Rupprecht Podszun[1]

Should gatekeepers be allowed to combine data?

Ideas for Art. 5(a) of the draft Digital Markets Act

Should digital gatekeepers be allowed to gather data from users and combine data from different sources? That is one of the key substantive questions of the Digital Markets Act. It is currently addressed in Art. 5(a) of the draft DMA. There are two problems with the current wording: First, it is not specific enough to work as a self-executable provision. Secondly, it could happen that users are nudged into giving consent easily so that the gatekeepers can continue to expand their sets of personal data, without users having a "real" say and with third parties losing out in competition. In this contribution, I analyse this problem. My suggestion is to resort to a "rating solution": Qualified entities, e.g. trusted data intermediaries, should rate, certify or label the data options offered by the gatekeepers and serve as "data guides" for consumers. I also look at other policy options and at a way to solve a competition problem on the way.

4 June 2021

[1] Prof. Dr., Chair for Civil Law, German and European Competition Law, Heinrich Heine University Düsseldorf; Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich. The author thanks Sarah Langenstein and Philipp Bongartz for their valuable comments. Contact: ls.podszun (at) hhu.de.

I. Problems with the current draft of Art. 5(a) DMA

The digital gatekeepers, i.e. the ecosystems that run the Internet, collect data all the time and try to use these data commercially.[2] Access to a large amount of data is an important competitive parameter, and it raises questions of privacy. Thus, the European Commission introduced a provision in Art. 5(a) of the draft Digital Markets Act to address the issue of data collection by digital gatekeepers.[3] Its prominent position as the first ex ante obligation for digital gatekeepers signalises the importance of this provision.

1. The current wording

In the current draft of the DMA, Art. 5(a) reads as follows:

> "In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:
>
> (a) refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679."

Essentially, this rule provides for a prohibition of merging data from different sources. Yet, the prohibition may be overcome if users consent. Consent needs to be compliant with the General Data Protection Regulation (GDPR) and users need to have a choice. This means, as recital 36 reveals, that there needs to be an offer to provide services without this kind of data-gathering (otherwise the user would only have the "choice" to take it or leave it – which is not choice).

The wording of Art. 5(a) suggests that the DMA is that "strange animal"[4] that some see in it: it has elements of protecting privacy as well as elements of protecting competition. At first sight, the collection and combination of personal data primarily seems to be a privacy issue that is to be dealt with under the GDPR. Yet, in the prominent German *Facebook case* the German competition authority Bundeskartellamt prohibited Facebook the merging of data from different sources to "super-profiles" as an abuse of dominance – thereby framing

[2] Cf. Maurice E. Stucke/Allen P. Grunes, Big Data and Competition Policy, 2016, 4.33.

[3] European Commission, 15.12.2020, 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.

[4] Cf. Simonetta Vezzoso, The Proposed Digital Markets Act: What Kind of (Regulatory) Animal Is It?, 2021, available at https://competitionwave.blogspot.com/2021/05/the-proposed-dma-what-kind-of.html.

these data-related practices as a matter of competition law.[5] The Bundeskartellamt had argued that the violation of data protection rules as laid down in the GDPR amounts to an abuse of dominance by Facebook under national competition law rules equivalent to Art. 102 TFEU. *Caffarra/Scott Morton* argue that Art. 5(a) is directly influenced by this hybrid case.[6]

In the Bundeskartellamt's case, Facebook shall no longer be allowed to merge data collected on Facebook itself (the network), other Facebook services like Instagram, WhatsApp or third-party services where Facebook collects data thanks to its Business Tools. If Facebook loses this possibility, this comes close to an "internal divestiture"[7] of the companies – at least regarding data, one of the key parameters of the Facebook business. It is of high relevance how this issue is dealt with in the DMA.

2. Problems of the current version

The provision currently has two major shortcomings, its vagueness and the option of easy consent. It also does not take the opportunity to address the data access issue for third parties.

a) Unclear terms in the provision

The first shortcoming of the current version of Art. 5(a) is that this rule is too vague to qualify as an ex ante self-executable per se rule. As part of Art. 5 the rule shall be self-executing without a regulatory dialogue (as foreseen in Art. 7 for other obligations).[8] To be self-executing it needs to be exact and precise so that compliance and monitoring are easy to handle.

It may be relatively clear what "personal data" are, what it means to "combine" such data,[9] what qualifies as "other services offered by the gatekeeper" or "third-

[5] Bundeskartellamt, 6.2.2019, Case B6-22/16; the case is available at https://www.d-kart.de/en/der-fall-facebook/ including an update on the current state of the matter (at the time of writing, the case is pending with the European Court of Justice upon reference by the Higher Regional Court of Düsseldorf.

[6] Cristina Caffarra/Fiona Scott Morton, The European Commission Digital Markets Act: A translation, 2021, available at https://voxeu.org/article/european-commission-digital-markets-act-translation.

