Reining in Big-Tech

Optimal enforcement under the Digital Services Act package

Candidate number: 9002

Number of words: 30 036
# Table of contents

## 1 INTRODUCTION

1.1 Big-Tech and VLOPs

1.2 The Digital Services Act Package

1.3 Research questions and relevancy

1.4 The scope and outline

1.5 Methodology

## 2 PRIVATE AND PUBLIC ENFORCEMENT OF REGULATION ON BIG-TECH AND VLOPS

2.1 Introduction

2.2 What is private enforcement?

2.3 Private enforcement vs. public enforcement

2.4 Legislation of interest

2.4.1 The GDPR

2.4.2 EU Competition Law

2.4.3 E-commerce directive

2.4.4 USA Legislation of interest

2.5 Final thoughts

## 3 ENFORCEMENT OF THE DIGITAL SERVICES ACT PACKAGE

3.1 Introduction

3.2 The DMA

3.2.1 General Information and Objectives

3.2.2 Subject matter, scope and definitions

3.2.3 The obligations

3.2.4 Enforcement approach

3.3 The DSA

3.3.1 General Information and Objectives

3.3.2 Subject matter, scope and definitions

3.3.3 The obligations

3.3.4 Enforcement approach

3.4 Enforcement under DMA and DSA

3.4.1 Is private enforcement under the DMA possible?

3.4.1.1 The preparatory work and Commission signals

3.4.1.2 Lack of provisions pertaining to private enforcement in the legislative text
3.4.1.3 Filling the procedural gaps in the DMA ............................... 51
3.4.1.4 Final thoughts ......................................................................... 55
3.4.2 The power of the national courts under the DSA ............................ 55
3.4.3 Optimality of DMA/DSA enforcement .............................................. 57
  3.4.3.1 Designation of gatekeepers and VLOPs ...................................... 57
  3.4.3.2 Commissions workload .......................................................... 60
  3.4.3.3 The goals at hand and the enforcement they call for .................... 63
  3.4.3.4 The future of private enforcement under the DMA/DSA .......... 66

4 CONCLUSION .......................................................................................... 69

TABLE OF REFERENCE ........................................................................... 71
1 Introduction

1.1 Big-Tech and VLOPs
Technologies like online platforms and digital services in general have undoubtedly changed the way we live our lives. The European Commission has stated that "online platforms are strong drivers of innovation and play an important role in Europe's digital society and economy [covering] a wide range of activities including online marketplaces, social media, creative content outlets, app stores, price comparison websites, platforms for the collaborative economy as well as search engines [increasing] consumer choice, [improving] efficiency and competitiveness of [the] industry and [enhancing] civil participation in society." In other words, online platforms and digital services have infiltrated several aspects of how our society functions at its core, bringing with them many societal-wide benefits for users, but also the internal market itself with regard to new business opportunities and facilitation of cross-border trading.

Most of the 10 000 online platforms that operate in Europe's digital economy are small and medium-sized enterprises (SMEs). That being said, a small number of the largest enterprises capture the biggest share of the overall value generated, benefiting from sectoral characteristics like strong network effects which are often embedded in their own platform ecosystems. These platforms "represent key structuring elements of today's digital economy, intermediating the majority of transactions between end and business users."

For the longest time, these large platforms have operated and grown under scrutiny, but also a general void in regulations aimed directly and specifically at them, allowing them "[amass] a major impact on, have substantial control over the access to, and [get] entrenched in digital markets" in turn leading to "significant dependencies of many business users on these large platforms, which leads, in certain cases, to unfair behavior vis-à-vis these business users" and "negative effects on the contestability of the core platform services concerned." These negative effects are undesirable as they in turn lead to "inefficient outcomes in the digital sector in terms of higher prices, lower quality, as well as less choice and innovation to the detriment of European consumers."

Likewise, information society services and intermediary services, such as social networks and online platforms in general, are today an important part of the Union's economy and the lives

---
1 European Commission (2022)(a).
3 Ibid.
4 Ibid.
5 Ibid.
of Union citizens, allowing "consumers to conclude distance contracts with traders [and] business users and to impart and access information and engage in transactions in novel ways." It is without a doubt that these services have contributed greatly to societal and economic transformation in Europe.  

Under the Covid-19 pandemic, technologies ensured that life could go on even with the steepest restrictions on our freedom of movement, showing the importance of technology and the "dependency of our economy and society on digital services [highlighting] both the benefits and the risks stemming from the current framework for the functioning of digital services." These services are now used daily, but this increase in use has made the risks more visible and prevalent and also introduced new challenges for Union citizens, companies, and society itself. These technologies are however here to stay, so much is for sure, as it is clear that their most positive effects are extremely desirable worldwide. In the joint report by the Earth Institute at the University of Columbia and Ericsson, it is stated that "meeting [the new Sustainable Development Goals] calls for a transformation of societies far deeper and faster than in the past – a rate of change that Business-As-Usual (BAU) approach simply cannot deliver" and that "the key accelerator technology that can get us off the BAU path is Information and Communication Technology."  

The risks of these technologies, be that unfairness leading to less innovation or infringement of fundamental rights, should on the other hand not be overlooked. Regulation of digital services pertaining to the mitigation and elimination of these risks and adequate enforcement of such regulation is therefore of utmost importance. As the EU also has stated:

"Responsible and diligent behavior by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union [...], in particular the freedom of expression and information, the freedom to conduct a business, the right to non-discrimination and the attainment of high level of consumer protection. [A] targeted set of uniform, effective and proportionate mandatory rules should [...] be established at Union level [to safeguard and improve the functioning of the internal market]."  

---

6 Regulation 2022/2065 Preamble (1).
8 Ibid.
9 Regulation 2022/2065 Preamble (1).
10 Sachs (2016).
11 Regulation 2022/2065 Preamble (3) and (4).
In recent years, the largest online platforms have fought in numerous inefficiently tackled competition cases, often focused on abuse of dominance or monopoly and anti-competitive mergers, raising an argument that traditional competition tools are less effective in reaching satisfactory outcomes in these cases, embedded in competition law enforcement in the digital sphere being "too complex, too slow, and at times too specific to protect effective competition in these markets or lacking the remedial measures necessary to preserve and restore the benefits of a competitive market to consumer", calling forth the need for ex-ante regulation of digital platforms.\textsuperscript{12} EU has also stated that existing Union law has not adequately addressed "the identified challenges to the well-functioning of the internal market posed by the conduct of large providers of digital platforms, which are not necessarily dominant in competition-law terms."\textsuperscript{13}

Aiming to combat the unfair practices of the world's largest online platforms and Big-Tech, protect the fundamental rights of Union citizens and other persons using digital services, and tackle the enforcement issues pertaining to these goals, the European Union has adopted two new regulations, The Digital Markets Act\textsuperscript{14} (DMA) and the Digital Services Act\textsuperscript{15} (DSA) which together constitute The Digital Services Act package. The goals, as formulated by the Commission\textsuperscript{16}, are I) to "create a safer digital space in which the fundamental rights of all users of digital services are protected", and II) to "establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally."\textsuperscript{17} The regulations aim to do this in their own right, tackling their respective areas, their mutual goal being to once and for all rein in very large online platforms (VLOPs) and Big-Tech and secure prosperity and safety in the European Digital Market.

