Max Planck Institute
for Innovation and Competition

Max Planck Institute for Innovation and Competition Research Paper No. 21-25

To Break Up or Regulate Big Tech?

Avenues to Constrain Private Power in the DSA/DMA Package

Heiko Richter, Marlene Straub, Erik Tuchtfeld
(*Editors*)

Max Planck Institute for Innovation and Competition Research Paper Series

Editors

Dr. Heiko Richter, LL.M. (Columbia), Dipl.-Kfm.
Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich

Marlene Straub, LL.M. (Edinburgh)
Student at the Oxford Internet Institute and Research Assistant at the Centre for Socio-Legal Studies, Oxford, and Editor at Verfassungsblog, Berlin

Erik Tuchtfeld
Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, and External Editor at Verfassungsblog, Berlin

Imprint

2021
Max Planck Institute for Innovation and Competition
Marstallplatz 1, 80539 Munich, Germany

ISBN 978-3-00-070284-6

Foreword

Together with Verfassungsblog, the Max Planck Institute for Innovation and Competition hosted an Online Symposium on the topic "To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package". These contributions are collected in this eBook. Originally, they were published successively on the Verfassungsblog between 30 August and 7 September 2021 at https://verfassungsblog.de/category/debates/power-dsa-dma/.

The key question is whether the Digital Services Act (DSA) and the Digital Markets Act (DMA) are suitable instruments to regulate private power in the digital arena. The concentration of private power in the digital realm is not tenable – on this there is transatlantic consensus. This consensus extends across domains of private power, ranging from power over markets and consumers' behaviour, power over private rule-making to power of and over opinion. But how to regulate such forms of power? And how to cope with the fact that Big Tech's all-encompassing influence questions even these basic definitions and concepts of power? There is no consensus on solutions, but clear trends towards regulatory intervention are visible.

In the US, the antitrust debate was long dormant, but has returned even stronger, led by academics who have been invited into the Biden administration. The suggestion to 'break up' Big Tech companies carries a different weight, if coming from within the US government. Moreover, the reform of Section 230 on limited liability and Good Samaritan protection has a global impact, potentially overshadowing any regulation outside the US.

The EU has already set a quasi-global standard when it comes to regulating power of and over data subjects, by putting the GDPR in place. In contrast, the European Commission's numerous investigations into anticompetitive conduct from Big Tech have been criticised for being relatively slow and ineffective. Besides, liabilities and right protection on the internet are still governed by rules, which have been conceptualized more than two decades ago. Against this backdrop, the Commission published two proposals in December 2020: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Foreseeably, they will be the landmark pieces of digital policy this legislature.

The DSA aims at protecting users' fundamental rights on intermediaries and platforms, while also making these 'safer'. But introducing greater responsibility and accountability among intermediaries might even entrench their power. This dilemma is particularly salient in the realm of content moderation: there is a genuine risk of reinforcing private actors' role as the governors of and power over speech online. One may legitimately argue for private companies moderating speech at different thresholds rather than referring to the human rights frameworks which bind governments. But if exceptionally powerful intermediaries determine what speech is acceptable at scale, does assigning them responsibility and accountability at the threat of liability invite censorship? Who decides what behaviour is responsible? Circularly, would such assignments

of responsibility and accountability invite dependence on private actors, while public institutions retreat from this space? Also beyond content moderation, similar debates on assigning intermediaries greater responsibility and accountability exist across the DSA's scope. For example, in amorphous due diligence obligations, in the notice and takedown regime, towards systemic risks and towards gaps in the proposal (e.g. an absence of provisions on behavioural targeting or the adtech industry). Each of these issues has the potential to strengthen private power, if not addressed with enough precision.