[7] Andreas Mundt according to the Bundeskartellamt press release of 7.2.2019, available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[8] Facebook is very critical of this approach without the possibility of a "protected first attempt", see the Facebook position paper, "Facebook Comments on the Regulatory Design of the Digital Markets Act", March 2021, p. 2.

[9] Even this may be not so clear, cf. Irish Council for Civil Liberties, "Greater Protection in Article 5 (a) of the Commission's proposal for a Digital Markets Act", 25.1.2021.

party services", yet all these terms used in Art. 5(a) may come under closer scrutiny if dissected by lawyers in proceedings. Even more difficulties in interpretation may arise from the obligation to offer "specific choice", to obtain "consent in the sense of Regulation (EU) 2016/679" and to "present" choice and consent to users.

"Specific choice" is undefined. According to recital 36 of the draft DMA end users shall be enabled "to freely choose to opt-in to [the combination of personal data from different sources] by offering a less personalised alternative."

This seems to mean that users shall have at least two different options, yet it remains unclear what a "less personalised alternative" would entail. Recital 36 continues in stating that "[t]he possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites".

This could be interpreted as meaning that the less personalised alternative requires a complete abstinence from any combination of data. There could be sensible solutions in between, however. It is not clear whether the alternative needs to be equally good or what strings may be attached if users refrain from opting in. For instance, a less personalised alternative could come with significantly reduced features of the products or require payment of a fee.

The European Parliament's rapporteur has suggested to require a "less personalised but equivalent alternative".[10]

It also remains unclear what constitutes proper consent. Taking recourse to the GDPR does not provide an unequivocal solution. The term "consent" is defined in Art. 4 No. 11 GDPR:

> "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

This is not the place to discuss the exact requirements of "consent" in this sense, but it is discernible that terms like "freely given", "specific", "informed", "unambiguous" require interpretation. Lengthy litigation may follow, and that runs counter to the aim of Art. 5(a) DMA to define a clear-cut standard. The Guidelines of the European Data Protection Board give a 30-plus pages briefing of

[10] European Parliament, 1.6.2021, Draft Report on the proposal for a regulation of the European Parliament and of the Council – Contestable and fair markets in the digital sector (Digital Markets Act) (Rapporteur: Andreas Schwab), 2020/0374(COD), Amendment 8.

what constitutes consent in the sense of the GDPR,[11] and it may not be unfair to state that this document is neither conclusive nor uncontroversial.

The ambiguity extends to the question of the right presentation to users. In recital 36 of the DMA it is said that the options "should be proactively presented to the end user in an explicit, clear and straightforward manner."

What exactly does that mean? The standards of fairness that are guiding the DMA require a free and informed decision of end users.[12] What information do users need? Are they still free in their decision if they are influenced or given a poor choice? Will they be able to assess the advantages and disadvantages of several options? Is it allowed to present options in different formats?

The consent requested from users for the use of cookies under the current regime provides an example of what may lie ahead. *Utz et al.* have undertaken research on how users deal with the cookie acceptance buttons that were necessitated by the GDPR. The authors of this study state:

> "We find that users are more likely to interact with a notice shown in the lower (left) part of the screen. Given a binary choice, more users are willing to accept tracking compared to mechanisms that require them to allow cookie use for each category or company individually."[13]

So the exact presentation on screen already makes a significant difference. Does the DMA accept any of the forms?

It has been criticized more generally that the GDPR standard is used in Art. 5(a) DMA.[14] For companies this may mean a risk of double exposure to fines if they violate GDPR and DMA. While this may be seen as a minor problem that could be handled in practice, it is questionable whether the DMA should rely on the GDPR for setting the standard. This makes sense if the rationale for Art. 5(a) is the protection of privacy. If the focus is on different issues (e.g. competition) it may be possible to have a different, possibly stricter approach. Yet, different standards for consent could also be confusing in practice and would mean a double burden for undertakings to check.[15] Data protection activists fear that the requirements in the DMA may undermine the "purpose limitation principle" of

[11] European Data Protection Board (EDPB), Guidelines 05/2020 on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[12] Cf. recital 14 and Articles 5 and 6 of Directive 2005/29/EC (Unfair Commercial Practices Directive).
[13] Christine Utz et al., (Un)informed Consent: Studying GDPR Consent Notices in the Field, 2019, p. 1, available at https://arxiv.org/pdf/1909.02638.pdf.
[14] Romina Polley/Friedrich Andreas Konrad, Der Digital Markets Act – Brüssels neues Regulierungskonzept für digitale Märkte, WuW 2021, 198 (201 f.).
[15] Cf. for the German rule in section 19a Tobias Lettl, Der neue § 19a GWB, WRP 2021, 413 (421).

the GDPR.[16] Art. 5(a) does not seem to require a distinct limitation to certain purposes.