1.2 The Digital Services Act Package

The objective of the DMA is to "allow platforms to unlock their full potential by addressing at EU level the most salient incidences of unfair practices and weak contestability so as to allow end users and business users alike to reap the full benefits of the platform economy and the digital economy at large, in a contestable and fair environment."\textsuperscript{18} The envisioned benefits of the DMA are, as formulated by the Commission, I) "ensuring a fairer business environment for business users who depend on large online platforms to offer their services in the single market", II) "new opportunities for investors and start-ups to compete and innovate in the online platform environment without having to comply with unfair terms and conditions limiting their

\textsuperscript{12} OECD (2021) p. 11.
\textsuperscript{13} Regulation 2022/2065 Preamble (5).
\textsuperscript{14} Regulation 2022/1925.
\textsuperscript{15} Regulation 2022/2065.
\textsuperscript{16} The European Commission.
\textsuperscript{17} European Commission (2023)(a).
\textsuperscript{18} COM/2020/842 p. 2-3.
development", III) "more and better services for consumers pertaining to switching of providers", IV) "direct access to services and fairer prices" and V) "opportunities for gatekeepers to innovate and offer new services."

The DSA on the other hand sets out to reform the existing EU e-commerce legal framework while "maintaining the core principles of its liability regime, the prohibition of general monitoring and the internal market clause, which it considers to still be valid today." By "[c]onfirming the objectives of the e-Commerce Directive, the regulation [intends to] implement measures which have consumer protection at their core, by including a detailed section on online marketplaces, and which ensure consumer trust in the digital economy, while respecting users’ fundamental rights."

Akin to the GDPR\textsuperscript{21}, The Digital Services Act package seemingly intends to achieve compliance mainly through the threat of issuing enormous fines for non-compliance, that being fines of up to 6\% of global turnover in the event of non-compliance with the DSA by VLOPs and even a ban on operating in the EU single market in case of repeated serious breaches,\textsuperscript{22} and a fine of up to 10\% of total worldwide turnover in the event of non-compliance with the DMA and 20\% for a repeat offence.\textsuperscript{23}

Even though the envisioned preventive enforcement is not without merit, the question of private ex-post enforcement of the regulations is in many ways yet to be answered. The regulations tackle this in a different manner, DSA being the regulation that devotes far more provisions to the question than the DMAs singular provision in Art. 39 on cooperation with national courts. This is not abnormal seeing that the regulations have a very different approach to enforcement, DSA being Member State-based and DMA being Commission-based or centralized.

Particularly the DMA lacks any explicit recognition of how exactly the regulation is to be enforced in the national courts, even though the Commission itself has stated that "the DMA as a regulation, contains precise obligations and prohibitions, that can be enforced directly in the courts."\textsuperscript{24} The omission of concrete procedural provisions begs the question of whether procedural rules of competition law should be applied, whether the DMA should be complemented by other EU law/national law, or whether the regulation requires legislative changes for private enforcement to at all be possible.

\textsuperscript{19} European Commission (2022)(b).
\textsuperscript{20} COM/2020/825 p. 1.
\textsuperscript{21} Regulation 2016/679.
\textsuperscript{22} European Commission (2022)(c).
\textsuperscript{23} European Council (2022).
\textsuperscript{24} European Commission (2023)(b).
Seeing that the enforcement approach of the DMA is Commission-based, another question that arises is the mere practicality and effectiveness of such enforcement. The bulk of the decisions in the scope of the regulation fall within the power of the Commission, such as designation on who the obligors are, which in a sense diminishes the national courts from awarding civil remedies where infringement is present, but the Commission’s designation is not.

Even though the DSAs approach to enforcement is Member-State-based, with private enforcement being far more prevalent, this does not apply to the VLOPs. The regulation itself raises several questions regarding the power struggle that may incur between the Member States and the European authorities. Zeybek has stated that "[i]n line with the delicate balance between the country-of-origin principle and the wish of Member States to exercise power over online platforms directly, the DSA reflects a complex interaction between national and European authorities."\textsuperscript{25} It is therefore of interest to examine this balance, but also examine whether the proposed enforcement under the DSA is an effective tool in the fight against VLOPs and Big-Techs infringements.

1.3 Research questions and relevancy

The focus of this thesis is enforcement of regulation as a tool for combating unfair and unlawful behaviors of Big-Tech companies and VLOPs. A question that needs to be answered on a general basis is what kind of enforcement has been a good enforcement approach to pushing back such behavior historically. By viewing past legislation pertaining to these actors we will try to examine what optimal enforcement entails. In doing so this thesis will examine the both private and public enforcement's suitability as a means to combat unlawful behavior pertaining to Big-Tech and VLOPs.

This thesis will further delve into issues pertaining to the enforcement of the Digital Services Act package specifically, with one overall goal being answering whether national courts indeed are effectively empowered to award civil remedies to the victims of DMA/DSA infringements, and by doing so are one of the forces which will over the coming years be able to lay the groundwork for responsible and diligent behavior by these enterprises and a level playing field in the Union. The other goal of the thesis is to identify flaws with the proposed enforcement and recommend solutions where this is prevalent.

This thesis will show that The Digital Services Act package as it stands pertaining to Big-Tech and VLOPs needs to be revised. It will show that although inspiring, the almost sole public enforcement approach of the regulations at hand will undoubtedly lead to inertia. The thesis will establish a need for expansion in rules pertaining to private enforcement of the provisions

\textsuperscript{25} Zeybek (2022).
pertaining to VLOPs and Big-Tech, towards reaching the optimal enforcement, and securing that the goals of the Digital Services Act package are met.

The Digital Services Act package has been approved by the European Parliament and the Council of the European Union. The DMA and the DSA will indisputably change how our digital services operate, materially and competitively. Even though the acts won’t take effect immediately in full, the need for clarity on their procedural side is of importance. The European Union has already stated that social media platform Twitter could face sanctions after the suspension of journalists.26

This thesis will show that there is no clear and straightforward answer pertaining to the question of private enforcement under the Digital Services Act package, elevating the importance of discussion of precedents, viability and conformity. If the Digital Services Act Package indeed opens possibilities for infringed parties to seek civil remedies, it is of detrimental importance to understand the scope of these possibilities and by doing so assuring that the legal system is prepared for the role this may lay upon it, but also its role in finally reining in tech giants and VLOPs.

1.4 The scope and outline
We will begin this thesis by discussing private and public enforcement of regulation on Big-Tech and VLOPs in Chapter II. This will be done by first answering what private enforcement is under Section 2.2, before comparing it to public enforcement under Section 2.3. The point of this exercise is to determine when and why these types of enforcement are optimal, whether that be on their own or in unison. We will further apply this knowledge to, whilst also gaining practical knowledge from, relevant legislation pertaining to Big-Tech and VLOPs, hereunder the GDPR, EU Competition Law, E-Commerce Directive and legislation from the USA. The overall goal of Chapter II is to extract the relevant information pertaining to future enforcement efforts under the Digital Services Act package.

We will then move on to discussions of the Digital Services Act package under Chapter III, firstly general examination of the objectives and obligations under Sections 3.2 and 3.3, with the goal of giving the reader an overview of legislation’s material aspects. We will then move on to a more specific analysis of the procedural aspects of the regulations under Section 3.4, examining what they will entail, the issues with them, and discussing possible solutions, all whilst applying the knowledge we have gained from Chapter II of the thesis. We will finally make a brief conclusion under Chapter IV of the thesis.

26 Milmo (2022).
The thesis will not delve into the specifics of the national law of each of the EU Member States. National legislation and case law will however be used as an example where this is illustrative.

