and transfer right (ATR) that may be stand-alone or included in the Digital Markets Act, or in a modernized and amended Data Act.

II. THE DIGITAL MARKETS ACT—EX ANTE REGULATION IN REFERENCE TO DATA

In December 2020, the European Commission published a proposal for a Digital Markets Act, which both includes ex ante rules and gives the Commission new regulatory tools to address certain platforms with gatekeeping capabilities. It is been hailed as something just short of a revolution: a regulation levelling the playing field in an arena where the large platforms have had free rein for too long and the regulation was enacted in July 2022 to take effect in 2023.

The Digital Markets Act indeed opens for a new interoperable internet, where the so-called gatekeepers are restricted. Leveraging, including self-preferencing and other forms of abuse, is prohibited. However, in reference to creating a levelled playing field in relation to access and use of data, there may be some hidden limitations to a genuinely interoperable use of services and flow of data that can be used by the gatekeepers providing so-called core platform services to their business users.\(^{13}\)

It should be clear that Article 6 paragraphs (1), (9) and (10) in the regulation, read in combination, stipulate an obligation for gatekeepers to give access and transfer data to their business users, to a level that could be regarded as an ATR for business users vis-à-vis gatekeepers. A right that business users, regardless of size or whether also being a gatekeeper, could presumably go to court to claim. These provisions state that the gatekeepers are de facto not allowed to use the data generated by a business user on the platform, in competition with the business user (see also Article 5 (1)). Interestingly, the obligation in Article 6 (1), but not the obligations in (9) and (10), reflects that business users have some sort of preferential right to the data generated, vis-à-vis the platform provider. Indeed, it is a bilateral, preferential right to each data point.\(^{14}\)

According to the Digital Markets Act, the gatekeeper retains the prerogative to make all data available to all users. Yet, in parallel, business users have been granted a data advantage vis-à-vis the gatekeepers. Indeed, the combination of Article 6 paragraphs (1), (9) and (10) implicitly creates a form of compulsory access obligation that mirrors a limited property right to the data generated by the business user on the platform—ie, a type of property granted to the business user. The right to access can also be traded, or at least access should be given to third parties contracted by the business user to act as processors of this data on behalf of the business user. The combination of the obligations stated in Article 6 of the Digital Markets Act amounts to an ATR for the business user, yet the question is whether it is an overriding or countervailing right that would keep gatekeepers from using their IPRs to prevent access.

\(^{13}\) For a definition of a core platform service and a gatekeeper and how the obligations for the gatekeepers are triggered, please see the proposal for the Digital Markets Act, \(<\text{https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en}>\) accessed 10 December 2021.

\(^{14}\) The obligation stipulated in Art 6(1) of the Digital Markets Act almost mirrors the right held in Art 7 of the database directive.
The preamble to the Digital Markets Act solemnly claims that the purpose is to ensure that gatekeepers do not undermine the contestability of core platform services as well as the innovation potential of the dynamic digital sector by restricting the ability of business users to effectively port their data, business users and end users should be granted effective and immediate access to the data they provided or generated in the context of their use of the relevant core platform services of the gatekeeper, in a structured, commonly used and machine-readable format. This should apply also to any other data at different levels of aggregation that may be necessary to effectively enable such portability. It should also be ensured that business users and end users can port that data in real time effectively, such as for example through high quality application programming interfaces. Facilitating switching or multihoming should lead, in turn, to an increased choice for business users and end users and an incentive for gatekeepers and business users to innovate.\(^\text{15}\)

Thus, so-called inferred data, where the gatekeeper has drawn some conclusion from the dataset, should also be made accessible. Drawing the line between data that originate from the business users and data that originate from the business (model) of the platform can be very difficult. Indeed, the preamble claims that data generated by business users and end-users, as well as data inferred from that data, should be encompassed by the obligation, but it can be difficult to identify the boundaries for that dataset in a given case.\(^\text{16}\)

The preamble continues by stating: ‘[i]n order to ensure that business users have access to the relevant data thus generated, the gatekeeper should, upon their request, allow unhindered access, free of charge, to such data. Such access should also be given to third parties contracted by the business user, who are acting as processors of this data for the business user. Data provided or generated by the same business users and the same end users of these business users in the context of other services provided by the same gatekeeper may be concerned where this is inextricably linked to the relevant request. To this end, a gatekeeper should not use any contractual or other restrictions [author’s italics] to prevent business users from accessing relevant data and should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required under Regulation (EU) 2016/679 and Directive 2002/58/EC. Gatekeepers should also facilitate access to these data in real time by means of appropriate technical measures, such as for example putting in place high quality application programming interfaces.’\(^\text{17}\)