The rapporteur of the European Parliament, *Andreas Schwab*, suggested in his report to amend Art. 5(a) by adding a more specific requirement for consent by stipulating that consent needs to be granted

> "in the sense of Article 6 (1) a) of Regulation (EU) 2016/679; alternatively, the gatekeeper may rely on the legal basis included under Article 6 (1) of Regulation (EU) 2016/679 with the exception of lit b) and f) of Article 6 (1) of Regulation (EU) 2016/679."[17]

This limits the possibility of consent by excluding two of the cases foreseen in Art. 6(1) GDPR. A further clarification should be sought with regard to data from other services of the gatekeeper that are not core platform services in the sense of the regulation, but part of the undertaking.[18]

Art. 5(a) needs to live up to the expectation of being self-executable. Even with the amendment, this does not seem to be the case.

b) Users easily agree

The rule may also be too friendly with data combination (and thus with digital gatekeepers): If the gatekeepers manage to obtain user consent (an exercise they are not bad at, judging by their ability to nudge and guide users in their ecosystems), they gain the permission to combine a wide variety of user data. The consent option in Art. 5(a) is not restricted: Once, consent is given, the companies may still build "super-profiles". The hurdles, as has just been seen, are not clearly defined. What is more: If gatekeeper know to play their users, placing the boxes in the right fields, experimenting successfully with how to make users agree, the effect of Art. 5(a) could be minimal in practice: End users will have to do one more click – and nothing changes for the use of data.[19]

Utz et al. in their research on cookie acceptance pointed out how the design matters into getting users to consent:

> "We also show that the wide-spread practice of nudging has a large effect on the choices users make. Our experiments show that seemingly small

[16] Cf. Irish Council for Civil Liberties, "Greater Protection in Article 5 (a) of the Commission's proposal for a Digital Markets Act", 25.1.2021.
[17] European Parliament, 1.6.2021, Draft Report on the proposal for a regulation of the European Parliament and of the Council – Contestable and fair markets in the digital sector (Digital Markets Act) (Rapporteur: Andreas Schwab), 2020/0374(COD), Amendment 53.
[18] Daniel Zimmer/Jan-Frederick Göhsl, Vom New Competition Tool zum Digital Markets Act: Die geplante EU-Regulierung für digitale Gatekeeper, ZWeR 2021, 29, 40.
[19] Cf. Digitalcourage, "Digital Markets Act: Bündnis fordert Nachbesserungen beim DMA", 26.5.2021.

> implementation decisions can substantially impact whether and how people inter-act with consent notices."[20]

Accordingly, the rather unspecific requirements in Art. 5(a), even if read together with recital 36 and the GDPR, may have little meaning for real-world practice.[21] If the DMA shall protect users from tumbling into data-hungry business models, requirements need to be much more specific and the option to consent easily needs to be reconsidered. Otherwise, the DMA provision runs the risk of being another formalistic obstacle with little impact for users – other than getting on their nerves. Art. 5(a) would be pseudo-solution. Many users may agree, potentially without really considering that they forfeit a fundamental right. Control by big tech companies over individuals thanks to knowledge of all sorts of personal, even highly sensitive data would simply continue. "Surveillance capitalism"[22] would flourish.

This is all the more irritating since users so far have shown that they opt for stricter data protection and less data hungry business models if offered a real choice. The results from the research by *Utz et al.* cited above already indicate this. If facing a choice, only a small number of users agrees with sharing data with other app providers.[23] This was recently underlined by the new Apple Tracking Transparency (ATT) system where users to a large degree decided not to let other companies have access to their data.[24] Even if it is argued that the complexities of the ATT programme and the disadvantages for third parties have not been communicated in a proper way to users, this only shows how susceptible this approach is to guidance, misguidance or nudges.

c) Data access for third parties

Art. 5(a) in its current version may also be seen as a missed opportunity to solve a competitive bottleneck problem. The starting point of the rule is a competitive one: The accumulation of data means that gatekeepers have advantages in competition over competitors that are less successful in reaching customers and obtaining consent. Gatekeepers may raise market entry barriers, the contestability of platforms is reduced and annexed services, e.g. on aftermarkets, are more easily integrated into the digital ecosystem of the gatekeeper. This minimises the

[20] Christine Utz et al., (Un)informed Consent: Studying GDPR Consent Notices in the Field, 2019, p. 1, available at https://arxiv.org/pdf/1909.02638.pdf.
[21] Cf. VAUNET, Positionspapier zum Digital Markets Act, 23.2.2021, p. 3, including the idea of a neutral single sign-on alternative.
[22] Shoshana Zuboff, Surveillance Capitalism, 2018.
[23] For payment data with in-app-sales this is confirmed by an investigation of the Autoriteit Consumer & Markt, Report of 11.3.2019 – Market study into mobile app stores, p. 93.
[24] Flurry, iOS 14.5 Opt-in Rate - Daily Updates Since Launch, 2021, available at: https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

chances in competition for third parties. Recital 36 cites these concerns as the motive for introducing the obligation in Art. 5(a).

