Interpreting the EU Digital Markets Act Consistently with the EU Charter's Rights to Privacy and Protection of Personal Data

Mikołaj Barczentewicz *

Abstract

Depending on implementation details, the EU Digital Markets Act (DMA) may have negative consequences regarding information privacy and security. The DMA's interoperability mandates are a chief example of this problem. Some of the DMA's provisions that pose risks to privacy and to the protection of personal data are accompanied either by no explicit safeguards or by insufficient safeguards. The question is then: how to interpret the DMA consistently with Articles 7-8 of the EU Charter of Fundamental Rights which ground the rights to privacy and the protection of personal data? Using the example of the prohibition on restricting users from switching and subscribing to third-party software and services (Article 6(6) DMA), I show that Charter-compatible interpretation of the DMA may depart from the intentions of the DMA's drafters and even be perceived by some as significantly limiting the effectiveness of the DMA's primary tools. However, given that—unlike the GDPR—the Charter takes precedence over a mere regulation like the DMA, such policy objections may have limited legal import. Thus, the true legal norms (legal content) of the DMA may be different than what a superficial reading of the text could suggest or, indeed, what the drafters hoped to achieve.

1. Introduction[1]

Depending on implementation details, the EU Digital Markets Act (DMA) may have negative consequences regarding information privacy and security. The DMA's interoperability mandates are a chief example of this problem. Even advocates of this legally enforced interoperability recognize the increased privacy and security risks

* Associate Professor, University of Surrey.

[1] This paper builds on my: 'Privacy and Security Implications of Regulation of Digital Services in the EU and in the US' [2022] Stanford Law School, TTLF Working Papers No. 84; 'Minimizing Privacy Risks in Regulating Digital Platforms: Interoperability in the EU DMA', CPI Antitrust Chronicle, July 2022; 'How the New Interoperability Mandate Could Violate the EU Charter' (Lawfare, 6 July 2023)<https://www.lawfaremedia.org/article/how-the-new-interoperability-Mandate-could-violate-the-eu-charter>.

that it entails.[2] These concerns have been underscored by both the Organization for Economic Cooperation and Development and scholarly commentators.[3]

Some of the DMA's provisions that pose risks to privacy and to the protection of personal data are accompanied either by no explicit safeguards or by insufficient safeguards. The question is then: how to interpret the DMA consistently with Articles 7 and 8 of the EU Charter of Fundamental Rights, which ground the rights to privacy and the protection of personal data? Using the example of the prohibition on restricting users from switching and subscribing to third-party software and services (Article 6(6) DMA), I show that Charter-compatible interpretation of the DMA may depart from the intentions of the DMA's drafters and even be perceived by some as significantly limiting the effectiveness of the DMA's primary tools. However, given that—unlike the GDPR—the Charter takes precedence over a mere regulation like the DMA, such policy objections may have limited legal import. Thus, the true legal norms (legal content) of the DMA may be different than what a superficial reading of the text could suggest or, indeed, what the drafters hoped to achieve.

This article discusses in more detail only the DMA's prohibition on gatekeepers restricting users from switching and subscribing to third-party software and services (Article 6(6) DMA). In a previous publication, I similarly analysed the DMA's obligation 'on interoperability of number-independent interpersonal communications services' (Art 7 DMA).[4]

The question of Charter-compatible interpretation of the DMA is not the only way the correct legal interpretation of the DMA is likely to be heavily affected by the EU primary law (treaty-level legal norms). As I noted elsewhere, another prominent example is in the DMA's rules meant to ensure its harmonising effect.[5] Others have

---

[2] See eg Cory Doctorow and Benedict Cyphers, 'Privacy Without Monopoly: Data Protection and Interoperability' (*Electronic Frontier Foundation*, 12 February 2021) <https://www.eff.org/wp/interoperability-and-privacy>.

[3] OECD, 'Mapping Data Portability Initiatives, Opportunities and Challenges' (OECD Digital Economy Papers, No 321, 2021) <https://one.oecd.org/document/DSTI/CDEP/DGP(2021)1/FINAL/en/pdf>; Peter Swire, 'The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations' (2022) 6 Geo. L. Tech. Rev. 57.

[4] Mikołaj Barczentewicz, 'How the New Interoperability Mandate Could Violate the EU Charter' (Lawfare, 6 July 2023) <https://www.lawfaremedia.org/article/how-the-new-interoperability-mandate-could-violate-the-eu-charter>.