The DMA is intended to mitigate this concern – at least to some extent and with regards to market power. It aims to establish a level playing field among digital corporations, ensuring competitiveness, growth and fostering innovation, while targeting gatekeeper – meaning very big and powerful – platforms, in particular. This approach means a fundamental shift towards preventive regulation. It contains a bundle of prohibitions of practices (e.g. as self-preferencing, or combining personal data from their core platform services with data from other sources) and obligations (e.g. providing access, interoperability, transparency, and sharing of information and data). But does the DMA provide an effective toolbox, and is it ready to cope with the future realities of digital markets? And to what extent can it sustainably solve the problems of private power? The DMA may be regarded as too cautious, as it does not cover situations of relative power dependency, and it presumes a primacy of behavioral over structural remedies. Yet, the DMA would immensely increase the power of the European Commission as a regulatory authority, and its sole reliance on effective public enforcement presupposes a well-functioning public government apparatus. This inevitably leads to a fundamental question: Must the entrenchment of private power necessarily be accompanied by an empowerment of the state, or is the empowerment of other private actors a desired complement or even a better solution?

Evidently, there is a caveat to every statement made, and every statement invites more questions, but they all boil down to this: how does a regulatory choice affect an intermediary's power, and to what extent can the measures included in the DSA and DMA mitigate adverse effects? Any prudent regulatory solution must stand the test of time and consider the distribution of power long-term. It must prove resilient against the backdrop of constant technological progress and socio-economic developments. When tackling these issues, it is therefore essential to bridge disciplinary silos: data protection law, consumer protection law, copyright law, competition law and constitutional law each consider solutions to address private power. But more than ever before, the age of Big Tech has driven these disciplines to overlap and work with each other.

Accordingly, this eBook brings together several contributions from different perspectives, which also aim to extend the scientific discourse on the topic to a wider audience. We are sincerely grateful for the commitment of all authors and the good cooperation.

The Editors

Table of Contents

II. The Digital Markets Act (DMA)

III. Enforcement

Enforcement of the DSA and the DMA – What did we learn from the GDPR?

Suzanne Vergnolle

In trying to overcome the cross-border enforcement's pitfalls of the GDPR, the Commission's proposals for a Digital Services Act and Digital Markets Act are largely expanding the Commission's enforcement powers. Unfortunately, what is touted as a solution for cross-border enforcement issues, might lead to new difficulties and challenges due to the risks of the centralization of power with the Commission.

Remember May 2018, when our mailboxes were full of emails explaining how companies were, as they put it, "better protecting our privacy"? For privacy experts, it was a moment of achievement and excitement: the long-awaited General Data Protection Regulation[1] (GDPR), was *finally* entering into application. This regulation is often presented as a "success story"[2], or as a "model for policymakers"[3]. Unfortunately, the hopes surrounding its effectiveness have gradually allayed. Data protection experts are still desperately waiting to see tangible improvements for peoples' privacy.

Some[4] attribute this to failures from European governments, which are underfunding and understaffing their national data protection authorities (DPAs), while others[5] lament the impracticality of the GDPR's vague language. Most commentators, however, agree on one thing: the one-stop-shop[6] mechanism instituted by the GDPR is ineffective or, at least, broken. The past years have unveiled this mechanism as a slow and inefficient system, which even the European Commission recognized[7] in 2020. We should hope that the Commission is trying, in its most recent regulatory proposals, to avoid repeating the same mistakes.

At a first glance, it might seem so. Both the Digital Services Act[8] (DSA) and the Digital Markets Acts[9] (DMA) put forward new enforcement mechanisms avoiding bottleneck national investigations seen with the GDPR. In a nutshell, the DSA framework organizes the exemption from liability for providers of intermediary services (Article 1 § 1 DSA[10]), and the DMA provides harmonized rules "ensuring contestable and fair markets in the digital sector" (Article 1 DMA[11]).

Both proposals are essentials because they aim at fostering innovation, growth, and competitiveness notably by bridling concentration of private power. However, their success is contingent to a solid and effective enforcement. Otherwise, their principles and rules might remain a toothless tiger and face the same disillusion and criticisms[12] than the GDPR.

In trying to overcome the cross-border enforcement's pitfalls of the GDPR (Part I), the Commission's proposals are largely expanding the Commission's enforcement powers.

By doing so, the institution is fully applying the adage: "you are never as well served as when you serve yourself." Unfortunately, the solutions for cross-border enforcement put forward in both proposals (Part II) might lead to new difficulties and challenges, notably because of the risks of the centralization of power with the Commission.

I. Issues with cross-border enforcement in the GDPR

One reason explaining why the GDPR garnered such attention is the level of fines DPAs can impose on organizations. Article 83 sets forth fines of up to 10 or 20 million euros, and 2% or 4% of the entire global turnover of the preceding fiscal year, depending on the violation.