Yet, the rule does not look at the competitive angle of data collection. It does not make any reference to the hindering effects of the data combination and it does not address the problem that gatekeepers could possibly succeed in obtaining consent, their free ticket for the ride to data power.

It has thus been suggested to link consent to the duty that gatekeepers share the data obtained in this way with business users more generally. This duty would primarily favour business users that were instrumental in establishing the relationship of gatekeeper and end user. For instance, if a small retailer on a retail platform manages to do a transaction with a consumer, it would be fair, so it is argued, that data is shared with the small retailer and does not exclusively rest with the gatekeeper. It could even be contemplated to share data with a larger group of business users if it is shared with the gatekeepers. In the current form, Art. 5(a) does not really address the competitive problem identified in the recitals.

II. Differing objectives

Before turning to an alternative suggestion for Art. 5(a) it may be worth to reconsider the objectives of this rule. The rule serves a multitude of purposes without clearly favouring one of them.[25]

1. Four different objectives

Four different objectives motivate the provision:

Firstly, the right to privacy – protecting personal data is an objective in itself. In the EU reading this requires that users decide for themselves (as the right-holders over their personal information) what to do with their personal data. But more than that, the GDPR makes it a principle to act in a way that promotes "data minimisation" (Art. 5(c) GDPR), i.e. limit the collection and use of data to what is necessary for the purpose in question.

[25] Cf. Heike Schweitzer, The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Markets Act Proposal, 2021, p. 11.

Secondly, users shall have a choice. Consumer choice has been rediscovered as an element of the market economy.[26] Focussing on this decision-making power (now not as right-holders of privacy rights but as economic actors) strengthens the role of the customer. She is the "referee in the marketplace", the one taking autonomous decision on economic questions.[27]

Thirdly, an even more competition-centred view sees the data question as one of enabling business users to compete: The objective is to ensure a level playing field for business users with digital gatekeepers. These gatekeepers shall not be enabled to extend their reach and to raise market entry barriers.[28] This motive is prominently cited in recital 36.

Finally, a bit less specific, one of the objectives is to limit the data accumulation by digital gatekeepers as the largest and most powerful corporations on earth. This is not just a question of privacy or a better position in competition or respect for consumer choice, but a simple question of power: A company that has personal data at its disposal may wield enormous political, economic and social power over users.

These four objectives speak for a limitation of the use of data in the hands of digital gatekeepers. All these objectives are underlying Art. 5(a) DMA.

2. The German approach in section 19a

It is interesting to compare the DMA draft with section 19a (2) No. 4a of the German competition act (*Gesetz gegen Wettbewerbsbeschränkungen*) in its 2021-version. This version somehow pre-empted the DMA, and here the legislator refrained from making a direct reference to the GDPR and instead focussed on the competitive angle of data combinations:

> "(…) the Bundeskartellamt may prohibit such undertaking from
>
> 4. creating or appreciably raising barriers to market entry or otherwise impeding other undertakings by processing data relevant for competition that

[26] Robert H. Lande/Neil W. Averitt, Using the 'Consumer Choice' Approach to Antitrust Law, Antitrust Law Journal, Vol. 74 (2007), 175; Paul Nihoul in Paul Nihoul/Nicolas Charbit/Elisa Ramundo, Choice: A New Standard for Competition Law Analysis?, 2016, 9. Cf. Josef Drexl, Wirtschaftliche Selbstbestimmung des Verbrauchers, 1998.

[27] This motive plays a larger role in the Bundesgerichtshof's decision on Facebook, cf. BGH, 23.6.2020, Case KVR 69/19. Cf. Rupprecht Podszun, Der Verbraucher als Marktakteur, GRUR 2020, 1268 ff.

[28] On different competition-related theories of harm based on data access cf. Jan Krämer/Daniel Schnurr, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, 2021, p. 2 ff.

have been collected by the undertaking, or demanding terms and conditions that permit such processing, in particular

(a) making the use of services conditional on the user agreeing to the processing of data from other services of the undertaking or a third-party provider without giving the user sufficient choice as to whether, how and for what purpose such data are processed".

The link to free competition is much stronger here: The rule starts with reference to raising market entry barriers and the hindering of competitors while the choice of users is only referenced in this context and not with explicit reference to the style of consent. It needs to be borne in mind that section 19a of the German act (other than Art. 5(a)) is not meant as a self-executable rule.