[5] Mikołaj Barczentewicz, 'German Big Tech Actions Undermine the DMA' (ICLE Issue Brief 2023-06-22, June 2023) <https://laweconcenter.org/resources/german-big-tech-actions-undermine-the-dma/>.

persuasively argued that an interpretation of the DMA, which does not guarantee its effectiveness as a harmonization measure, would threaten the law's validity under Article 114 of the Treaty on the Functioning of the European Union (TFEU).[6]

2. Importance of the Charter Rights to Privacy and Protection of Personal Data in Interpreting Secondary EU Law

The Charter protects both the right to respect for private and family life (Article 7) and the right to the protection of personal data (Article 8). As commentators have noted, the CJEU seems to have adopted an implicit hierarchy of rights and objectives of general interest, and the rights protected by Articles 7 and 8 are arguably very high in that hierarchy.[7]

In accordance with Article 52(1) of the Charter:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

As AG Kokott writing extra-judicially (with Christoph Sobotta) stressed, the fundamental character of the rights protected by the Charter is such that 'secondary law, such as regulations, directives or decisions are to be annulled if they are incompatible with fundamental rights.'[8] However, if it is possible to interpret a provision of secondary EU law consistently with the Charter, then 'preference must be given to that interpretation which ensures that the provision retains its effectiveness and which does not detract from its validity.'[9]

---

[6] Alfonso Lamadrid de Pablo and Nieves Bayón Fernández, 'Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and How to Fix It' (2021) 12 Journal of European Competition Law & Practice 576. See also Jasper van den Boom, 'What Does the Digital Markets Act Harmonize?–Exploring Interactions between the DMA and National Competition Laws' (2023) 19 European Competition Journal 57.

[7] Sybe De Vries, 'The EU Single Market as "Normative Corridor" for the Protection of Fundamental Rights: The Example of Data Protection' in Sybe De Vries, Ulf Bernitz and Stephen Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing, Oxford: Hart Publishing* (Hart Publishing 2015) 244–45.

[8] Kokott Juliane and Christoph Sobotta, 'The Charter of Fundamental Rights of the European Union after Lisbon' (EUI Working Paper AEL 2010) 6.

[9] ibid 7.

In one of the early cases following the Charter gaining binding legal force, the CJEU decided that a provision of a regulation was invalid due to incompatibility with Article 7, 8, and 52(1) of the Charter.[10] In *Volker and Schecke*, the Court invalidated a provision of Regulation No 1290/2005 on the financing of the common agricultural policy, which required indiscriminate publication of personal data of beneficiaries of EU funds.[11]

Perhaps the best-known conflict between Articles 7 and 8 of the Charter and secondary EU law was the subject of the Court's judgment in *Digital Rights Ireland*.[12] In that decision, the CJEU held that a whole directive, the Data Retention Directive, was invalid due to its incompatibility with Articles 7, 8, and 52(1) of the Charter.[13]

Soon after *Digital Rights Ireland*, the Court applied Articles 7 and 8 of the Charter in a more 'horizontal' context in *Google Spain*.[14] *Google Spain* is potentially relevant here for at least three reasons. First, this case 'shows that also outside the field of security and within the context of the internal market, the Court gives considerable weight to privacy and data protection.'[15] Second, the Court made it clear that Articles 7 and 8 may affect the interpretation of duties that secondary EU law may impose on some persons in favour of other persons. Third, according to the CJEU at least some specific rights stemming from Articles 7 and 8 override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[16]

An important question about Articles 7 and 8 in the present context is to what extent restrictions of *security*-protecting measures constitute restrictions of the rights grounded in those articles. Security is not identical with privacy or with the protection of personal data. In fact, some efforts to improve user security could restrict the users'

---

[10] Joined Cases C–92 and 93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662 (Volker and Schecke). See also De Vries (n 6) 244–245.
[11] *Volker and Schecke* (n 9).
[12] Joined Cases C-293 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communication et al and Kärtner Landesregierung et al* [2014] ECLI:EU:C:2014:238 (Digital Rights Ireland).
[13] ibid; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).
[14] *Digital Rights Ireland* (n 11).
[15] De Vries (n 6) 246.
[16] *Digital Rights Ireland* (n 11).