The text above indicates that the model for data access imagined by the Commission is that the gatekeeper makes a data access application programming interface (API) available to business users. The gatekeeper is not allowed to use

---


16 Possibly, a way to address this is to require the use of blockchain, with rights for the business users to access the blocks reflecting the definition in the art 6 (1), (9) and (10). cf Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final.

contractual or other restrictions to prevent such access. Is this a right overriding any and all IPRs held by the gatekeeper? The main question is whether this gateway to access and portability of data is in fact such a revolutionary tool for creating interoperability, or whether, in the end, intellectual property legal systems or the GDPR will de facto prevent data access and portability.

III. LEGAL CONTROL OF DATA ON AND BY PLATFORMS

The fact that the internet content layer was not subject to either heavy regulation or a functional market regulation during its early development should invite curiosity. Though there is now an emerging consensus that big tech firms must be tamed, as the Digital Markets Act clearly indicates, that has not always been the case. The policy choice in both the USA and the EU throughout the 20th century was to treat the internet not as a telecom network or as a service subject to sector-specific regulation, but as an information society service. As such, the internet was subject to significantly less regulation than either the telecommunication industry and services or the broadcasting media sector, with editorial and constitutional control. The policy choice by both the USA and EU prevented the development of a general economic law (Wirtschaftrecht or droit économique) or market law for the digital economy. The enormity of this policy choice should not escape us, as it created a curious pattern: while the cables and radio waves used to convey the internet and media were regulated, the content on the internet—be it information such as news and messages or data being mined or harvested—was largely unregulated (and remains so to this day).

The data and the information (as such) they encompass are thus not currently covered by property rights, regardless of how private and valuable they are. No one owns personal data, although the ‘data subject’ in the EU retains some rights in regards to the data, under the GDPR. Moreover, economic rights (ownership)
to data can co-exist with personal data protection. Though the data are personal in
the sense that individuals hold rights to them under the GDPR, economic rights to
the data can be held by other entities.\textsuperscript{24} While the personal (or consumer) manda-
tory porting right (Article 20 GDPR) is not financial, it may serve as a source of
competition.\textsuperscript{25} In fact, it works as a consumer protection rule. Individuals have the
right to port data and that right cannot be contractually eroded or derogated.
However, it is in relation to non-personal data, especially in reference to the ‘indus-
trial internet’, that the discussion about property rules and a porting right has
flourished.

This notwithstanding, if an individual piece of data (personal or non-personal)
fulfils the requirement for IPRs, it can be covered by copyright.\textsuperscript{26} Indeed, both per-
sonal and non-personal data can be protected for the benefit of platform providers.
Technical protection measures (TPMs), cf Article 6 of the Directive 2001/29/EC of
the European Parliament and of the Council of 22 May 2001 on the harmonization
of certain aspects of copyright and related rights in the information society
(InfoSoc), can prevent access to copyright-protected content and unfortunately also
to unprotected data. ‘Hacking’ or breaching TPMs to gain access to unprotected
data can be a violation of Article 6 InfoSoc. Moreover, the gateways to platforms, the
APIs, may be copyright-protected in EU law, thus restricting access.\textsuperscript{27} Interestingly,
late in the process text was inserted in one of the recitals, reading ‘[f]urthermore, the
gatekeeper should not be allowed to engage in any behaviour undermining interop-
erability as required under this Regulation, such as for example by using unjustified
technical protection measures, discriminatory terms of service, unlawfully claiming a
copyright on application programming interfaces or providing misleading informa-
tion. Gatekeepers should not be allowed to circumvent their designation by artifi-
cially segmenting, dividing, subdividing, fragmenting or splitting their core platform
services to circumvent the quantitative thresholds laid down in this Regulation’.\textsuperscript{28}
What effect the text will have is uncertain. Can the Regulation limit the possibility
for gatekeepers to make use of injunction under intellectual property law to prevent
infringements? Probably not, while the gatekeeper may violate the Digital Markets
Act and be liable under general EU law.