As of late August 2021, at least 760 fines have been imposed, corresponding to more than 1 billion euros[13]. However, they are unevenly spread out across the European Union. The Irish Data Protection Authority (DPC) has only issued a few fines (less than 10) since 2018[14]. This is concerning as most Big Tech companies have their main establishment in Ireland, making the DPC their lead authority. Per the one-stop-shop mechanism[15], a single lead supervisory authority located in the Member State in which an organization has its "main" establishment must coordinate cross-border complaints and investigations into that organization's compliance with the GDPR. Most of the high-profile cases include cross-border processing of personal data, triggering the application of the one-stop-shop. Currently, a backlog of at least 28 cases[16] against Big Tech firms is under investigation by the Irish DPC. Only two have led to a decision and a fine, increasing the frustration from other DPAs[17] and widespread criticism from NGOs[18] to Members of the European Parliament[19].

A case against WhatsApp illustrates well the difficulties of GDPR's enforcement. When Facebook purchased WhatsApp in 2014, it assured[20] nothing would change for its user's privacy. However, in 2016, WhatsApp announced[21] modifications to its privacy policy, organizing a data sharing with Facebook. The change drew widespread regulatory scrutiny across Europe and some national authorities adopted a decision[22] before the entering into force of the GDPR. Since then, the Irish DPC has been the lead authority investigating the company's compliance with the regulation. In December 2020, the DPC sought feedback from other DPAs on its draft decision but was unable to find a consensus with the other authorities.

Thus, when in early 2021 WhatsApp made another unclear change to its privacy policy[23], regulators' attention sparkled again across Europe. In an emergency proceeding, the Hamburg DPA (the city where Facebook has its German headquarters) banned Facebook from processing WhatsApp users' data. The DPA also put pressure on the European Data Protection Board (EDPB) to intervene and make its emergency order "a binding decision" for all Member States. On July 15, 2021[24], the EDPB denied the emergency nature of the situation and charged the Irish DPC to conduct an investigation, without providing any timeline to do so, infuriating civil society organizations and the Hamburg DPA[25], unable to take matters into its own hands. However, on July 28, 2021, while addressing the merits of the objections of DPAs on the Irish draft decision, the

EDPB required the DPC[26] to adopt its final decision within one month, which finally happened on September 2, 2021[27]. To sum up, a decision impacting the privacy of millions of data subjects takes years to see the light and might not even be addressing the most recent issues of the company's behavior. This case well illustrates how convoluted and ineffective GDPR's enforcement mechanism is.

Originally presented as a necessary tool to foster efficient and coherent GDPR interpretation, the one-stop-shop mechanism has already proven to induce delays in procedure and widespread frustration. It also shows that the inactivity of one single authority can act as a bottleneck and put at risk the rights of all data subjects across Europe. This paralysis may, in part, have informed the recent Court of Justice decision[28] clarifying that non-lead DPAs can initiate legal proceedings before the courts of their own Member States against a company with its main establishment elsewhere in the EU.

If only one lesson is drawn from the GDPR's enforcement scheme it should be that a system centralizing its oversight around one institution should make sure the chosen institution is up for the tasks.

II. Solutions for cross-border enforcement in the DSA and the DMA

Enforcement of the DSA and the DMA might be easier since the scopes of the initiatives are much smaller than the GDPR. In fact, while the GDPR applies indifferently to the public and private sector, the two proposals are only targeting some private organizations (online intermediaries services[29] for the DSA and gatekeeper providers of core platform services[30] for the DMA). Also, while the GDPR applies to all processing of personal data, the DSA mainly targets regulation of online content and the DMA sets out obligations to ensure "contestable and fair markets"[31] across the Union.

As for enforcement, even though the two legislative initiatives adopt different approaches, they both give the European Commission a central role. Another common feature is the various timelines set out by the two initiatives to avoid latency and inertia, which appears as a lesson drawn from the GDPR.