3. Counter-objectives

With the objectives of Art. 5(a) in mind it should also be clear that combining data is not just a *bad* thing. It is much more convenient for users to navigate within a digital ecosystem if the central operator of that ecosystem knows all relevant data and has an exact user profile at hand. This convenience argument, however, is a weak one: It is often convenient to give up personal liberties, but that should not induce policy choices in favour of restricting freedom.

It is more compelling to raise the innovation defence. Collecting and combining data is part of "Big Data", and big data entails the promise of innovation or of discoveries that could propel progress. It is precisely the digital gatekeepers that hold the data power and the analytical tool to innovate on the basis of data. There may be a certain trade-off with innovation if the provision in Art. 5(a) DMA leads to less generous access to data for Google, Amazon, Facebook, Apple and Microsoft.

Having said that, this argument is probably less strong than it seems at first sight. The innovative steps that will bring about progress are presumably not primarily in the field of e-commerce, advertising or communication. It would need further consideration whether data-based innovation in the fields of healthcare or climate change are really dependent on the merged user data of customers in e-commerce.

III. Rating data options – a proposal to involve trusted data intermediaries

My proposal is to amend Art. 5(a) and to give consumers a real choice by presenting a rating of the different options offered by the gatekeeper. This rating should be provided by trusted data intermediaries, acting as neutral "data guides" for consumers.

1. The key elements of this proposal

This proposal brings in a third party that is an independent organisation that rates, certifies or labels different data approaches put forward by the gatekeepers (and possibly other companies). These organisations would work as guides for consumers and would enable consumers to take a decision without having to read and understand lengthy data policies.

To make it more concrete: A digital gatekeeper would be required by Art. 5(a) to set out a data policy and to offer different options for users. These options are examined by independent data experts (that are called "Data Guides" in this proposal). These experts rate the different options according to the standards they chose – consumer friendliness of the service, data protection or impact for competition. Essentially, the task of the Data Guides is to assess whether users get good value for data when accepting a certain option. Consumers are used to decide about this trade-off when paying with money. In cases where they are paying with data, they need guidance.

In this scenario if a user is about to enter the universe of a gatekeeper she is presented with the different options, offered by the gatekeeper, and gets as an additional information the rating by the independent experts. This could, for instance, be in the form of a rating ("6 out of 10 in terms of respect for privacy, 8 out of 10 in terms of pro-competitiveness, 7 out of 10 in terms of services granted") or with a colour-code as in traffic lights, just for consumers ("green: very consumer-friendly – red: dangerous"). Users would only need to pick the recommendation they like best. It could be technically possible for users to navigate the Internet with one chosen option in the sense of a pre-installed user policy to choose certain data approaches while surfing the web. This would reduce the inconvenience to decide anew from website to website.

In addition to the rating the Data Guides could also act as auditors for compliance with the data policies set out before. In this sense, they would monitor what the gatekeepers do in this field and would help the European Commission in enforcement.

A possible wording of the proposal could be an addition to the current wording of Art. 5(a):

The gatekeeper needs to have at least three independent and neutral data experts to rate its data policies and the options offered to users. The ratings need to be published in a well visible way with the choice screen. The ratings shall communicate the recommendation of the data experts in an easy-to-understand manner. The data experts are remunerated according to fees, paid by the gatekeepers, set by the [European Commission]. The independence and objectivity of the data experts is controlled by the [European Commission].

The data experts also have the right to examine compliance with the standards set in the data policies. For this, they have the right to examine the data handling of gatekeepers like auditors according to Art. […].

2. The role of independent Data Guides

Simonetta Vezzoso has already pointed out that trusted intermediaries "could provide fundamental support in managing end users' consents, according to their privacy and other preferences".[29] This could have the effect of countering "consent fatigue". Here, this proposal is spelt out in detail and made practical.

Each gatekeeper would be obliged to cooperate with at least three independent data experts. This could be combined with the audit obligation in Article 13 DMA. The experts act as *Data Guides* for consumers – similar to apps that already exist to assess how data-hungry other apps are. The Data Guides could come, for instance, from qualified entities in the sense of Art. 3 of the Directive 2009/22/EC of the European Parliament and the Council on injunctions for the protection of consumers' interests, i.e. consumer organisations or other NGOs. They would be remunerated for their work by fees from the gatekeepers. The details of remuneration and the exact requirements for acting as a Data Guide in this sense could be set out by the Commission. Their investigations need to be conducted independently, in a neutral and objective manner, and with the necessary expertise. The Commission would be in a position to check this or give some confidence to qualified entities or the choice of consumers in this regard. Obviously, it is of utmost importance that the Data Guides are not influenced by the gatekeepers.

Apart from assessing ex ante the data policies these organisations would also have the right to monitor compliance with the standards ex post. The Data Guides would need access to the data handling to monitor and could have certain

[29] Simonetta Vezzoso, The Dawn of Pro-Competition Data Regulation for Gatekeepers in the EU, 25.1.2021, p. 14.

rights in that regard – just as stipulated in the auditing processes of DMA and DSA.

