



# The Proposed Digital Markets Act and Access to Data: A Revolution, or Not?

Björn Lundqvist

Published online: 23 February 2021

© Max Planck Institute for Innovation and Competition, Munich 2021

The recently published proposal for a Digital Markets Act will have gone unnoticed by few. The proposal includes *ex ante* rules and gives the Commission new regulatory tools to address certain digital platforms with gatekeeping capabilities. It has been hailed as something just short of a revolution – an unfair competition law regulation levelling the playing field in an arena where the large digital platforms have reined free for too long.

The proposed Digital Markets Act indeed opens up for a new interoperable internet where leveraging, including self-preferencing and other forms of abuse conducted by the gatekeepers are restricted. However, regarding the creation of a levelled playing field in relation to access and use of data, there are possibly some “hidden” limitations to a genuine interoperable use of services and flow of data from the gatekeepers, providing so-called “core platform services”, to their business users.<sup>1</sup>

It should be clear that Art. 6(a), (h) and (i) in the proposed regulation, in combination, stipulates an obligation for gatekeepers to give access and transfer data to their business users, to an extent that could be regarded as an access and portability right for business users vis-à-vis gatekeepers – a right that business users could presumably go to court to claim. It stipulates that gatekeepers are not allowed to use the data generated by business users and their end users on the platforms, in competition with the business users, while the obligation in Art. 6(h) and (i) reflects that business users have some sort of right to gain access, port and re-use the data generated by their action on the platforms. This means there is a right to receive a

<sup>1</sup> For a definition of a core platform service and a gatekeeper and how the obligations of gatekeepers are triggered, see the proposal for the Digital Markets Act, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en>.

B. Lundqvist (✉)

Associate Professor of European Law, Head of EU Law, Co-Director of the European Economic LLM programme, Stockholm University, Stockholm, Sweden  
e-mail: bjorn.lundqvist@juridicum.su.se

steady stream of data from the platforms – a stream that can also be transferred to third parties.

This could be a game changer. The combination of Art. 6(a), (h) and (i) creates a compulsory access and use regime benefitting the business users, stopping just short of a property right, to the data generated by the business user and its end users on the platform.

However, the issue is whether the gateway for business users to access data is in fact such a revolutionary tool for creating interoperability, or whether the intellectual property legal system, trade secret rules or GDPR will in the end, de facto, prevent data access, re-use and portability. It seems obvious that the gatekeepers will try to claim that the obligation to give access, and for business users to re-use the data generated on their platforms, should not be enforced because the data are walled in by intellectual property rights, represent trade secrets or concern personal data.

Data as such is not covered by any property right irrespective how valuable or personal the data is. Yet, data can still be protected. Technical protection measures (TPMs, cf. Art. 6 InfoSoc Directive) can prevent access to copyright-protected content and unfortunately also unprotected data. “Hacking”, or breaching TPMs to gain access even to unprotected data can be a violation of Art. 6 InfoSoc Directive.<sup>2</sup> Moreover, the “gates” to platforms, the application programming interfaces (APIs), may, perhaps, be copyright protected, and thus can be used to restrict access both in practice and legally.<sup>3</sup> Furthermore, a big hurdle for gaining access to data is that the gatekeeper, when storing data in a database, could most likely claim *sui generis* database protection under the 1996 Directive and, depending on the technical set-up, the business user, utilizing the obligation in the proposal, could both access and use data to an extent that an infringement of the *sui generis* right is at hand.<sup>4</sup>

So, will the access to data be off limits for business users? The application of the above rights to refuse the application of the obligation in the proposal can perhaps be denied. The proposal could be viewed as creating an overriding obligation to grant access that “trumps” any sort of rights held by the gatekeeper. Thus, in the end, there is no infringement inherent in the access and re-use of the data by business users. Yet, the rights describe above together with the rules regarding trade secrets, and that personal data is off limits, seem to create enough uncertainty that gatekeepers may choose deny that the obligation to grant access to data in the proposed Digital Markets Act should be applicable. This is unfortunate.

<sup>2</sup> Gustavo Ghidini (2010), *Innovation, Competition and Consumer Welfare in Intellectual Property Law*, Edward Elgar, p. 114.

<sup>3</sup> See the US case *Google LLC v. Oracle America, Inc.*, which certainly may have EU policy implications. See the interesting paper discussing APIs, Jörg Hoffmann and Begoña Gonzalez Otero, “Demystifying the Role of Data Interoperability in the Access and Sharing Debate” (29 September 2020). Max Planck Institute for Innovation & Competition Research Paper No. 20-16, Available at SSRN: <https://ssrn.com/abstract=3705217> or <https://doi.org/10.2139/ssrn.3705217>.

<sup>4</sup> *Trading Data in the Digital Economy: Legal Concepts and Tools*. Münster colloquia on EU law and the digital economy III. 1st edn. Baden-Baden: Nomos. pp. 25–58. The gatekeepers can, moreover, claim that the datasets they collect are trade secrets under the EU Trade Secrets Directive, or in the case of personal data, might be off-limits under the GDPR.

It is true that business users also have tools for accessing data under the intellectual property law system. The new data mining regulation in the (new) Software Directive, used in conjunction with the proposed Digital Markets Act, could perhaps bend open the gates to the platforms, to access the keepers' data. The reverse engineering doctrine in the Software Directive could also perhaps be used together with the proposed Digital Markets Act, in analogy, for breaching the keepers' gates. However, the application of these exemptions is uncertain at best.

Generally, the Commission or the European legislator needs to clarify whether the unfair competition rules being drafted in the Digital Markets Act are capable of creating access and portability of data unilaterally, or in combination with the legal tools of data mining and reverse engineering. Should the proposed rules in the Digital Markets Act be viewed as creating an obligation for gatekeepers to grant access to intellectual property law or trade-secret-protected subject matters (held by the platform or third party)? Or is the Digital Markets Act even a developed reverse engineering – data mining – tool for business users and end users to apply?

Notwithstanding the above, some inspiration can perhaps be taken from the 2019 Public Sector Information Directive, which tries to address the issue concerning gaining access to governmental data, even though such data could also be considered off limits due to third-party intellectual property rights, rights held by the government authority, or the GDPR. It stipulates that a government authority cannot utilize its database right so as to deny re-use to public sector data. How about that? Perhaps, at least a similar clarification could be inserted in the Digital Markets Act.

So, to create a levelled playing field with reference to access to data, the proposal for a Digital Markets Act is a revolution, or not? It remains a bit unclear.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.