rights to privacy and to the protection of personal data (eg by processing personal data to a disproportionate degree). This is why, for example, as the European Data Protection Supervisor (EDPS) noted in his opinion on planned amendments to EU cybersecurity rules, if identification of risks to user security requires additional processing of user data (IP addresses or device identifiers), this must be done in accordance with privacy and personal data protection principles like data minimization.[17] However, as the EDPS also noted, 'security is essential for compliance with EU data protection law,' which is recognized by the GDPR itself (security is one of the chief principles of personal data processing in Article 5 GDPR). The issue is, then, not whether information security, in general, is an Article 7 or 8 concern. Instead, the issue is whether the security-protecting measures that could be restricted due to the DMA are the kind of security measures that ensure privacy and the protection of personal data.

3. Interoperability and Risks to Privacy and Protection of Personal Data

For brevity, I focus here on one regulatory solution adopted by the DMA: interoperability mandates. At the most basic level, in the context of digital services, interoperability refers to the capacity to exchange information between computer systems. Email is an example of an interoperable standard that most of us use today. It is telling, however, that supporters of interoperability mandates point to services like email as their model examples. Email (more precisely, the SMTP protocol) originally was designed in a notoriously insecure way.[18] It is a perfect illustration of the opposite of privacy-by-design.[19] As originally conceived, email offered roughly the same levels of privacy and security as a postcard message sent without an envelope that passes through many hands before reaching the addressee. Even today, email continues to be a source of security concerns due to its prioritization of interoperability.[20]

Using currently available technology to provide alternative interfaces or moderation services for social-media platforms, third-party developers would have to be able to

---

[17] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (11 March 2021) <https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf>.
[18] See eg Zakir Durumeric and others, 'Neither Snow nor Rain nor MITM... an Empirical Analysis of Email Delivery Security', *Proceedings of the 2015 Internet Measurement Conference* (2015).
[19] See Article 25 of the Regulation (EU) 2016/679 (General Data Protection Regulation).
[20] See eg Sydney Li, 'A Technical Deep Dive into STARTTLS Everywhere' (*Electronic Frontier Foundation*, 25 June 2018) <https://www.eff.org/deeplinks/2018/06/technical-deep-dive-starttls-everywhere>.

access much of the platform content potentially available to a user. This would include not just content produced by users who explicitly agree to share their data with third parties, but also content — eg posts, comments, likes — created by others who may have strong objections to such sharing. It does not require much imagination to see how, without adequate safeguards, mandating this kind of information exchange would inevitably result in something akin to the 2018 Cambridge Analytica data scandal.[21]

Imposing a legal duty on digital service providers to make their core services interoperable with any third party creates, as noted by Cory Doctorow and Benedict Cyphers, at least three categories of risks:
1. Data sharing and mining via new APIs;
2. New opportunities for phishing and sock puppetry in a federated ecosystem; and
3. More friction for platforms trying to maintain a secure system.[22]

Friction in ensuring security

Bearing in mind Doctorow & Cyphers' last point, a crude interoperability mandate could make it much more difficult for service providers to keep up with the fast-evolving threat landscape. For example, it may seem a good idea to require service providers to submit all changes to their interoperability standards (interfaces) for external review, possibly by a public authority. This could potentially help to ensure that service providers do not 'break' interoperability or discriminate against some third-party services that would want to benefit from it. However, imposing such a requirement would introduce delay in responding to new threats, potentially putting user data at risk. When it can take just seconds to exfiltrate millions of user profiles, delaying security patches by weeks or even days through regulation is unacceptable.

'Phishing and sock puppetry'

True interoperability of digital services would mean a two-way exchange of information. For online platforms like social networks, this would mean that, eg a Facebook user could interact with users of other interoperable platforms as if they were also Facebook users (exchange direct messages, see their posts, add comments

[21] On the Cambridge Analytica scandal, see eg U.K. Information Commissioner, 'Investigation into Data Analytics for Political Purposes' <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/>.
[22] Doctorow and Cyphers (n 2).

and so on). Doctorow & Cyphers recognized that this would mean that any identity controls (eg Facebook's requirement to use real names) could easily be undermined if criminals or state actors run or control their own interoperable platforms. Those in control of such a platform could appear to users of other platforms as their friends in an attempt to hack them (eg phishing through direct messages). Such deception already happens on major online platforms, but those platforms are legally free to adopt measures to counteract it. A broad interoperability mandate would disallow service providers from vetting other providers and from imposing their own identity requirements (eg requiring the use of real names).