Platforms can also claim that the datasets they collect are trade secrets as defined
under the new EU directive,\textsuperscript{29} or in the case of personal data, might be off-limits

\textsuperscript{24} Josef Drexl, ‘Designing Competitive Markets for Industrial Data - Between Propertisation and Access’


\textsuperscript{26} Jacopo Ciani, ‘A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to
the Internet of Things: Towards a Wider “Holistic Approach”’ in Mor Bakhoum and others (eds),
Personal Data in Competition, Consumer Protection and Intellectual Property Law. MPI Studies on Intellectual

\textsuperscript{27} In the EU, APIs could possibly be considered copyright-protected, while the US Supreme Court recently
in Google LLC v Oracle America, Inc, 593 US 18-956 (2021) found that APIs fell under the fair use
exception.

\textsuperscript{28} DMA recital 70.

\textsuperscript{29} cf Art. 3 of the Trade Secret Directive and preamble 16, stating that ‘Reverse engineering of a lawfully ac-
quired product should be considered as a lawful means of acquiring information, except when otherwise
under the GDPR. Large players may use the GDPR to refuse access to data, also under the rules in Article 6 of the Digital Markets Act. Owing to the great uncertainty about what is actually restricted by the GDPR, and the *de facto* difference between data protection authorities’ GDPR application and the regulation’s theoretical reach, large technology firms use GDPR offensively and limit their data-sharing activities far beyond the apparent obligations of the GDPR.\(^{30}\) In fact, empirical evidence shows that when the GDPR was introduced, data-driven markets suffered from increased concentration.\(^{31}\) However, perhaps the biggest hurdle to gaining access to the data is that the platform providers, when storing data in databases or in a private centralized blockchain, could most likely hold *sui generis* database protection under the 1996 directive.

The application of the intellectual property rules in reference to the obligation in the Digital Markets Act can perhaps be denied. In the end, it might be found there is no infringement inherent in the access and re-use of data by business users. Yet the rights described above, together with the right to trade secrets and the fact that personal data can be claimed to be off-limits under the GDPR, seem to create enough uncertainty that gatekeepers may choose to deny that the obligation to grant access to data in the Digital Markets Act should be applicable since such access and re-use could allegedly infringe upon the rights and obligations of the gatekeepers.\(^{32}\)

It is true that business users also have tools for accessing data under the intellectual property law system. The data mining regulation in the (new) Software Directive, in conjunction with the Digital Markets Act, could perhaps open the gates to allow access to the gatekeepers’ data. The reverse engineering doctrine in the Software Directive could also perhaps be used together with the Digital Markets Act to breach the gates. However, the application of these exemptions is uncertain at best and may result in litigations.\(^{33}\)

Given these uncertainties, a more comprehensive right to access and port data should be enacted for the benefit of business users of platforms. It needs to be clarified whether the Digital Markets Act is capable of creating access and portability of data unilaterally or in combination with the countervailing rights of data mining and reverse engineering in the area of copyright. Should the rules in the Digital Markets Act be viewed as creating an obligation for gatekeepers to actually allow use and access also of subject matter protected under intellectual property law or as trade contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by law'.


\(^{33}\) ibid.
secrets (when held by the platform or a third party)? Or is the Digital Markets Act a reverse engineering—data mining—tool, for business users and end users to apply? Is it a development of the reverse engineering right inherent in copyright law, cf the EU Software Directive, paralleling the data mining exemption under the new Copyright Directive? Rather, it seems that the data collected by the platforms and their data-driven business strategies are encompassed by IPRs and other forms of legal obstacles, which would at least give the gatekeepers a possibility to deny access and have this issue resolved by the court system.

IV. INSTITUTIONAL PROBLEMS WITH COMPETITION LAW

It seems clear that it is difficult to extract an access and porting right under substantive competition law, but major institutional or procedural difficulties exist with a competition-law solution to the problem of accessing and porting data. The tests, eg the exceptional circumstance doctrine, are difficult to apply, and obtaining relevant judgements can take considerable time. Microsoft, Google Shopping and even the Apple case now being investigated by the EU Commission are examples of where the business case for obtaining a judgement is lost long before the judgement is finally rendered. When the judgement is finally received, the data that the business users wanted access to has lost its value, and the relevant market or industry may even often fall into the hands of the dominant firm that committed the abuse.

The established doctrines, such as the exceptional circumstances doctrine or the essential facility doctrine, took decades to develop, and de facto similar cases in the business community are few and far between—even after the implementation of these doctrines on an EU level. Dominant firms use litigation to slow and hamper access to facilities (or to IPRs or technology, for that matter). To imagine that business providers, under the doctrines mentioned here, would be able to get access and port data on a real-time basis could be naïve.