1.5 Methodology

This thesis seeks to shed light on ex-post enforcement of legislation on Big-Tech and VLOPs. As the main goal is determining how regulation on Big-Tech and VLOPs should be optimally enforced and whether DMA and DSA indeed as they stand are to be optimally enforced, several research methodologies are used.

A doctrinal legal research methodology is applied throughout this thesis. This can be seen in Chapters II and III in discussions on legislation such as the GDPR, legislation pertaining to EU Competition Law, the E-Commerce Directive and the Digital Services Act package. The use of this research methodology is a given in discussing the procedural aspects of specific legislation. We have to look at the text of the provisions themselves as well as the relevant case law to better understand the procedural rules in front of us and identify their qualities and weaknesses. This thesis has a high focus on relevant commentaries pertaining to the issues of legislation it discusses and combines past research to get the clearest possible picture of what has gone wrong with past legislation on Big-Tech and how it should be addressed.

The focal point of the thesis is the Digital Services Act package, EU legislation. The thesis, therefore, centres on legal sources of EU relevance. Primary, secondary and supplementary law is used in analyses. National law is rarely explicitly examined because of the scope of the thesis. Its existence and role in the EU are however acknowledged as important.

As we are looking into the enforcement of laws, this thesis distances itself from a formal-dogmatic approach. The procedural elements of the legislation in this thesis are not only examined as laws; considerations are made about economics and politics which certainly play a crucial part in how the enforcement of laws functions. An empirical approach is therefore instead present where the letter of the law cannot give us a sense of how pragmatic the enforcement apparatus is. It is only by examining how the law has been enforced, that we can conclude if such enforcement has been optimal.

The majority of this thesis pertaining to optimal enforcement of the DMA and DSA applies a comparative research methodology. Where doctrinal legal research and empirical methodologies can get us closer to understanding what optimal enforcement of legislation pertaining to Big-Tech and VLOPs entails, it is only through comparing their enforcement with that of the Digital Services Act package, that we can get a sense of how well the latter will be enforced. Comparative research methodology is principally used in such a manner; comparing past legislation with each other and with that of the DMA and DSA. A small portion of the thesis is
devoted to acknowledging relevant proposed legislation outside the EU with the goal of getting another point of view.

One of the weak points of this thesis that must be recognized is based on the empirical data which has been used. Mapping of empirical data pertaining to public and private enforcement generally and that of regulation on Big-Tech and VLOPs is a colossal task. For this reason, the thesis significantly leans on past research conducted on these issues by experts in the field. Their views are as mentioned used intertwiningly, with the goal of getting the most precise picture of relevant factors pertaining to optimal enforcement of Big-Tech and VLOP legislation.

It should further be acknowledged that full enforcement of the Digital Services Act Package is yet to commence. Because of this, several assumptions, all though based on reason, are made and accepted in this thesis. The final judgement of the optimality of DMA/DSA enforcement is yet to be made based on how the enforcement pans out to work.

The thesis aims to be as objective as possible. It would however be remiss not to note that the presented data highly favours the use of private enforcement. Opposing views praising centralized European enforcement have not been specifically sought out nor presented. On the other hand, the benefits of a Digital Single Market have been panned out and given a proper place in the thesis in discussions on enforcement, without specifically addressing opposing views of this. The reason for the first emission is that the thesis doesn't suggest that public enforcement of the DMA and DSA is a bad approach, and public enforcement is after all very prevalent in the regulations. The reason for the second emission is based in scope of the thesis, that being specific discussions on enforcement.

The thesis deals with enforcement of the Digital Services Act package. As will become apparent, the enforcement apparatus of the DSA is enormous and deals with actors with different sizes and influence. The thesis therefore mainly focuses on those provisions regarding VLOPs. However, considering the overall enforcement is important in trying to understand the effectiveness of those enforcement mechanisms proposed for VLOP infringements.

Finally, even though the focus of the thesis is discussions on procedural aspects of relevant legislation, the ascertaining and to a degree analysing of the material rules is present where this is relevant. As we are dealing with specialized legislation, bearing in mind the material rules may help better understand the enforcement they call for.
2 Private and public enforcement of regulation on Big-Tech and VLOPs

2.1 Introduction
In this chapter of the thesis, we will investigate private and public enforcement pertaining to legislation on VLOPs and Big-Tech. We will first look at what private enforcement entails, before comparing private enforcement to public enforcement, trying to determine when and why each of these are more prevalent. Finally, we will investigate enforcement efforts which have been made or are proposed in such legislation, excluding the Digital Services Act package. We will continuously extract knowledge which will later be used in analyzing the Digital Services Act package.

2.2 What is private enforcement?
Law enforcement happens through several means. This thesis partially focuses on private enforcement of the Digital Services Act package pertaining to regulation of VLOPs and Big-Tech, and it is therefore of relevance to discuss what private enforcement exactly entails, look at private enforcement against its counterpart which is public enforcement and finally look at examples of private and public enforcement pertaining to regulation of VLOPs and Big-Tech both in legislation and specific case law. Let's start with a simple question; what is private enforcement?

Even though the question is simply phrased, the answer is far from well defined. Jens-Uwe Franck writes that "the gist of the concept [of private enforcement] is that a private individual can bring an action against [an] infringer to force them to end an illegal activity or to compensate a loss caused by an infringement", continuing "[t]hus, plaintiffs not only protect their own interest but also serve en passant the general interest in effective and efficient enforcement of the law."27 Public enforcement on the other hand, has a much clearer shared vision, that being government agencies, or union bodies in case of EU law, investigating suspicious activities and bringing eventual breaches of the law before courts, directly requiring that the infringement be ceased or imposing a fine on the breacher.

Podszun states that private enforcement in competition law has been around in EU Member States for a long time, pointing to the Notice on the handling of complaints to the Commission28 which states: "Depending on the nature of the complaint, a complainant may bring his complaint either to a national court or to a competition authority that acts as public enforcer."29 Interestingly, Podszun points out that "[d]espite this reliance on private enforcement in rejection

---

28 Commission Notice 2004/C 101/05.
decisions, there is little official recognition and support of the power of private enforcement in stopping infringements", the point being that private enforcement is mostly seen as the equivalent to damages claims, having no bearing on reversion or prevention of non-compliance with the rule of law. Podszun alike Franck does however himself acknowledge that private enforcement not only pertains to awarding of civil remedies, but in fact "may also lead to the prohibition of anticompetitive behaviour trough injunctions or full-fledged judgments given by regular courts."

In 2004, European Commissioner for Competition matters Mario Monti stated the following, "I believe the greater private enforcement of Community competition law would bring clear benefits for the functioning of the internal market and the competitiveness of the European economy", following up with the benefits: I) "[t]he threat of such litigation has a strong deterrent effect and would lead to a higher level of compliance", II) "[i]ncreased private action would further develop a culture of competition amongst market participants, including consumers, and raise awareness of the competition rules, and" III) "[p]rivate litigants may take action against infringements which the Commission and the national authorities would not pursue, or do not have sufficient resources to deal with." Monti would later in the speech go on to state that private action also would have benefits for private parties, such as compensation, civil sanctions of nullity in contractual relationships, awarding of legal costs, combining of claims and national courts being both obliged to hear cases and being better placed to award civil remedies.