Those risks are well-illustrated by how often users are victimized through one of the most widely used interoperable protocols: telephony and, in particular, telephone numbers.[23] Due to design choices in the interoperability of telephony systems, which entirely side-lined security concerns, it is often trivial for any malicious actor to 'spoof' the number that appears in a call recipient's 'caller ID' feature. They may thus appear to a victim as if they are calling from, eg the victim's bank. Having created an insecure-by-design system that facilitated widespread consumer harm, regulators are slowly and, to date, ineffectively playing catch-up.[24]

General data-sharing risks

Effective interoperability requires sharing of sensitive data among different service providers through new two-way real-time interfaces ('APIs'). Doctorow & Cyphers put forth a plan endorsing broad interoperability mandates,[25] but admirably, they acknowledge the important security and privacy trade-offs such a mandate would impose. Promoters of the bills analysed herein frequently do not account for such costs. It is, therefore, worth analysing these harms from the perspective of proponents of interoperability mandates. Doctorow & Cyphers are open about the scale of the risk: '[w]ithout new legal safeguards to protect the privacy of user data, this kind of interoperable ecosystem could make Cambridge Analytica-style attacks more common.'[26]

---

[23] See eg Jovi Umawing, *More than a Quarter of Americans Fell for Robocall Scam Calls on Past Year*, MALWAREBYTES (1 Jun. 2022) https://blog.malwarebytes.com/reports/2022/06/more-than-a-quarter-of-americans-fell-for-robocall-scam-calls-in-past-year.
[24] ibid.
[25] Doctorow and Cyphers (n 2).
[26] ibid 28.

The Cambridge Analytica incident illustrates the risks well. The personal data that Cambridge Analytica ultimately used was collected through a Facebook app created by an academic researcher.[27] The app was used by 270,000 people, who expressly granted permission for the app to access their account information, including information about their Facebook contacts. This is how the app's author collected data on more than 50 million Facebook users.

A potential future Cambridge Analytica could benefit from a poorly drafted interoperability mandate. Today, Facebook can and does stop third-party developers who try to exfiltrate data from the platform in violation of the company's terms. Some even believe that Facebook does so too vigorously.[28] But under an interoperability mandate, Facebook may be prevented from vetting and denying access to third parties if a user clicks 'yes' in a consent popup. And users may habitually click 'yes' in consent popups, irrespective of any 'dark patterns' that would nudge them to authorize the desired action ('popup fatigue').[29] This is understandable: users may simply want to access the desired functionality (eg to play a game) and may not be willing to invest sufficient time and effort to parse the consequences of what, exactly, they are authorizing.
Thus, one risk is that users will authorize interoperability to an extent that may later surprise them, even if the third-party service providers provide all necessary information in an accessible and intelligible form. It may just be that users will only start caring about the consequences of their choices once they materialize, not before they make a choice.

It is, however, unrealistic to expect all third-party service providers to obey the rules, including rules stipulating that one should act in accordance with unstated user expectations. Some third-party providers may act in good faith when they push the boundaries of what is permitted due to the (potentially erroneous) belief that users are better served in some particular way. But some will intentionally engage in illegal — even criminal — activity.[30] Such actors may come from foreign jurisdictions

---

[27] See also Kurt Wagner, 'Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users' (*Vox*, 17 May 2018) <https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data>.
[28] Mitch Stolz and Andrew Crocker, 'Once Again, Facebook Is Using Privacy As A Sword To Kill Independent Innovation' (*Electronic Frontier Foundation*, 20 November 2020) <https://www.eff.org/deeplinks/2020/11/once-again-facebook-using-privacy-sword-kill-independent-innovation>.
[29] See eg Cristian Bravo-Lillo and others, 'Harder to Ignore? Revisiting {Pop-Up} Fatigue and Approaches to Prevent It', *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (2014).
[30] As the Organisation for Economic Co-operation and Development (OECD) noted: 'Even where

(outside of the EU and the United States), which could render ex-post enforcement of legal rules against them particularly difficult.