Apart from the close parallel to auditing in the DMA and DSA, the idea to involve Data Guides also corresponds to some of the ideas in the Data Governance Act as proposed by the European Commission.[30] In that proposal, data sharing is made dependent upon intermediaries that take a clearing position.

3. The rationale of this proposal

The core idea behind this proposal is that users keep their authority to decide: They are the ones choosing the standard of data protection they wish to have. Yet, their decision is no longer an uninformed "click" on an annoying button that pops up, and it is not the pure click to accept all terms and conditions for lack of alternative. Their apathy to read data policies and their difficulties to understand the different choices would be overcome with this proposal. Users would be guided by experts they trust and would be required to take several big decisions without having to understand the details: What level of privacy do I want? Who are the organisations I trust? Would I accept to have a less convenient product for a higher standard of privacy? Do I wish to further competition of other businesses?

Data policies and the issues involved are so complex and so important that informed decisions are necessary. Since such informed decisions cannot be expected from the average, rational, time-sensitive user, some help is needed – and this help could be provided for by independent, trustworthy organisations. The Data Guides reduce the complexity of legal documents and the costs of reading. The European Data Protection Supervisor had requested a "user-friendly solution (of easy and prompt accessibility)" for consent management.[31] This is such a solution. It comes close to realise the four objectives of Art. 5(a) set out above.

The concept is inspired by the idea to use rating, branding or labelling in consumer contracts.[32] Ratings to inform customers are a standard feature in the modern consumer world, be it for food or for financial products. It solves the problem

[30] Cf. Article 9 of the draft Data Governance Act, Proposal for a Regulation of the European parliament and Council on European data governance, 25.11.2020, COM(2020) 767 final.
[31] European Data Protection Supervisor, Opinion 2/2021 on the Proposal for a Digital Markets Act, 10.2.2021, at para 25.
[32] Cf. Omri Ben-Shahar, They Myth of Opportunity to Read in Contract Law, European Review of Contract Law 2009, 1; Stefano Pellegrino, Branding Pro-Consumer Contracts: Developing a New Consumer Protection Technique in Light of the CESL Proposal, EuCML 2015, 3; Russell Korobkin, Bounded Rationality, Form Contracts, and Unconscionability, 70 University of Chicago Law Review 1203 (2003).

of information overload without resorting to massive state involvement, prohibitions or laisser-faire. To use the illustration by *Stefano Pellegrino* for the project to brand consumer contracts:

> "(…) almost no one who is purchasing eggs has the time or the ability to check how hens were treated during the production of their eggs. But the use of a simple stamp, "cage free", allows consumers to take even such a factor as animal rights into account while making their purchase choice. At the end of the day, such a factor may matter so much that many consumers are willing to pay a considerably higher price in order to protect hens' health. The key to such a success is to make a complex factor, such as "hens' health" or "consumers' legal protection", easily and instantly weighable by the consumer."[33]

The proposal has the advantage that the European Commission does not need to decide exactly upon the criteria that are of importance for consumers when making their choice. Instead, this is left to the market and the competition of Data Guides. It is their creativity how to serve the consumer interest, and it is the consumer who needs to understand once what is at stake to make up her mind whom to go with. For instance, the criterion of sharing data with other business users for competitive reasons could be an element that is part of that ranking, and users could decide how important they find it to let small retailers have a chunk of the data pie.

From an enforcement perspective, it seems reasonable to rely on third parties. Experiences in other areas show that private organisations may be very helpful in solving complexity and compliance problems that the state regime cannot solve alone, e.g. in unfair commercial practices law. The enforcement burden for the European Commission would be eased. An element of private enforcement enters the DMA world (which is most welcome).[34] The difficult decision what constitutes choice and consent does not need to be solved within compliance proceedings of the gatekeeper versus the European Commission but is solved by the decision of users based on the ratings of trusted agencies.

[33] Stefano Pellegrino, Branding Pro-Consumer Contracts: Developing a New Consumer Protection Technique in Light of the CESL Proposal, EuCML 2015, 3 (5).

[34] Cf. Giorgio Monti, The Digital Markets Act – Institutional Design and Suggestions for Improvement, TILEC Discussion Paper 2021-004, 2021, p. 11; Rupprecht Podszun/Philipp Bongartz/Sarah Langenstein, Proposals on how to improve the Digital Markets Act, Policy paper for IMCO, 2021, p. 9.

IV. Other policy options

There are other policy options to address some of the shortcomings of the provision in Art. 5(a) DMA.

1. Making the rule more precise

The rule could entail further obligations that make it more precise.[35]

In particular, Art. 5(a) could contain standards for the presentation of the options to users. For this, the law could prescribe more detailed information duties with specific substantial information or warnings that need to be given.