The fact that competition law cannot address the issue of data access and portability is not very surprising. Competition law in Europe (and in the USA), as it has developed during recent decades, is not capable of addressing paradigm shifts in society or the economy. It is a legal system that can be used to make a few adjustments to the competitive environment of highly efficient firms and economies. However, on its own, competition law cannot be the basis for economic regulation of the data-driven economy as such. New systems must be developed to regulate a new economy and new legal systems, including property rights.

37 It took the EU Commission seven years to render a decision in the Google shopping case, and the case is still lingering in the courts. The Microsoft case saga was also long. Few, if any, believing that in the end, Google (or Microsoft, for that matter) will lose their market power as a result of the EU Commission’s decision.
Nevertheless, competition law may have several benefits and uses in the data-driven economy. The anticompetitive issues raised in reference to platforms should be judged under competition law, such as self-favouring—when platforms treat the offers of competitors differently from their own offers when providing access to supply and sales markets; leveraging market power—directly or indirectly impeding competitors on a market in which the respective undertaking can rapidly expand its position even without being dominant, provided that the impediment is likely to significantly obstruct the competitive process; and hindering interoperability and data portability—making the interoperability of products or services, or data portability, more difficult and thereby impeding competition. When such breaches have been identified, data access and portability may be a suitable remedy on a case-by-case basis. However, competition law has its limitations, and cannot be used to create general rights schemes (\textit{erga omnes}) to be applied \textit{ex ante}. Indeed, property rules are the fundamental \textit{ex ante} rules, while they require the implementation of something akin to a property system.

Competition law is a sophisticated tool, designed to address certain inefficiencies in highly core service-driven, old-economy firms. It is not truly suited to addressing major changes in the economy; it involves too many steps to identify Proving market dominance in data-related markets is a difficult undertaking and highly case specific. Similarly, the very stringent requirements for establishing abuse were developed for the old economy and may need to be adapted to those related to the data-driven economy. It is also very difficult to establish open data streams as a remedy under competition law. Finally, the enforcement system of competition law does not seem sufficiently effective to guarantee competitive markets for the mass phenomenon of data lock-ins caused by connected devices. Hence, a better approach could consist of sector-specific, competition-oriented property regulation.

Indeed, forcing collaboration based on competition law is difficult and rare. For such a remedy to work, an authority or independent entity needs to be put in charge, but mandating firms to collaborate is still difficult when they have no desire to collaborate. The only real case where firms were mandated to collaborate is the US Aspen Skiing case, which required ski resorts to collaborate to provide joint ski pass.\textsuperscript{38} The EU Microsoft case did include a requirement for Microsoft to share source code etc, but not to collaborate; at any rate, it was a very difficult remedy to uphold.

All in all, while obstruction of interoperability, data collection and the subsequent gatekeepers’ use of data to enter their customers’ markets could be addressed as leveraging, self-preferencing or obstruction under Article 102 TFEU, access to data \textit{erga omnes} is a difficult remedy to create.

V. AN ACCESS AND TRANSFER RIGHT FOR DATA?

Generally, the Commission needs to clarify whether the rules being drafted in the Digital Markets Act should be viewed as creating rights. If so, are these rights that business users can genuinely use to access also intellectual property law-protected subject matter (held by the platform or a third party)?

As purported above, there is ample reason for enacting an ATR, which would benefit business users of platforms.

Can a right to data be negative in the sense that it grants neither exclusivity of data nor a right to refuse other parties to use individual data points, while at the same time including an ATR? That would imply that business users would have a right to access data and a right to transfer data that reflects the provider’s quantitative data collection activities on a platform, to a different provider, without being locked into the first platform. Could this be achieved without legislation? Probably not; new legislation and even a new right would likely need to be implemented—in the form of a right for business users of platforms to port sales and user data.

One solution could be to amend the new Digital Markets Act to clearly visualize a reverse engineering and decompilation tool combined with a data mining exemption that benefits business users, while clearly stating that a gatekeeper may not prevent a lawful business user of its platform from accessing and porting its own data. This could be included in the Digital Markets Act, stipulating not only an access and porting obligation for the gatekeepers but also a countervailing ATR for business users that offsets the rights held by the gatekeeper. This countervailing measure should thus be available only for use against the core platform providers—the gatekeepers.