As such, private enforcement should primarily be seen as enforcement of law with the primary characteristic of deterring non-compliance and infringements and developing the nooks and crannies of the given law. Secondarily, private enforcement has the positive effect of remedying infringements and restoring balance between private parties. This statement should not elevate the importance of the primary characteristic; for an infringed private party, restoration of balance is naturally the main objective and focus. The important thing is recognizing that private enforcement indeed is a suitable measure for achieving market goals that go beyond awarding of civil remedies in one particular case and is therefore of both public and private interest.

In the following section we will take a closer look at the difference between private and public enforcement on a general level. Both types of enforcement are relevant for The Digital Services Act package.

---

30 Speech/04/403 p. 2
31 Ibid. p. 3
2.3 Private enforcement vs. public enforcement

Public enforcement of law is well explained through the notion of parens patriae\textsuperscript{32}. Indeed, public enforcement is at its core use of governmental resources to investigate, find and sanction non-compliance with law on behalf of the citizens. A general distinction which could be made about private and public enforcement is that they serve different purposes in different situations and areas of law; whereas an area such as criminal law naturally favors use of public enforcement, enforcement of torts and contract law for instance, primarily depends on private enforcement. The main reason for this distinction is that a user of private enforcement depends on knowledge on who their infringer is, whilst this isn’t always the case in public law.\textsuperscript{33} Enforcement of certain areas of law also naturally demands more resources than other, resources sparsely available to private parties. For instance, we can state that suing for compensation after buying a faulty car demands less and more available resources than suing a company which through its pollution has inflicted cancer on a community. It should be noted that even the last example can be an object of private enforcements efforts, a fairly normal practice in the USA\textsuperscript{34}, but the somewhat clear assumption is that a government with far more resources is better equipped to fight such lawsuits on behalf of its citizens. As we will see, in some cases, companies can however be more naturally equipped to take matters into their own hands.

The abovementioned distinction between private and public enforcement of law is general. The distinction does however emphasize that private and public enforcement both are preferable in different situations. An important step in determining viability of private enforcement under the DMA and the DSA is determining when and why these different types of enforcement are preferable. Private and public enforcement are furthermore not mutually exclusive\textsuperscript{35}, but a question that is relevant here is whether application of both is preferable in enforcement of one and same legislation.

Klöhn outlines the differences between private and public enforcement in a paper trying to determine when laws should be enforced publicly and when they should be enforced privately. Klöhn writes that the discussion on private vs. public enforcement “is a part of the economic theory of regulation” concerning “the optimal structure of law, namely, who should be the actor initiating and prosecuting the enforcement of laws”.\textsuperscript{36}

\textsuperscript{32} “Parent of the country or homeland”, The doctrine under which a state has third party standing to bring lawsuits on behalf of a citizen see Cornell Law School (2022) definition by Legal Information Institute at Cornell Law School.

\textsuperscript{33} Polinsky (2005) p. 4.

\textsuperscript{34} See i.e. Pierson (2006), Class action PG&E litigation over groundwater contamination, case settled for $295 million.

\textsuperscript{35} See i.e. GDPR Art. 77 (public enforcement) and Art. 79 (1) (private enforcement).

\textsuperscript{36} Klöhn (2010) p. 2.
With regard to private enforcement the paper outlines that private enforcement may give the judiciary a better opportunity to "refine vague and general standards" by bringing more suits into the court of law, further outlining that private parties are more likely than public to "develop novel strategies."

With regard to contract law for instance, Klöhn points out that private parties have better incentives and are therefore "in the best position to litigate contractual matters." The point undoubtably has merit; pursuing the wrongdoings committed against you and trying to remedy them through such legal pursuit is naturally grounded in a higher level of determination than that of a government agency doing so on your behalf. This is simply because the government has less to lose should the case not end up in your favour. This determination surely inspires greater research and cleverer strategies which in turn may help the judiciary get a clearer picture of what is perhaps a muddy area of law and in turn arrive at the correct conclusion. It is also natural to assume that funding your own lawyers gives the opportunity to seek better and specialised council, who in turn has to perform well or risk losing the client.

Klöhn further points out that private enforcement can be more efficient because a private party may have better information about the wrongdoing, a point we have already made. He does however state that private enforcement may lead to overenforcement, assuming that private enforcement doesn’t generate high costs. The argument is fairly grounded seeing that a private party with a subjective point of view more often may deem their knowledge to be knowledge of illegal wrongdoing, rather than a legal annoyance. The argument is however less valid without the assumption on litigation costs which are usually high, and therefore deter frivolous litigation.

Finally, with regard to private enforcement, Klöhn points out the danger of increasement in erroneous decisions on difficult issues decided on by courts alone without involvement of a public body beforehand. This argument definitely strikes at the core of the principle of separation of powers and the delicate balance between the judicial and the executive branch. A decision contrary to the material of the legislative branch which the executive branch executes, would do more harm than good by stealing future resources towards resolving the issues that arise from the decision. Furthermore, it could be argued that the judiciary is less inclined to rule

---

37 Ibid. p. 13, the paper assumes that private actors bring more suits to court (statistics on private v. public litigation).
38 Ibid. p. 15, see also p. 9 "public service employees usually receive a fixed salary and do not gain directly from enforcing the law".
39 Ibid. p. 10, the paper mentions that private individuals in some areas of law "have a "natural" informational advantage".
41 Ibid.
on huge and difficult matters without prior and thorough knowledge of the views of the executive and legislative branch, simply because the magnitude of power the judiciary has is often in the hands of the legislative branch. This could in turn lead to an ineffective judiciary branch.

Another negative side of private enforcement of Big-Tech legislation specifically is outlined by Podszun:

"Companies like Google, Amazon or Facebook are among the most powerful in the world, and private litigants will think twice before taking on such undertakings-their resources guarantee them access to the best lawyers and a stamina to fight cases til the end. This prospect may disincentivize claimants, in particular if they are dependent on the gatekeeper. In addition, courts may be less inclined than competition agencies to approve of new theories of harm, in particular with relation to digital gatekeepers."

Pdkszun however dismisses this "common theme" of ineffectiveness of private enforcement due to the David-Goliath ratio between claimants and Big-Tech companies by looking at concrete case law. We will revisit this in Section 2.4.2 of this thesis on EU Competition Law.

With regard to public enforcement, Klöhn states that it can be beneficial due to its high ability to deter wrongdoers. Public enforcement, carried out by government agencies or public prosecutors, sends a clear message that violations of the law will not be tolerated, and wrongdoers will be held accountable, one of the main principles of criminal law. The threat of fines, penalties, or even imprisonment can deter potential wrongdoers from engaging in unlawful activities. This deterrence effect helps maintain social order and promotes compliance with the law, which private parties in turn greatly benefit from simply by being a part of a just society.

As stated, Klöhn's opinion is that private enforcement may be more efficient because the private party may have better information about the wrongdoing. Such assumption isn’t always the case, however. Polinsky in greater detail describes why public enforcement is better when the private party in fact doesn’t have information about the wrongdoing. A lack of information calls for gathering of information. Polinsky writes that the state in such cases most often will not permit private parties to use force. The same goes for capture of violators and prevention of reprisals. Furthermore, government agencies have and continue to develop expensive information systems to aid enforcement, something private parties may find hard to capture the

42 The argument is alarming but not removed from reality, see i.e. U.S. Const. Art. III, Section 2, Clause 2 which gives the Congress the power to make "exceptions" to the Supreme Courts appellate Jurisdiction.
43 Podszun (2021)(a) p. 2.
benefits of fully. We can assume that resources spent on such information systems are better spent on innovation etc.