The rule could also contain a prohibition to work with "dark patterns" or to nudge users into a certain acceptance schemes. For instance, it could be forbidden to use default solutions that are particularly data-intense or to present the buttons for acceptance of data combinations in a more attractive way than the buttons for a less data-hungry alternative.

A possible wording could add the following sentences to the existing version:

Gatekeepers need to provide specific information about the kind of data collected, the sources of these data, the future use, the possibilities of concrete third parties to access these data, the duration of storage and the relevance of the data for the gatekeeper.

Users must have the choice between at least two different versions of the products or services of which one works on the basis of data minimisation. The version with limited use of data must not be less attractive or more costly than the other version but for the loss of functionalities that necessitate the data combination.

The presentation of the different options may not differ in format, colour, size or similar aspects. There must not be a default option unless the least data intense version is the default.

Gatekeepers must not influence the autonomous user decision through technical, psychological or other means.

[35] On the proposal by rapporteur *Andreas Schwab* see above. Cf. the proposal by the Irish Council for Civil Liberties, "Greater Protection in Article 5 (a) of the Commission's proposal for a Digital Markets Act", 25.1.2021, inserting "and, or, cross-using" after "combining" and introducing a requirement to present specific choice "in the case of each processing purpose" of the GDPR.

This approach has as an advantage that users may be in a better position to take an informed decision. The disadvantage is that the exact design still remains in the hands of the gatekeeper so that some seductive parameters can still be set. It will be hard to prescribe exactly what information and what presentation is needed. Users are confronted with an information overload that most of them will not be willing or able to read or handle.[36]

With this option, gatekeepers may inform their customers better, but they will still remain in an overwhelmingly strong position and will be the ones steering the information and decision-making process.

2. Requiring a confirmation by e-mail

Art. 5(a) could be combined with a confirmation solution which requires that users do not only click a button but give their consent via e-mail. Consent could thus be made dependent upon a higher standard of confirmation. The following sentence could be added to Art. 5(a):

Consent needs to be confirmed in writing by e-mail. Each change of the data policy requires renewed consent via e-mail. The e-mail that requests consent needs to contain clear information about the data policy.

This addition would give users more time to reflect. Requiring further steps may set a higher hurdle for consent. Also, users can better follow the data policy and can save information, potentially for litigation purposes. The constant change of policies without renewed information or consent would be broken.

Such a solution would require more traffic, however, it is more burdensome for users. It also does not stop users from consenting and leaves the information overload problem unsolved. In case users agree, gatekeepers may still build their advantage in data. They are the ones deciding about the level of information and about the process of consent. Still, requiring e-mail confirmation is a standard feature for Internet security and may be used to secure some higher level of commitment in consumer law.

[36] This has been well established, i.a. by Omri Ben-Shahar, The Myth of Opportunity to Read in Contract Law, 5 ERCL 2009, 1 (23f.); Oren Bar-Gill/Omri Ben-Shahar, Regulatory Techniques in Consumer Protection: A Critique of the Common European Sales Law, CMLRev 2013, 109.

3. Displaying the monetary value of consent

Gatekeepers may also be obliged to show the commercial value of the data they wish to collect and combine. This would give users a better understanding of the trade-off they are ready to accept. The wording could be as follows:

Before a user grants consent, the gatekeeper shall show the current monetary value of the user's consent. The methodology to calculate this value needs to be made transparent and needs to be plausible.

Such an amendment would make users aware that they are "paying" with their data, it would be the "pricing privacy" approach.[37] While personal data are protected from a rights perspective, they are used by gatekeepers for their commercial value. The monetary signpost solution would bridge this gap between personal rights and the exploitation of this right. Users have the chance to understand the business models of "free" platforms and would see their own data-related decisions with a new perspective. They could make up their minds whether the service they get is good value for their consent.

While this solution has a lot of appeal for supporters of market solutions, it comes with some strings attached. Firstly, it would require some plausible form of calculation of the value of data. It is unclear at present whether that will work. (Possibly, the fast-speed auctioning models in place for ads could serve as a blueprint for the quick calculation of the value of data and consent.)

Secondly, the value of consent to data combination will not represent the full value of user consideration since many platforms do not directly engage in selling data but in using data for advertisements,[38] future transactions etc. How to factor this in would be a point of major difficulty.

Thirdly, the monetary signpost may lead to the logical next step of giving users the opportunity to sell their data. This would, however, mean that personal information are traded to an even larger degree. Privacy could become a concept for those who can afford it.

---

[37] Gianclaudio Malgieri/Bart Custers, Pricing Privacy – The Right to Know the Value of Your Personal Data, Computer Law & Security Review, 2017, available at SSRN: https://ssrn.com/abstract=3047257; Nicola Jentzsch et al., Monetising privacy, Study for ENISA, 2012, available at https://www.enisa.europa.eu/publications/monetising-privacy; Victoria Fast/Daniel Schnurr, The Value of Personal Data: An Experimental Analysis of Data Types and Personal Antecedents, 2020, available at SSRN: https://ssrn.com/abstract=3611232 or http://dx.doi.org/10.2139/ssrn.3611232.