Indeed, the indispensable attribute here is that an ATR for business users of platforms must be accompanied by the appropriate legal and technical tools for gaining access to the data; these tools must be able to penetrate contingent subject matter that is protected by intellectual property law. The Digital Markets Act could be given a property angle, or could be connected to a non-waivable reverse engineering and data mining right, extended to cover the situations addressed by the Digital Markets Act. Another alternative could be to state that the rights of the gatekeeper or platform provider (the TPM creator, as provided in Article 6 of InfoSoc, the creator of a database, as provided in Article 7(1) of Database Directive, the copyright owner, in accordance with applicable copyright legal systems, or the trade secret beneficiary) cannot be exercised by the platform provider in order to prevent access, porting or re-use of data, beyond the limits set by the regulation. This would amount to creating a countervailing right or exemption for business users of platforms.39

It should also be the obligation of the gatekeeper to store the data in such a way that third-party rights are not violated by the access and portability of the business user. Such an obligation should be encompassed in the Digital Markets Act. Moreover, the business users should only be limited by GDPR to the same extent as gatekeepers. The need for a levelled playing field call for equal access under GDPR for gatekeepers as well as business users using the same platform. The gatekeepers need to either provide similar access to business users through consent provisions or limit their own access under GDPR to personal data, should the individual in question refuse to encompass business users in the consent given to the platform.

39 The proposed Data Governance Act also addresses the interface between the access right to public data in the PSI Directive and third-party IPRs, and both the PSI Directive and the proposed Data Governance Act address the issue of database rights held by government authorities. Accordingly, government authorities should not be able to claim that right vis-à-vis a business user. cf Proposal for a regulation of the European parliament and of the council on European data governance (Data Governance Act) COM/2020/767 final.
A second solution could be to grant a ‘proper’ property right to the business users: an ATR vis-à-vis all platforms. Such a right could be included in an updated version of the Database Directive, or in the proposed Data Act, granting a business user an ATR to the dataset that represents ‘its’ generated data on a platform, when the business user has invested time and effort, qualitatively and/or quantitatively, in the platform. When the investment reaches the degree that the selection or arrangement of the data collection that was provided to the platform is original, or the ‘author’s own intellectual creation’, or when the business user contribution to the platform is substantial, the user would obtain a *sui generis* dataset right to the data generated on the platform.40

The ATR to the business user’s data should thus be triggered when the business user holds *sui generis* protection to the database or dataset it has created or contributed to the platform. An example of this dataset could be a collection of information references regarding a business user’s product line that is marketed on the platform, when the business user invests sufficient time and effort to reach the triggering level for database protection. The included data should also have reached a volume that reflects a value for the business user as well as for a potential market. The platform provider should then be obligated to respect the business user’s ATR to the dataset generated by the user’s action on the platform, *inter alia* relevant sales and customer data generated by the actions of customers and users of the dataset that the business user has furnished to the platform. Technically, the dataset could be accessed through an API. The platform provider normally retains a *sui generis* database right in reference to all activities on the platform, but cannot prevent the business user from accessing and porting the dataset associated with the business user’s rights and data.41 The business user should have a right to port the dataset in its entirety or substantial parts thereof. The business user’s ATR should also cover situations where they wish to access and use non-substantial parts of the database that reflect their data in a ‘repeated and systematic’ manner; cf Article 7(5) of the Database Directive. Indeed, neither Article 7(1) nor Article 7(5) of the Database Directive should be applicable vis-à-vis a platform provider in reference to a user’s data.

The different ATRs described above respect the platform provider’s business model. Indeed, the business model of the platform should still be respected, given that the platform provider retains a *sui generis* database right and can access and use any business user’s data. The platform provider will have access to individual business users’ data points and can build a general database that reflects the aggregated data of all business users; such a database will likely be necessary to provide the platform service and respect the platform provider’s business model. The platform provider will have the possibility to obtain the aggregated data from all business

40 Indeed, business user data are platform data—data that are collected by sensors, created through business user activities or contributed by the business user. As discussed below, the aggregated data should be controlled by the platform provider.