The DMA enforcement mechanism

The enforcement's provisions of the DMA are sitting in Chapter V[32] (especially Article 25 and seq. DMA). Every step – investigation, monitoring, and enforcement powers – is centralized with and conducted by the Commission, granting minimal involvement to Member States. Per article 32 DMA[33], the "Digital Markets Advisory Committee" is a comitology committee[34] whose members will be representatives from the Member States, with referral capacity under Article 33 DMA[35], according to which three or more Member States can request the Commission to open a market investigation. In effect, Member States' role is limited to an advisory function.

As noted by some commentators[36], this centralized approach is rather unusual in the area of EU digital and economic regulation. Whether the Commission puts in place adequate staffing to tackle, all by itself, the extent of the DMA's tasks is yet to be seen. One of the consequences could be a sub-optimal level of enforcement, effectively

reproducing the bottleneck scheme seen with the GDPR. Unfortunately, the DMA does not offer alternative legal action or safeguards to avoid such an outcome. Article 35[37] merely provides the European Court of Justice a limited right to review some of the Commission's decisions (the ones imposing fines or periodic penalty payments).

The DSA enforcement mechanism

Even though the DMA's enforcement relies solely on the Commission, which is *per se* questionable, it has the benefit of providing a clear system. This is not the case for the DSA's enforcement, which involves various actors[38] alongside the Commission in a maze of responsibilities.

Each Member State needs to appoint a Digital Services Coordinator[39] who is responsible for supervising the intermediary services established in their Member State. All providers of intermediary services must designate a "single point of contact" for direct communication or, if they do not have an establishment in the Union, designate a legal representative in one of the Member States in which they offer services (Articles 10 and 11 DSA[40]). Similarly to the one-stop-shop mechanism of the GDPR, the Digital Services Coordinator (DSC) of the provider of intermediary services' main establishment (Coordinator of establishment) has sole jurisdiction (Article 40[41] DSA). However, unlike in the GDPR, the DSA provides strict deadlines for the Coordinator of establishment to answer a request of investigation and enforcement from another DSC or the Board of Member States Digital Services Coordinators (Board). Article 45 § 4[42] DSA requires the Coordinator of establishment to provide its assessment "without undue delay and in any event **not later than two months** following receipt of the request". If this time limit is not met, or if the DSC or the Board does not agree with the assessment, it can refer the matter to the Commission, which shall assess the matter **within three months**. Then, the Commission can send back the matter to the Coordinator of establishment for review, after which it has **two months** to "take the necessary investigatory or enforcement measures". To illustrate, if a matter is referred to the Coordinator of establishment on January 1st, and it passes through all stages, a decision should be made at the latest on August 1st. In comparison, it took more than three years to Luxembourg's DPA to reach a decision against Amazon[43] under the GDPR's enforcement system.

A different enforcement regime is organized for very large online platforms, over which the Commission has direct supervision powers and can, in the most serious cases, impose fines of up to 6% of the global turnover of a service provider. For these platforms, the Commission is the central and main regulator[44]. The Board has a purely advisory role, leaving the Member States outside of this system. If some commentators[45] hope this system may foster efficiency and speediness in oversight procedures and rightly compare it to what already exists in competition law, a more cautious commentator might be alarmed by the risks surrounding such centralization. Excluding Member States from the most serious cases and providing a monopolistic role to the Commission may led to dangerous consequences.

A critical evaluation of enforcement solutions in the DSA and the DMA

If the enforcement mechanisms laid down in the DSA and DMA avoid some of the issues of delays and inertia existing in the GDRP's cross-border enforcement system, they are not exempt of criticisms. Many Member States, including France, Germany, and the Netherlands, have already expressed[46] concerns that the DMA might have negative effects on existing national competition law regimes and their enforcement. In this regard, they asked for clarification on the articulation between the DMA and national competition law. They also asked to grant greater power to Member States.

Foremost, the centralization of power around the European Commission is problematic. First, as discussed above, the DMA places a heavy enforcement burden on the Commission who will need to gather and analyze an enormous amount of data[47], particularly during the launch phase. To be able to meet the extent of its responsibilities, the Commission will have to expand the number of its officials, but also its skillset to include *inter alia* computer and data scientists. The latter absence of technical know-how is already been considered[48] one of the reasons behind GDPR's enforcement failures.