[38] Cf. the obligation in Article 24 of the Digital Services Act to disclose the parameters for personalised advertisements, see European Commission, 15.12.2020, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), COM(2020) 825 final.

4. Mandating data sharing with business users

Art. 5(a) could be amended in a way that obliges gatekeepers to share all data they receive from users with their business users (mandated data sharing).[39] In the present draft, Art. 11(2) DMA goes into the direction of supporting business users in obtaining consent. The change would be to make data sharing mandatory for gatekeepers. This would require that gatekeepers automatically ask end users for their consent and to grant access to the data obtained. If users do not agree to have business users combine their data, the gatekeeper would not receive this permission either.

The choice put forward by the gatekeeper to the user must necessarily entail that the same rights conferred upon the gatekeeper are conferred upon business users [involved in the transaction or provision of the service]. Users may only agree to either grant the rights to all requesting parties (gatekeepers/business users) or to none.

If consent is granted the gatekeeper must make the data obtained instantly accessible to business users.

Such a rule would serve two very different purposes: On the one hand, the advantage of gatekeepers in competition with other companies would be reduced since business users gain the same data-related rights, too. The hindrance of competitors in aftermarkets would be limited. Competition may have a (little) chance.

On the other hand, users might think twice when confronted with a larger number of companies that request access to their data. This may raise data awareness and lead to less confirmations in total.

While the first argument caters to those who wish for more competition, the second one is a pro-privacy argument. If gatekeepers are successful in obtaining consent and a data sharing obligation is attached to this, this would mean that personal information are widespread via a platform. The conflict of competition law on the one hand and data minimisation on the other is obvious. The rule also limits choice of users since they cannot assign rights to one company only.

[39] Cf. Jan Krämer/Daniel Schnurr, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, 2021, p. 20 ff.

5. Prohibiting the combination of data

While the solutions presented so far worked on the premise that the collection and combination of data by gatekeepers still remains possible, one may also consider the option to prohibit the building up of super-profiles. Art. 5(a) would then read as follows:

Gatekeepers shall refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data.

This is a more radical solution. It would mean a major success for privacy. It would also limit the data accumulation of digital gatekeepers, thereby taming their power and keeping a level playing field for third parties.

Yet, it would strip users of their right to consent and thereby limit their decision-making authority again. It comes at the cost of reduced potential for innovation – an argument that may be less important as seen above. One may keep in mind that there is a link to the designation of gatekeepers: The less gatekeepers there are, the higher the standards should be. For the GAFA companies one may have tougher rules than for 10-20 other gatekeeper companies.

V. Conclusion

The Digital Markets Act is meant to be the answer to the data economy power and unfairness problems. The power of gatekeepers has a lot to do with their command over personal data of users. The unfairness is founded in the asymmetry of digital gatekeepers vis-à-vis consumers and business users. If the DMA shall have an impact it must be tough on data accumulation.

Radical solutions have not been in the spotlight:[40]

- Gatekeepers could be prohibited to collect personal data other than those technically necessary to perform services.
- Gatekeepers could be structurally separated, either vertically or horizontally, thereby splitting datasets.
- Gatekeepers could be forced to have Chinese Walls within the corporation with a strict internal separation of commercial branches and accordingly data.

[40] For some of these remedies see Jan Krämer/Daniel Schnurr, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, 2021, p. 12 ff.

- The time consumers spend in one digital ecosystem could be limited so they do not leave their data marks for too long, or the retention period of data in companies could be limited.
- The number of users served as customers by one core platform service could be limited.

It seems that despite the rather harsh rhetoric against the GAFAs such solutions are not on the political agenda at present. Other, more technical solutions (e.g. processing data in decentralised channels) have not yet found significant support. It may be an option to test such "privacy enhancing technologies" in "privacy sandboxes".[41]

If more radical solutions are not feasible, the DMA should at least provide a more practical solution than it does at present. The current version of Art. 5(a) as a key provision of the DMA is not far-reaching enough. It runs the risk of achieving very little in practice for privacy and for competition.

The rating and monitoring of data policies by independent experts, the Data Guides, is a solution that would bring about a change in data combination. It would keep the idea of user autonomy alive but make users much better equipped to exercise their rights. Users would profit from the reduced complexity of data policies and terms & conditions. Private enforcement would be strengthened, the monitoring of data handling would be enhanced. The asymmetry in the relationship of digital gatekeepers and consumers would be reduced.

[41] Cf. Jan Krämer/Daniel Schnurr, Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies, 2021, p. 19.