We have discussed Klöhn's opinions on prevalence of frivolous lawsuits with regard to private enforcement. Klöhn argues the opposite with regard to public enforcement stating that "[w]hile this danger exists in a system of public enforcement of laws as well, it does not seem as severe because public agencies have a limited budget and can be held accountable for excessive litigation." Indeed, governmental agencies are funded by the state, meaning that their litigation pursuits must be grounded in a reasonable amount of evidence pointing to illegal activities. If not, the agencies and the government itself would be the target of severe scrutiny, perhaps even political upheaval.

With the abovementioned point in mind, public enforcement according to Klöhn may suffer from resource constraints. Public enforcement agencies often have limited resources, such as funding, personnel, and expertise, to effectively enforce laws and regulations at every turn. This can hinder their ability to monitor and detect violations against private actors, investigate cases thoroughly, and impose penalties on wrongdoers. We can further assume that government agencies responsible for public enforcement may be subject to bureaucratic inefficiencies, such as cumbersome decision-making processes, lack of coordination between different departments, and complex regulatory frameworks. These inefficiencies can in turn result in slow enforcement actions, inconsistent application of laws and lack of transparency in the enforcement process. Additionally, the “bureaucratic red tape” may impede the effectiveness of enforcement actions and discourage innovation in enforcement strategies. Resource constraints can also lead to a backlog of cases, delayed enforcement actions, or even selective enforcement, which may allow some violations to go unpunished. Klöhn states that this happens every day; "the police overlook minor infractions of the traffic code; building inspectors ignore violations of building-code provisions that, if enforced, would prevent the construction of new buildings in urban areas". As we have discussed, this issue is not uncommon in private enforcement where private parties are far less resourceful than the government agencies in cases of magnitude, hindering desirable enforcement on the basis of cost. Resources are therefore a constraint on both public and private enforcement, yet the point that a government is better equipped to fight cases of magnitude

---

48 See The Economic Times (2007) "Red tape is a derisive term for excessive regulation or rigid conformity to formal rules that is considered redundant or bureaucratic and hinders or prevents action or decision-making."
49 Klöhn (2010) p. 12, the paper does however outline that "such discretionary non-enforcement can reduce the social costs of overinclusion, laws containing enforcement mechanisms for both favourable and non-favourable instances of enforcement, without a corresponding increase in under-inclusion."
where illegality is visible\textsuperscript{50}, stands at least when it comes to private citizens being the infringed party.

We have also mentioned that frivolous litigation from states side may lead to scrutiny/political upheaval, and it is therefore important to outline that public enforcement is also susceptible to potential political influences. Klöhn doesn’t mention this point, but this thesis would be remiss if we weren’t to touch upon the subject bearing in mind the political climate of our age.\textsuperscript{51} Governments are formed by political parties with their own political agendas in mind. This can lead to situations where enforcement priorities are shaped by political agendas, rather than the objective needs. In turn, this can lead to important cases being overlooked or frivolous cases being blown out of proportion. The principle on separation of powers is meant to remedy such situations with an independent judiciary, yet the rule of law would either way be hurt just by such occurrence or rather the stagnation in enforcement. As there are no concrete studies to show to with regard to this point, we will not give it an elevated spot in this thesis.

As we can gather, both private and public enforcement have their up- and downsides. The natural conclusion is therefore that each type of enforcement has a sacred part in achieving optimal enforcement of laws. Klöhn’s article shows us that the optimal mix of private and public enforcement depends on the specific circumstances and the underlying objectives of the legal system. Factors such as the type of law being enforced, the potential harm caused by violations, and the available resources for enforcement should be considered when determining the most efficient enforcement mechanism.

With regard to the type of law being enforced as a factor, it should be noted that different laws have different objectives and complexities, which may require tailored enforcement approaches. For instance, enforcing criminal laws as stated, often demands a higher level of government intervention and a more robust public enforcement mechanism due to public safety concerns. In contrast, enforcement of contract or intellectual property laws may rely more on private parties, who have a personal stake and better information on the issue and their infringer.

With regard to potential harm caused by violations as a factor, it should be noted that the severity of harm resulting from violations plays a crucial role in deciding the appropriate enforcement mechanism. In cases where the potential harm is widespread or severe\textsuperscript{52}, public enforcement may be more appropriate due to its ability to protect the broader public interest and deter future

\textsuperscript{50} i.e. example where a company’s pollution leads to a whole community getting sick with cancer.

\textsuperscript{51} We have since 2016 been witnessed several calls for investigations in the USA from both sides of the political aisle in different cases, some well-grounded and others perhaps not so much.

\textsuperscript{52} i.e., environmental pollution, financial fraud, or public health risks.
violations. For less severe or localized harms, private enforcement may be a more efficient and targeted approach.

With regard to available resources for enforcement as a factor it should finally be noted that the resources available for enforcement, such as funding, personnel, and expertise, can impact the effectiveness of the chosen enforcement mechanism. Public enforcement may be more efficient in jurisdictions with well-funded and staffed regulatory agencies, while private enforcement may be preferable in situations where public resources are limited. In some cases, a combination of both public and private enforcement might be the most efficient approach to ensure that laws are effectively enforced while optimizing the use of limited resources.

By taking these factors into account, policymakers and legal authorities can design enforcement strategies that strike the right balance between public and private mechanisms which ultimately leads to optimal enforcement of law. The question that remains is how these factors define optimal enforcement of legislation concerning VLOPs and Big-Tech, especially the DMA and the DSA. To determine this, we will have to examine such legislation as well as the impact and success it has had.

In the following section we will look at past legislation which is of interest pertaining to the discussion of suitability of private and public enforcement as a measure for VLOP and Big-Tech compliance. This includes the GDPR, EU Competition Law, the E-Commerce Directive which the DSA builds on, but also some proposed legislation in the USA pertaining to competition issues. The relevance of the E-Commerce directive is grounded in "Member States […] increasingly introducing […] national laws on the matters covered by [the DSA], in particular, diligence requirements for providers of intermediary services as regard the way they should tackle illegal content, online disinformation or other societal risk."\(^5^3\) In light of this, the discussion on this will also on a more general level touch upon national law. Discussions will focus on both sides of enforcement. Understanding the prevalence of them also entails discussions on the interplay between them.

### 2.4 Legislation of interest

#### 2.4.1 The GDPR

The General Data Protection Regulation is a comprehensive data protection legal framework that has applied in the EU since 2018.\(^5^4\) The Regulation replaced the previous Data Protection

---

\(^5^3\) Regulation 2022/2065 Preamble (2).

\(^5^4\) European Commission (2022)(d).
Directive\textsuperscript{55} with the purpose of harmonizing data privacy regulation within the Union and ensuring a high level of data protection for Union citizens.\textsuperscript{56} The Regulation "lays down rules relating to the protection of natural persons with regard to processing of personal data and rules relating to the free movement of personal data" pursuant to Art. 1, personal data meaning "any information relating to an identified or identifiable natural person" pursuant to Art. 4 (1) and processing meaning "any operation or set of operations which is performed on personal data" pursuant to Art. 4 (2).