Also, the enforcement powers provided to the Commission put the European separation of powers at stake. Traditionally, the Commission is presented as the executive arm of the European Union. However, its footprint has been expanding both in the legislative and judicial branches – a trend that continues with the DSA and the DMA. Both enforcement mechanisms are highly reliant on the Commission and don't provide an enforcement role to national judiciaries (under Article 41 § 3[49] of the DSA, they are left with a power to renew order restricting access of recipients of the service, which only happens after exhaustion of many other actions). By allowing itself to adopt "non-compliance decisions" (Article 58[50] DSA and Article 25[51] DMA) and impose heavy fines to the organizations (Article 59[52] DSA and Article 26[53] DMA), the Commission is more than the executive arm of the European Union; it is also applying its law and punishing law-breakers, like a court would do. Another element highlighting this role are the procedural rights recognized to the services and gatekeepers, such as the right to be heard and access to the file (Article 63[54] DSA and Article 30[55] DMA). Because the courts are often under-dimensioned or less specialized, it is becoming common in the digital sector to grant enforcement powers outside the court system.

To sum up, the Commission drafted the two initiatives (as the executive branch), will contribute to the legislative discussions (as an involved negotiator), and will be a key actor of their enforcements (as a judge). Such centralization of power can cause long-term democratic problems. As Montesquieu put it: "power curbs power" and it is of the utmost importance to make sure that power is distributed between institutions so they can operate as checks and balances and make sure there is no abuse or corruption of power. Unfortunately, the current system does not enable this.

Also, because the Commission was not created as a judiciary institution, it is not equipped or organized to take up that role. If the regulation stays as it is the Commission will need to drastically evolve or put at risk the enforcement of both regimes. We would not want latency, inertia, and blind eyes to become a common feature of the enforcement of European Digital Regulations.

In conclusion, what did we learn from the GDPR? Apparently, not enough. Both the DSA and DMA are centralizing most of their enforcements around one institution, the Commission. To avoid facing similar issues of latency and inertia, it seems crucial to better involve Member States, while providing a swift timeline for their contribution, and probably provide the judicial power with a bigger role. Fortunately, the proposals being still under negotiation, lots of refinements could still be made.

This article has originally been published on Verfassungsblog 2021/9/03, https://verfassungsblog.de/power-dsa-dma-10/.

Dr. Suzanne Vergnolle is a Post-Doctoral Fellow at the Swiss Institute of Comparative Law and the University of Lausanne.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) OJ L119/1.
[2] European Commission, "GDPR the fabric of a success story" (June 2020).
[3] Trevor Butterworth, "Europe's tough new digital privacy law should be a model for US policymakers" 23 May 2018 *Vox* https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge accessed 25 September 2021.
[4] Brave, "Europe's governments are failing the GDPR" (April 2020) p 3.
[5] Chris Jay Hoofnagle and others, "The European Union general data protection regulation: what it is and what it means" (2019) 28 Information & Communications Technology Law 65.
[6] European Commission, "What happens if my company processes data in different EU Member States?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-happens-if-my-company-processes-data-different-eu-member-states_en accessed 25 September 2021.
[7] European Commission, "Data protection as a pilar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" (communication), COM(2020) 264 final.
[8] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[9] European Commission, "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.
[10] *n 8* p 44.
[11] *n 9* p 33.
[12] Adam Satariano, "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates" (27 April 2020) NY Times https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html accessed 25 September 2021.
[13] GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights accessed 25 September 2021.