41 An updated version of the Database Directive could clarify that the platform provider should hold the *sui generis* right to the database and thus considered the main investor and bearer of the risk for setting up that database. The legislator should not pursue a strategy to respect joint ownership (makers) of the *sui generis* database for aggregated data. *Compare* Josef Drexl. ‘Data Access and Control in the Era of Connected Devices’ (2018) Study on behalf of the European Consumer Association BEUC.
users—a dataset not covered by the business users’ ATR rights. Moreover, the platform provider should have the right to provide public access to the general database encompassing the aggregated data. Therefore, the platform provider should bear the cost of setting up and storing the database and datasets.

VI. SOME CONCLUDING THOUGHTS

Ownership is not defined at the EU law level, and the Member States’ legal systems define ownership differently. There is a dichotomy between the civil law and the common law understanding of ownership. While civil law recognizes a limited number of property rights and a limited number of legal objects that can be subjected to these property rights, common law is more flexible and allows private parties more freedom in the types of ownership interests that they can create. In civil law jurisdictions, property is based on law or legal acts. Ownership is thus an absolute dominion encompassing all the listed rights to the relevant object. However, in the common law tradition, the notion of ownership includes a variety of different rights to the same property. Ownership can be a sliding scale. The ATR suggested in this article is a bundle of rights that does not include several of the rights normally included in a property right.

Previous attempts in academia to promote a producer data right have argued that producers should have a right to individual data points, and, indeed, any information they produce. However, the proponents for such a property regime have been unclear as to whether the protected subject matter encompasses information or merely syntactical elements of data. These two aspects may create a risk that the producer data right develops into a stranglehold on the right to information, with the potential to greatly increase transaction costs. It could increase the bureaucracy of data-driven markets, and it is unclear whether such a right would truly benefit innovation and the creation of data markets and data-driven markets.

The concept proposed above for an ATR would not entail such risks; in addition, it provides a clear distinction: information will be accessible, but there is no exclusivity to information or the syntactical elements of data (ie, 1s and 0s). Moreover, the ATR is not vested in individual data points.

A fundamental thrust of arguments that support the introduction of a property right to data is how technology advancements have brought us to a point where data and information are separated from individuals’ personalities and skills. The new paradigm implies that data can be controlled, collected, and stored, ie, that they have

44 ibid.
45 van Erp (n 43).
46 ibid.
48 Several authors discuss this, see for example ibid. and Drexl (n 42).
left the realm of thoughts and ideas to become tangible items, at least in the virtual world. Data are the new raw materials for many diverse services. Data are also the cornerstones for developing models to predict future events.

Indeed, one fact cannot be avoided in this context: a property legal system is an allocation-of-power regime that distributes and disseminates power. Such allocation of power, as discussed above, can be viewed in various ways: a reward for labour investment, an expression of personality, a basis for economic freedom, or in terms of economic utility (efficiency-based). In several aspects, various justice-related arguments have been presented in regard to the paradigm of dominance of the strong and powerful over the weak in an unregulated scenario, or when the legal system promotes the wrong group over other groups in society. With this viewpoint, the economic rights inherent in property are not an end in themselves, but a means to protect something else—often the investment in capital or time to create tangible goods or intangible information—which on a grander scale implies that property protects the distribution of opportunities and the function of the liberal market economy as such. In essence, a property right is the foundation of a legal system and a major function in the protection of the liberal economy. Clearly defined property rights enable transactions and efficient allocation of resources. Indeed, a property regime reflecting ATRs is necessary, because an ATR reflects a reward for labour and is an expression of personality, or a reward for an investment, while it directs the data to the entities that need them for trade and innovation, ie, business users’ data to business users. The new right system also diffuses the inherent power of information resting in the hands of the few and disseminates data among several stakeholders, to promote innovation, progress and the creation of markets for trading data. An ATR will increase trade in data and will function as a tool to increase the volume of data on the market. Moreover, licensing ATRs will introduce a new market, which could become an additional layer for competition and prosperity.

The ATR also creates something more: it increases potential access to information in the commons. Implementing strong ATRs will transfer data from the gatekeepers to users that can transfer or sell data, or even make the data freely available. Indeed, data will be more available than before, giving journalists, activists and civil society the possibility to access data, because these will be traded and marketed to a larger extent than when platforms hoard them. The vision or dream of having a free and democratic internet, where data and services are freely available to all, is more likely to be fulfilled with an ATR than without one.

---

49 Daria Kim, ‘No One’s Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy’ (2017) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 697.


51 For a similar list see Heiko Richter, 'The Power Paradigm in Private Law' in Mor Bakhoun and others (eds) (n26) 552 et seq.