4. Mandated Interoperability in the DMA: How to Interpret the Safeguards?

The original DMA proposal included several interoperability and data-portability obligations regarding the designated 'core platform services' of 'gatekeepers' — ie, the largest online platforms. Those provisions were changed considerably during the legislative process. The final DMA text contains, among other provisions:

1) a prohibition on restricting users — 'technically or otherwise' — from switching among and subscribing to software and services 'accessed using the core platform services of the gatekeeper' (Art 6(6));
2) an obligation for gatekeepers to allow interoperability with their operating system or virtual assistant (Art 6(7)); and
3) an obligation 'on interoperability of number-independent interpersonal communications services' (Art 7).

To varying degrees, these provisions attempt to safeguard privacy and security interests, but if read literally and in isolation from the broader legal context, the first two do so in a clearly inadequate way, and the third is at risk of being unduly watered down. In this article, I analyse only the first of the three — the mandate pertaining to switching and subscribing to third party-services (Article 6(6)).

First, the Article 6(6) prohibition on restricting users from using third-party software or services 'accessed using the core platform services of the gatekeeper' notably applies to web services (web content) that a user can access through the gatekeeper's web browser (eg, Safari for iOS).[31] Given that web content is typically not installed in the operating system, but used through a browser (ie, likely 'accessed using a core platform service of the gatekeeper'), earlier 'side-loading' provisions (Article 6(4), which is discussed further below) would not apply here.

---

individuals and organisations agree on and consent to specific terms for data sharing and data re-use, including the purposes for which the data should be re-used, there remains a significant level of risk that a third party may intentionally or unintentionally use the data differently.' *Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use Across Societies*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2019), chapter 4, Risks and challenges of data access and sharing.' https:/www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.

[31] Web browsers are defined as core platform services in Art 2(2) DMA.

Article 6(6) itself does not include any privacy or security safeguards. The corresponding recitals (53-54) clarify only that:

> The mere offering of a given product or service to consumers, including by means of pre-installation, as well as the improvement of the offering to end users, such as price reductions or increased quality, should not be construed as constituting a prohibited barrier to switching.

However, what may be required to protect user privacy and security is not merely 'increasing the quality' of a gatekeeper service (eg a web browser), but organising this service in such a way as to make it more difficult for users to access unsafe third-party services (eg websites), which is more likely to be 'construed as constituting a prohibited barrier to switching.'

This leads to what looks like a significant oversight: the gatekeepers appear to be almost completely disabled from protecting their users when they use the Internet through web browsers, one of the most significant channels of privacy and security risks. The U.S. Federal Bureau of Investigation ('FBI') has identified 'phishing' as one of the three top cybercrime types based on the number of victim complaints.[32] A successful phishing attack normally involves a user accessing a website that is impersonating a service the user trusts (eg an e-mail account or corporate login). Browser developers can prevent some such attacks, eg by keeping 'block lists' of websites known to be malicious and warning about, or even preventing, access to such sites. An exceptionless prohibition on platforms restricting their users from accessing third-party services, however, would also prohibit this vital cybersecurity practice.

Compare that approach with Art 6(4), applicable in cases of installed third-party software, which allows the gatekeepers to take:

> measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, provided that such measures go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.

---

[32] Federal Bureau of Investigation, *Internet Crime (IC3) Report 2020* (2020) < https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf >.

The gatekeepers can also apply:

> measures and settings other than default settings, enabling end users to effectively protect security in relation to third party software applications or software application stores, provided that such measures and settings go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.

None of those safeguards, insufficient as they are on a literal reading (see the discussion below of Art 6(7)) are present in Art 6(6). Worse still is that the anti-circumvention rule in Art 13(6) applies here, prohibiting gatekeepers from offering 'choices to the end-user in a non-neutral manner.' That is precisely what a web-browser developer does when warning users of security risks or when blocking access to websites known to be malicious — eg to protect users from phishing attacks.

This concern is not addressed by the general provision in Art 8(1) requiring the gatekeepers to ensure 'that the implementation' of the measures under the DMA complies with the GDPR, as well as 'legislation on cyber security, consumer protection, product safety' (see also Section IV.B for more detailed discussion). The first concern is that this would not allow the gatekeepers to offer a *higher* standard of user protection than that required by the arguably weak or overly vague existing legislation. Also, if the DMA's rules (including future delegated legislation) could be viewed as more specific — in the sense of constituting *lex specialis* — than EU rules on privacy and security, establishing a coherent legal interpretation that would allow gatekeepers to protect their users would likely be unnecessarily difficult.[33]

Potential incompatibility with the Charter

In this section, I consider an interpretation of Article 6(6) DMA that would likely lead to incompatibility with the Charter. An alternative interpretation meant to ensure consistency with the Charter is suggested in the next section.