The GDPR applies to all natural and legal persons that process or control personal data of data subjects within the union, regardless of where they are located, with some exceptions pursuant to Art. 3. A data subject is an identified or identifiable person pursuant to Art. 4 (1). The Regulation sets out a range of rights regarding individuals' personal data pursuant to Chapter III. It further imposes significant obligations pertaining to processing of personal data carried out by controllers, meaning entity determining "the purposes and means of the processing of personal data" pursuant to Art. 4 (7) and processors, meaning entity "which processes personal data on behalf of the controller" pursuant to Art. 4 (8). The GDPR is therefore of significant importance pertaining to regulation of VLOPs and Big-Tech which naturally process large amounts of personal data.

The Regulation includes provisions on public enforcement such as imposing of fines for non-compliance with the Regulations set of obligations pursuant to Art. 83. Every data subject has a right to lodge a complaint with a supervisory authority pursuant to Art. 77 (1). These are Data Protection Authorities, DPAs, established in each Member State pursuant to Art. 51 (1). Where the data subject is not satisfied with a decision of a particular DPA, the data subject has a right to an effective judicial remedy against the decision pursuant to Art. 78 (1).\textsuperscript{57} Finally, matters can also be brought before the Board\textsuperscript{58} cf. Art. 78 (4).

The Regulation also has provisions on private enforcement, allowing infringed parties to bring legal action against controllers and processors for infringement of their rights. Art. 79 (1) of the GDPR states that "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the Regulation", without prejudice to any available administrative or non-judicial remedy. Proceedings against such a controller or processor "shall be brought before the courts of the Member State where they have

\textsuperscript{55} Directive 95/46/EC.
\textsuperscript{56} Regulation 2016/679 Preamble (10).
\textsuperscript{57} This can be viewed as part public, part private enforcement.
\textsuperscript{58} The European Data Protection Board.
an establishment" pursuant to Art. 79 (2). Art. 82 regards liability of controllers and processors and provides the right to compensation to those who have "suffered material or non-material damage as a result of an infringement of the Regulation."

GDPRs enforcement approach based on both public and private enforcement, seems like an idyllic solution for achieving compliance as well as awarding due civil remedies where infringements are present. GDPR is after all a massive piece of legislation, obliging many and giving rights to even more, calling forth the need for great resources to ensure enforcement. Perfection is however a standard hard to achieve, so we ought to ask ourselves what problems the GDPRs enforcement mechanisms have had during the past few years. Let's start by looking at private enforcement.

The biggest problem with private enforcement under GDPR, is that we have seen so little of it. In Norway for instance, *Legelistesaken*\(^{59}\) is one of the few cases that has been before the Supreme Court, and even in that instance, the case was litigated by The Norwegian Medical Association against Norway's DPA, meaning that the procedures started with a complaint to the DPA, making the enforcement public in part. Lodging complaints to the various DPAs has been the status quo pertaining to GDPR enforcement, and we ought to ask ourselves, why?

The natural conclusion to the question above is based in the practicality of the DPA route. It is after all easier to lodge a complaint to the DPA whilst also retaining the resources one would otherwise have to use taking the court route from the beginning. It is normal to take what seems like the easier route. Furthermore, examining right to compensation under Art. 82, it is also apparent that litigation based on this rule isn't as straightforward as it may seem. How is one to go about in ascertaining non-material damages resulting from an infringement of the Regulation? On the other hand, GDPR is still young, and there is reason to believe that a rule like that of Art. 82 would in time be fleshed out before the courts. Nonetheless, not much of private enforcement under GDPR has been seen, but what can we deduce from what we have seen?

Rucz writes that "[s]trategic litigation against public participation is a threat to public interest journalism" and that "[a]lthough typically a defamation claim underpins [such litigation], the GDPR may serve as an alternative basis."\(^{60}\) Strategic litigation against public participation (SLAPP) is a technique "to limit freedom of expression […] taking advantage of a legal void or grey zones between legal norms" the purpose being "not to seek justice but to intimidate, silence and drain the financial and physical resources of the targeted victims."\(^{61}\) An article by

---

\(^{59}\) HR-2021-2403-A.

\(^{60}\) Rucz (2022) p. 378.

Liberties points out that the GDPR "is giving rise to unintended consequences insofar as it is emerging as a new battleground for strategic lawsuits" pointing to Croatian Journalists' Associations statistics showing that high-ranking politicians, government members and public officials stand behind some of the 924 active lawsuits against journalists and media outlets in Croatia, whilst journalists and the media top the list of SLAPP targets.62

As we are researching enforcement targeting VLOPs and Big-Tech, the notion of SLAPPs being a problem is perhaps farfetched seeing that these types of companies and providers aren't the usual target of such litigation. On the other hand, an argument can be made that GDPRs private enforcement approach can lead to excessive and frivolous claims being directed at the largest companies processing personal data, with a goal of being awarded unjust civil remedies. However, no such conclusion can be drawn at this point.63 Furthermore, the argument can be made for any type of legislation giving private individuals and entities the right to seek civil remedies in courts. Abuse of procedural mechanisms is certainly prevalent with these kinds of legislation. It is however the courts that must recognize such abuse and deny the abusive litigation. The point must therefore be that GDPRs private enforcement mechanisms have seemingly not opened a floodgate for a myriad of frivolous lawsuits.

A far more prevalent problem with legislation such as GDPR stems perhaps from the knowledge people actually have about their rights. The Fundamental Rights Surveys report "Your rights matter: Data protection and privacy" conducted by the FRA64 and published on June 18th 2020 shows that 69% of the 35 000 people over 16 surveyed, know about the GDPR.65 Pertaining to question on awareness of who their data protection authority is, 71% answered that they are aware.66 Pertaining to a concrete right, such as the right to access personal data private companies have on them, only 51% of those surveyed stated that they are aware of this right.67 It should be noted that awareness does vary from country to country.68 The report does however show, that even though a majority is aware of the GDPR, which is understandable bearing the focus the Regulation has received publicly in mind, a smaller portion of those subject to the rights of the Regulation have even surface knowledge pertaining to the specific rights, which is alarming. It should be noted that the report is a few years old and not all the rights stemming from the GDPR were surveyed.

63 As we have stated, we have seen little to none private enforcement under the Regulation.
64 European Union Agency for Fundamental Rights.
65 FRA (2020) p. 1 and 12
66 Ibid. p. 14
67 Ibid. p. 12
68 Ibid. p. 14
As we have concluded under section 2.2.2, the type of law being enforced factors in when deciding optimal enforcement approach. With the abovementioned information in mind, we can therefore see why exclusive private enforcement of the GDPR would perhaps not be optimal. If the subjects of rights do not possess the information about the specifics of their rights, they probably don’t possess any knowledge of potential litigable infringements either. Without possession of such knowledge, the private enforcement mechanisms become irrelevant because they are not used, and the objectives of the law don’t get fulfilled because of lack of enforcement. That is not to say that private enforcement under the GDPR isn’t suitable; in cases where the private party is well aware of their rights and potential infringements, private enforcement certainly is a valid option. The point is that the GDPR shows that pertaining to legislation of its caliber, bearing in mind its objectives and complexities\(^69\), a mix of private and public enforcement is perhaps preferable. But how has this mix functioned in reality? Has the enforcement been effective? When we account for such small prevalence of private enforcement, this question would have to be answered by looking at GDPRs public enforcement mechanisms.

Some have claimed that GDPR has been a success.\(^70\) Others have however declared the opposite, stating that GDPR is still presenting challenges, some citing compliance as the main challenge.\(^71\) Others again are attacking the effectiveness of the GDPR public enforcement mechanisms.\(^72\) Compliance and complexity issues aside, we will now look at some possible problems the GDPR public enforcement has shown.