[14] Irish Data Protection Commission, "Annual Report 2020" (2021) p 48.
[15] *n 6*.
[16] Scott Ikeda, "Outgoing Privacy Commissioner Calls GDPR 'Broken,' Says That Basic Model 'Can't Work'" (1 July 2021) *CPO Magazine* https://www.cpomagazine.com/data-protection/outgoing-privacy-commissioner-calls-gdpr-broken-says-that-basic-model-cant-work/ accessed 25 September 2021.
[17] *n 16*.
[18] Access Now, "Three years under the EU GDPR – An implementation progress report" (May 2021).
[19] Samuel Stolton, "MEPs rue lack of GDPR sanctions issued by Irish data authority" (26 March 2021) *Euractiv* https://www.euractiv.com/section/data-protection/news/meps-rue-lack-of-gdpr-sanctions-issued-by-irish-data-authority accessed 25 September 2021.
[20] WhattsApp Blog, "Facebook" (19 February 2014) https://blog.whatsapp.com/facebook/?lang=en access 25 September 2021.
[21] WhattsApp Blog, "Looking ahead for WhatsApp" (25 August 2016) https://blog.whatsapp.com/looking-ahead-for-whats-app?lang=en accessed 25 September 2021.
[22] Michaela Ross, "Facebook, WhatsApp Fined by Spain for Failure to Obtain Consent" (16 March 2018) *Bloomberg Law* https://news.bloomberglaw.com/business-and-practice/facebook-whatsapp-fined-by-spain-for-failure-to-obtain-consent accessed 25 September 2021.
[23] Raphaël Grably, "Pour Whatsapp, le profit aux dépens de la confidentialité des données" (10 February 2021) *BFM Business* https://www.bfmtv.com/tech/pour-whats-app-le-profit-aux-depens-de-la-confidentialite-des-donnees_AD-202102100095.html accessed 25 September 2021.
[24] European Data Protection Board, "Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited" (12 July 2021).
[25] Hamburg Commissioner for Data Protection and Freedom of Information, "Press Release: Data exchange between WhatsApp and Facebook remains unregulated at European level" (15 July 2021) https://datenschutz-hamburg.de/assets/pdf/2021-07-15_EDSA_FB_en.pdf accessed 25 September 2021.
[26] European Data Protection Board, "EDPB adopts Art. 65 decision regarding WhatsApp Ireland" (28 July 2021) https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_en accessed 25 September 2021.
[27] Irish Data Protection Commission, "Data Protection Commission announces decision in WhatsApp inquiry" https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry accessed 25 September 2021.
[28] Heidi Waem, Simon Verschaeve, "EU: What's left of the GDPR's one-stop-shop? CJEU clarifies competences of non-lead data protection authorities" (5 July 2021) *DLA Piper* https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/ accessed 25 September 2021.
[29] *n 8* p 45.
[30] *n 9* p 37.
[31] *n* 9 p 34.
[32] *n 9* p 48.
[33] *n 9* p 54.
[34] European Commission, "Comitology" https://ec.europa.eu/info/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts/comitology_en accessed 25 September 2021.
[35] *n 9* p 55.
[36] Damien Geradin, "DMA proposal: Should there be a greater role for the Member States?" (7 April 2021) *The Platform Law Blog* https://theplatformlaw.blog/2021/04/07/dma-proposal-should-there-be-a-greater-role-for-the-member-states/ accessed 25 September 2021.
[37] *n 9* p 55.
[38] Crowell & Moring, "Digital Services Act: The European Commission Proposes An Updated Accountability Framework For Online Services (12 January 2021) https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Digital-Services-Act-The-European-Commission-Proposes-An-Updated-Accountability-Framework-For-Online-Services accessed 25 September 2021.
[39] *n 8* p 68.
[40] *n 8* p 50.
[41] *n 8* p 69.
[42] *n 8* p 74.

[43] Stephanie Bodoni, "Amazon Gets Record $888 Million EU Fine Over Data Violations" (30 July 2021) *Bloomberg* https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach accessed 25 September 2021.
[44] Ben Wagner, Heleen Janssen, "A first impression of regulatory powers in the Digital Services Act" (4 January 2021) *Verfassungsblog* https://verfassungsblog.de/regulatory-powers-dsa/ accessed 25 September 2021.
[45] *n 47*.
[46] Governments of France, Germany, and the Netherlands, "Strengthening the Digital Markets Act and Its Enforcement" (2021).
[47] Damien Geradin, "The DMA proposal: Where do things stand?" (27 May 2021) *The Platform Law Blog* https://theplatformlaw.blog/2021/05/27/the-dma-proposal-where-do-things-stand/ accessed 25 September 2021.
[48] *n 4*.
[49] *n 8* p 71.
[50] *n 8* p 81.
[51] *n 9* p 50.
[52] *n 8* p 81.
[53] *n 9* p 51.
[54] *n 8* p 83.
[55] *n 9* p 53.

Max Planck Institute for Innovation and Competition Research Paper Series

ISBN 978-3-00-070284-6