---

[33] See Damien Geradin, Konstantina Bania and Theano Karanikioti, 'The Interplay between the Digital Markets Act and the General Data Protection Regulation' (2022). <https://ssrn.com/abstract=4203907> (arguing that some DMA provisions may be lex specialis, though it is unclear which); 'Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences' (Centre for Information Policy Leadership 2023). <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_asis_may2023.pdf> (arguing that the DMA is not lex specialis to the GDPR).

On the interpretation presented above, Article 6(6) (together with Article 13(6)) DMA would prevent, for example, some popular web browser providers from implementing technical measures restricting user access to unsafe websites (eg known to be used for phishing campaigns). In other words, this provision may amount to a legal obligation imposed on service providers to *degrade* the level of privacy and personal data security protections they offer—in comparison with the current level of protection or in comparison with a potential level of protection that could otherwise be developed in the future. Unlike in the case of other provisions discussed here, this rule contains no exceptions that would allow for a proportionate response considering the privacy and data protection interests affected.

Article 8(1) – compliance with GDPR and other legislation

The general reference to compliance with the GDPR in Article 8(1) DMA does not address the issue with respect to many core platform services which do not involve the processing of personal data. The web browsers from my example normally run as software installed on a user's computer. Accessing third-party websites through a web browser does not necessarily involve the processing of any user's personal data *by the web browser's developer*. It may very well be, then, that the gatekeeper does not have any GDPR-provided obligations that could somehow act as exceptions to the Article 6(6) duty.

Aside from the GDPR, Article 8(1) DMA refers also to 'legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements.' This provision raises two main issues. Firstly, it is vague and unspecific, which may be a problem under the Charter's requirement that measures restricting rights must have clear and precise rules about their scope.[34]
Secondly, it is doubtful that—at least for many risks introduced by the DMA—there exists any other legislation that could sufficiently address those risks. Notably, no examples of 'legislation on cyber security, consumer protection, product safety' are given in the main text or in the corresponding Recital 65. As to whether sufficient safeguards are likely to come from such other legislation, it's worth looking at the European Commission's conclusions from the Impact Assessment to the 2022 proposal of the Cyber Resilience Act:

[34] *Digital Rights Ireland* (n 11) [54].

> Currently there are no specific cybersecurity requirements comprehensively and systematically applicable to all products with digital elements, hardware or software, accessing the internal market. Cybersecurity of software (embedded in hardware and upload-able or of generic use, i.e. standalone) in particular, of key importance for cybersecurity policies, is the least regulated even at the level of sector- or product-specific legislation with limited scope.[35]

And even when some other piece of legislation—like the GDPR—could be said to provide a relevant general duty to protect user privacy and security, a question could arise whether DMA provisions like Article 6(6) constitute *leges speciales*, thus taking interpretative precedence over arguably more general rules from other legislation.[36]

Proportionality analysis under Article 52(1) of the Charter

Assuming then that Article 6(6) may, in some circumstances, amount to a legal obligation to degrade the level of privacy and personal data protections provided to a user, it arguably constitutes a clear example of a restriction of rights protected by Articles 7 and 8 of the Charter. This calls for an analysis of the proportionality of that restriction under Article 52(1) of the Charter.

First, we must consider whether the measure pursues an 'objective of general interest recognised by the Union or the need to protect the rights and freedoms of others.' The stated objective of Article 6(6) is to ensure that 'gatekeepers should not restrict or prevent the free choice of end users' (Recital 65).[37]

---

[35] European Commission, 'Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020' (15 September 2022) SWD(2022) 282 final < https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment >. See also 'Study on the need of Cybersecurity requirements for ICT products' (15 December 2021) < https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products > 11-12.

[36] See n 33 above.

[37] Whereas, on the most general level (Article 1(1) DMA):

> The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users.

Accepting that this is an objective of the right kind, the question is then whether the measure is suitable for the attainment of the objective. Here too, we can accept—at least for the sake of argument—that the measure can contribute to the objective.