Vergnolle states that the problems with the GDPR enforcement are attributed to different factors; some blame the underfunding and understaffing of the DPAs, some GDPRs vague language, while most agree on one thing, “the "one-stop-shop" mechanism instituted by the GDPR is ineffective or, at least, broken”.\(^73\) Vergnolle further states that the “past years have unveiled this mechanism as a slow and inefficient system, which even the European Commission recognized in 2020”.\(^74\) Indeed the Commission accepts that further progress is essential towards making the handling of cross-border cases more efficient.\(^75\) For the purpose of understanding the potential problems of “the one-stop-shop” mechanism, we will briefly address what it entails before we look at the problems.

\(^{69}\) GDPR is undoubtedly a complex legislation, being an 88 page law with complex language.
\(^{70}\) European Commission (2020).
\(^{71}\) Smith (2021).
\(^{72}\) Vergnolle (2022) p. 103.
\(^{73}\) Ibid.
\(^{74}\) Ibid.
\(^{75}\) COM/2020/264 p. 5.
The “one-stop-shop” mechanism entails that the competent DPA for addressing concerns connected to processing of personal data across the borders of Union Member States is the DPA of the Member State where the controllers/processors have their main establishment. Furthermore, if the controller/processor processes data to fulfill an obligation under the national law of a Member State, “only the DPA of that EU Member State is competent”. The Commission has earlier regarded the mechanism as a means of ensuring cooperation between the DPAs in the case of cross-border processing. The mechanism may at first glance seem as a neat measure for ensuring serene enforcement, in so far as each DPA having their delimited area of competence, so what exactly has proven to be a problem?

Vergnolle writes that the one-stop-mechanism has “proven to induce delays in procedure and widespread frustration” also showing “that the inactivity of one single authority can act as a bottleneck and put at risk the rights of all data subjects across Europe”. Vergnolle's argumentation is founded in the fines which have been imposed as a result of non-compliance with the GDPR as of late August 2021: the 760 fines which had been imposed, are unevenly spread across the Union. One of the main concerns with this is that the Irish DPA has issued very few fines, whilst Ireland in fact is the country where most Big-Tech companies have their main establishment. Furthermore, “most of the high-profile cases include cross-border processing of personal data, triggering application of the one-stop-shop.” As of Vergnolles assessment, the Irish DPA had backlog of 28 cases against Big Tech firms under investigation. Vergnolle presents an illustrative case regarding the difficulties of the GDPR enforcement:

“When Facebook purchased WhatsApp in 2014, it assured nothing would change for its user’s privacy. However, in 2016, WhatsApp announced 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 before the entering into force of the GDPR. Since then, the Irish DPC has been the lead

---

76 European Commission (a)
77 Vergnolle (2022) p. 105.
78 Ibid. p. 104.
79 Ibid. - less than 10 fines issued since 2018.
80 Ibid. see also Gain (2023), an article published by Gain in siliconerepublic states that “the Irish DPC holds a special place in GDPR regulation and enforcement in the EU by virtue of the fact that many global tech giants, including Meta, Google and Apple, have their European headquarters here. This gives it the right to oversee most GDPR violation cases in the continent.”
81 Vergnolle (2022) p. 104, see also Gain (2023), the Irish DPA has handed out fines of more than €1bn in 2022. This may signal a more effective enforcement, but the article doesn’t mention how many of these cases were against Big-Tech companies.
83 WhatsApp Blog (2016).
84 Ross (2018).
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, 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, 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, unable to take matters into its own hands.”

What we can conclude is that GDPR public enforcement has turned out to be rather delayable and somewhat ineffective at tackling the Big-Tech companies because of its “one-stop-shop” mechanism. As Vergnolle writes, “[o]riginally 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” adding that “[i]t 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.” Alongside complexity in comprehension of the Regulations obligations possibly hindering the prevalence of private enforcement, these are the issues we will bear in mind in discussions on enforcement of the DMA and DSA. Before we move on to other relevant legislation, we will however quickly look at how the issue of one-stop-shop is being addressed.

Besides the Court of Justice decision clarifying that other DPAs than that of the country of main establishment may initiate legal proceedings before their own countries courts against a company, the Commission has signaled that it may propose a new law that will “attempt to significantly improve cooperation between different EU member states on privacy regulation and the GDPR” which may affect the Irish DPA. Even more interestingly however, especially pertaining to this particular thesis, is the apparent rise in private enforcement of the GDPR, inter

---

85 Grably (2021).
86 EDPB Urgent Binding Decision 01/2021
89 Ibid. p. 105.
90 Case C-645/19.
91 Vergnolle (2022) p. 105.
92 Gain (2023).
alia, in Germany. An article by Noerr\textsuperscript{93} states that “claims for damages for data privacy breaches were rarely enforced in the past” in Germany, but that new “[r]ulings awarding sums of damages of up to €5,000 per claim have encouraged more and more people to seek damages following data privacy breaches.” The article outlines that the German courts have submitted several questions to the CJEU, in hope of clarifying the unresolved issues about “non-material damage” which could potentially “kick of a mass filling of claims for damages for data privacy breaches.”\textsuperscript{94} The article deals specifically with private enforcement problems pertaining to the ambiguity of “non-material damages”. Public enforcement issues aren’t mentioned as a causal factor for this rise. This development is however quite interesting and possibly positive for the overall enforcement, in so far as it doesn’t lead to excessive litigation. It should be noted that it is hard to distinguish the effect of such enforcement on the Big-Tech companies, bearing in mind the sizes of the documented rewards. The article does however further state:

“Legal services providers have also caught wind of a lucrative new business model. Data privacy breaches often affect a large number of people equally. Since courts are now already awarding four-figure sums to individuals for fairly minor infringements, the players in an increasingly professionalized claimant industry hope to be able to file very large collective claims for damages. Legal services providers hope to build on their experience in other class actions such as cartel damages, the diesel emissions issue or the “cancellation argument” in consumer loan agreements. They are currently trying to litigate individual cases and obtain decisions in their favor from the highest German courts. The new class action models make the risk to companies even greater.”

The abovementioned point of view is very interesting pertaining to efficient enforcement. A fundamental breach of the GDPR affecting numerous plaintiffs in a class action lawsuit could have a devastating effect on the infringers. We will certainly play with this point of view in our discussions on the enforcement of the DMA and DSA, also revisiting it under Section 2.4.4 about U.S. legislation of interest, bearing in mind that it has yet to be proven.

\textbf{2.4.2 EU Competition Law}

EU competition law is primarily formulated in TFEU\textsuperscript{95}, Part Three, Title VII, Chapter 1. Art. 101 (1) under this chapter prohibits all agreements between undertakings, decisions by associations of undertakings and concreted practices which have as their object or effect the prevention, restriction or distortion of competition within the internal market. Art. 101 (3) states that such prohibition may be declared inapplicable in certain cases. Art. 102 (1) prohibits any abuse

\textsuperscript{93} Pan-European law firm.

\textsuperscript{94} Rücker (2022).

\textsuperscript{95} Treaty on the Functioning of the European Union.
by one or more undertakings of a dominant position. The provisions bear a striking resemblance to those of Art. 53 and 54 of the EEA Agreement\(^\text{96}\), meaning that EU Competition Law certainly has EEA relevance and applies in countries such as Norway, Iceland and Liechtenstein.