The next step is to ask whether the measure is strictly necessary—or in other words, whether it is the least restrictive measure capable to achieve the objective. It is hard to see how Article 6(6), interpreted as mandating the degradation of privacy and personal data protections without adequate (or likely any) safeguards, can satisfy the test of strict necessity. Notably, Article 6(6) does not contain even those safeguards that are included in other provisions of the same Article 6 (eg Article 6(4)). At the very least, such minimum safeguards could have been included without jeopardising the objective pursued.

Moreover, even if Article 8(1) could help to ground some exceptions in favour of privacy and security, at least in some situations (eg where the GDPR applies), it is doubtful that Articles 6(6) and 8(1) together provide 'clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.'[38] The DMA repeatedly invokes 'necessity and proportionality,' but such vague mantras are not a substitute for clear and precise rules.

Given that the measure fails the test of strict necessity, it is not necessary to consider proportionality *stricto sensu*. However, it is worth noting that the objective of promoting the scope of 'free choice' available to users is very unlikely to be seen by the CJEU as overriding the rights to privacy and protection of personal data. Unlike in cases like *Scarlet Extended*, we are not dealing here with a case of balancing of fundamental rights like the right to (intellectual) property and the right to privacy.[39] Arguably, all relevant fundamental rights count against such broad interpretations of the DMA (not only Articles 7-8, but also eg Article 16).

Aside from the question of balancing rights and interests, the importance of the measure for the objective pursued is rather dubious. The very nature of the measure is such that it *restricts the free choice* of consumers: for example, they would no longer be able to use the web browser they enjoy without giving up on some of its safeguarding features. The measure—like some other DMA provisions—seems to

[38] *Digital Rights Ireland* (n 11) [65].
[39] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI:EU:C:2011:771.

rely on an assumption that a choice to restrict one's other choices (eg to choose a browser that restricts access to dangerous websites) is somehow not valuable, ignoring that this is a fundamental tenet of data protection.

The risks discussed here will arise due to gatekeepers complying with obligations imposed on the DMA, without any (purportedly benefiting) user being able to express their will. At best, users will be able to take remedial action ex post (eg by configuring the service away from default settings). At worst, some risks will simply arise or be exacerbated irrespective of what a user may do (other than opting not to use gatekeeper service, which otherwise the user would have preferred to continue to use).

Interpretation consistent with the Charter

This section discusses how Article 6(6) DMA should be interpreted in the light of the Charter, and especially in the light of its Articles 7 and 8. Interestingly, neither the Charter's Article 7 nor 8 are invoked by the DMA. Instead, the DMA's Recital 109 refers to Articles 16 (freedom to conduct a business), 47 (right to an effective remedy and to a fair trial), and 50 (right not to be tried or punished twice in criminal proceedings for the same criminal offence) of the Charter. Of course, the fact that the DMA doesn't invoke Articles 7-8 of the Charter does not mean that those provisions are not applicable. However, this oversight strongly suggests that the drafters of the DMA did not fully appreciate the importance of Articles 7-8, as distinguished from secondary EU law like the GDPR. This by itself does not mean that the DMA cannot be read consistently with Articles 7-8, but it does at least raise a possibility that the DMA may contain provisions incompatible with Article 7-8 and thus invalid.

As suggested by the proportionality analysis from the previous section (Section IV.A), an exceptionless reading of Article 6(6) would arguably render it incompatible with Articles 7, 8, and 52(1) of the Charter. In other words, if this provision is to be saved from invalidity, it will require employing interpretative methods departing from the literal interpretation and possibly even contrary to the intentions of the DMA's proposers and drafters.

As the CJEU recently re-affirmed in *Ligue des droits humains*:

> … in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter Thus, if the wording of secondary EU legislation is open to more than

> one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law …[40]

How far can such an interpretation go? Although going against the clear literal meaning of a provision of secondary EU law (*contra legem*) may not be possible, *augmenting* the text with content not expressly included is certainly possible. In *Ligue des droits humains*, the Court interpreted Article 12 of the Passenger Name Records (PNR) Directive,[41] saving it from a general finding of invalidity even though, on its face, it contained a general and indiscriminate personal data retention provision for a period of five years, which was not justified by any sufficiently weighty objective of general interest.[42] To save Article 12, the Court found that it should be interpreted as being limited only to the kind of personal data in respect to which it would be justified under the Charter to retain it.[43]

Like the PNR Directive at issue in *Ligue des droits humains*,[44] the DMA states (in Recital 109) that it respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular Articles 16, 47 and 50 thereof. Accordingly, the interpretation and application of this Regulation should respect those rights and principles.
As discussed earlier, the lack of express mention of Articles 7 and 8 of the Charter is not a ground not to apply them—especially since the Charter provisions that are listed are preceded by 'in particular.'

I thus submit that to save Article 6(6) from invalidity, we can rely on the general objective of the DMA to respect the fundamental rights under the Charter and thus interpret Article 6(6) as not requiring gatekeepers to do *anything* that would amount to a restriction of a right to privacy or to the protection of personal data. In other words, my proposed solution is to ensure that Article 6(6) does not effectively restrict the rights in question *at all*.

---

[40] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* [2022] ECLI:EU:C:2022:491 (Ligue des droits humains) [86].
[41] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
[42] *Ligue des droits humains* (n 38) [248]-[262].
[43] ibid [262].
[44] *Ligue des droits humains* (n 38) [88]-[89].

Any intermediate interpretative solution, which would still allow a restriction of the rights in question, but to a smaller degree, faces a serious objection that such any such restriction would not be accompanied by 'clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.'[45] There is also an issue of legitimacy if a court were to try to engage in such more creative interpretation—it would arguably put itself in the role of the legislator.

In particular, an attempt to read into Article 6(6) some of the safeguards from other DMA provisions is unlikely to be sufficient to ensure consistency with the Charter. For example, interpreting Article 6(6) as permitting gatekeepers to adopt measures 'strictly necessary and proportionate' to protect user privacy and security would be inadequate. It would be inadequate because it is not a restriction of the rights of *the gatekeepers*, which is the most significant potential violation of the Charter here. Instead, the focus should be on the rights to privacy and the protection of the personal data of *the users*. A mere *permission* for gatekeepers to adopt some safeguards, if they wish to do so, is clearly not a proper measure to address the risk of infringement of the rights, a risk *created by the DMA*.

A better solution would be to interpret Article 6(6) as simply not applying to measures necessary to further privacy and protection of personal data. However, a reference to 'necessity' can itself be a source of inconsistency with the Charter because it turns safeguarding Charter rights into a limited *exception.* This solution may be justifiably seen as prioritizing DMA's goals (eg the DMA's controversial interpretation of what counts as promotion of user's 'free choice') over the rights protected by Articles 7 and 8 of the Charter—which would be hard to find support for in the case law of the CJEU.

Finally, Article 8(1) referring to gatekeepers' other legal obligations—eg under the GDPR—is also not a solution because at least some risks to privacy and personal data protection are outside of the scope of any other legal obligations that gatekeepers may have. In other words, the DMA creates risks for privacy and the protection of personal data that may not be addressed by any other EU legislation (like in my web browser example).

[45] *Digital Rights Ireland* (n 11) [65].

5. Conclusions

By and large, the DMA betrays a policy preference for privileging uncertain and speculative competition gains at the cost of introducing new and clear dangers to information privacy and security. This is clearly the case in Articles 5 and 6 of the DMA. Proponents of those or even stronger legislative interventions have demonstrated that they are much more concerned, for example, that privacy safeguards are 'not abused by Apple and Google to protect their respective app store monopoly in the guise of user security.'[46] Given the difficulties in ensuring effective enforcement of privacy protections, however (especially with respect to actors coming from outside of the EU, the United States, and other broadly privacy-respecting jurisdictions), the mentions of privacy and security in Articles 5 and 6 could amount to not much more than lip service.

Despite its *prima facie* significant flaws from the perspective of consistency with the EU Charter of Fundamental Rights, the DMA can be interpreted in a way that saves it from invalidation. This article proposed some ways to achieve that. It is reasonable to expect the European Commission to offer a systematic and detailed vision of concrete safeguards against the predictable and very significant privacy and security risks that the DMA could introduce if not interpreted carefully.

[46] Damien Geradin, 'Digital Markets Act (DMA): Where Is the Council Headed To?' (*The Platform Law Blog*, 18 October 2021) <https://theplatformlaw.blog/2021/10/18/digital-markets-act-dma-where-is-the-council-headed-to/>.