Private enforcement under the EU Competition Law has not always been a given; prior to 2001, no judgement from the Court of Justice stated that Member States have an obligation to rule on civil remedies in case of EU Competition Law infringements.\(^\text{97}\) The first clarification came in Court of Justices judgement in *Courage Ltd /v Crehan*\(^\text{98}\) in 2001 where the court stated the following with the respect to right to damages:

\begin{quote}
"(26) The full effectiveness of Article 85 [now 101] of the Treaty and, in particular, the practical effect of the prohibition laid down in Article 85(1) would be put at risk if it were not open to any individual to claim damages for loss caused to him by a contract or by conduct liable to restrict or distort competition.

(27) Indeed, the existence of such a right strengthens the working of the Community competition rules and discourages agreements or practices, which are frequently covert, which are liable to restrict or distort competition. From that point of view, actions for damages before the national courts can make a significant contribution to the maintenance of effective competition in the Community."
\end{quote}

The opinion was later reiterated in *Manfredi*\(^\text{99}\) in 2006:

\begin{quote}
"(61) It follows that any individual can claim compensation for the harm suffered where there is a causal relationship between that harm and an agreement or practice prohibited under [Art. 101]."
\end{quote}

Commission Notice from 2004 on the handling of complaints by the Commission under Articles 81 and 82 of the EC Treaty\(^\text{100}\) further stated that "[d]epending on the nature of the complaint, a complainant may bring his complaint either to a national court or to a competition authority that acts as a public enforcer" pursuant to Art. 7, cementing use of private enforcement as a means to enforce EU Competition Law.\(^\text{101}\)

---

\(^\text{96}\) Agreement on the European Economic Area.

\(^\text{97}\) Whish (2021) p. 313.


\(^\text{100}\) Treaty establishing the European Community.

\(^\text{101}\) Commission Notice 2004/C 101/05.
Despite the option of private enforcement under EU Competition Law, viability and effectiveness of such enforcement have been questionable. In the *Impact Assessment*\(^{102}\) published together with *Damages actions for breach of the EC Antitrust Rules*\(^{103}\) in 2008, the Commission stated that "the total amount of compensation […] that victims of antitrust infringements are currently forgoing ranges from approximately €5.7 billion […] to €23.3 billion […] each year across the EU" due to "the current ineffective legal framework in Europe".\(^{104}\) Implementation of the Damages Directive\(^{105}\) in 2014 was meant to remedy this problem by reaffirming "the *acquis communautaire*\(^{106}\) on the right to compensation for harm caused by infringements of Union competition law, particularly regarding standing and the definition of damage, as stated in the case law of the Court of Justice, [though] not [pre-empting] any further development thereof."\(^{107}\)

The implementation of The Damages Directive in 2014, can be viewed as a steppingstone towards fixing the issues reported on in the *Impact Assessment*. The Damages Directive "sets out certain rules necessary to ensure that anyone who has suffered harm caused by an infringement of competition law by an undertaking or by an association of undertakings can effectively exercise the right to claim full compensation for that harm" pursuant to Art. 1 (1), infringement of competition law being "an infringement of Article 101 or 102 TFEU" pursuant to Art. 2 (1) and full compensation being the amount that "place[s] a person who has suffered harm in the position in which that person would have been, had the infringement of competition law not been committed" pursuant to Art. 3 (2).

Regulation 1/2003 is today the backbone of Competition Law enforcement within the EU, regulating the application of Art. 101 and 102 (previously Art. 81 and 82 EC). The Regulation tackles both private and public enforcement. Pursuant to Art. 4, the Commission shall have powers under the Regulation. These include decision making powers pursuant to Chapter III of the Regulation as well as investigative powers and powers to impose penalties pursuant to Chapter V and VI respectively. Art. 6 on the other hand states that "[n]ational courts shall have the power to apply Articles [101] and [102] of the Treaty."

\(^{102}\) SWD/2013/0203.

\(^{103}\) COM/2008/165.

\(^{104}\) SWD/2013/0203 p. 23.

\(^{105}\) Directive 2014/104/EU.

\(^{106}\) See EurWork (2007) *Acquis communautaire* is a French term referring to the cumulative body of European Community laws, comprising the EC's objectives, substantive rules, policies and, in particular, the primary and secondary legislation and case law – all of which form part of the legal order of the European Union (EU). […] All Member States are bound to comply with the *acquis communautaire*.

\(^{107}\) Directive 2014/104/EU Preamble (12).
Private enforcement pursuant to Regulation 1/2003 happens before national courts. The choice of which national court is the correct court is decided by the Brussels Regulation. Art. 4 of the Brussels Regulation states that "persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State." Exception to this basic rule can be found in Art. 7 (2) which states that "in matters relating to tort, delict or quasi-delict, [a person domiciled in a Member State may be sued] in the courts for the place where the harmful event occurred and may occurred." There are several other Competition Law related exceptions provided by the Brussels Regulation, but the general point is that claimants in such cases may have a choice when it comes to most suitable court for their litigation.

Regulation 1/2003 is meant to establish cooperation between national courts and the Commission, which is well outlined in Art. 15 on cooperation with national courts and Art. 16 on uniform application of EU competition law. It should be noted here that the Commissions decisions outrank those of the national courts pursuant to Art. 16, making them legally binding in any following subsequent case, differing from the GDPR where a court may decide on damages whilst deviating from the findings of a decision struck by other competent authorities. Of importance, however, is examining the efficiency of enforcement under EU Competition Law which we shall do by looking at concrete case law.

As we have stated under Section 2.2.2 of this thesis, Podszun dismisses the "common theme" of ineffectiveness of private enforcement due to the David-Goliath ratio between claimants and Big-Tech companies. The bulwark of his argumentation takes basis in three competition law cases from Germany which he analyses: cases Netdoktor/Google, Amazon and Immoscout. In to following we will take a look at Podszuns analysis.

In the Netdoktor/Google and German Federal Ministry of Health case, the private health portal Netdoktor filed for an injunction against Google and the Ministry to stop their cooperation. The cooperation involved Google prominently displaying information from the Ministry's National Health Portal in a "Knowledge Panel" on its search page when users searched for health-related information. Netdoktor feared a drop in its advertising revenue due to the privileged display of information from the state-run portal.

---

108 Regulation 1215/2012.
109 Whish (2021) p. 324
110 LG München I, 10/02/2021–37 O 15721/20
111 Podszun (2021)(a) p. 2-6.
112 Ibid. p. 2-3.
The court granted the injunction based on Article 101 TFEU, stating that the Ministry acted as an undertaking in competition with private health portals. The court also identified a restriction of competition due to the exclusive reservation of a top spot in Google searches for the Ministry.\(^\text{113}\) The court did not find any efficiencies under Article 101(3) TFEU.

The judgment was a success for Netdoktor, and neither Google nor the Ministry appealed the decision. The case emphasizes "the need for Google to present search results in an undistorted way" and "not [to] privilege individual companies over others."\(^\text{114}\) Podszun writes that the case is notable for several reasons: 1) The court showed independence and made a ruling free from political considerations, 2) the case took less than three months from the complaint to the final decision, 3) the court did not resort to complex economic arguments or calculations, 4) the court applied a "relaxed" standard of proof, acknowledging the urgency of the claim and 5) the court hinted at the integration of media law with competition law, opening a window to adjacent fields of the law, raising questions about Google's role as a content curator and the government's involvement in reducing plurality of opinion.\(^\text{115}\)

In the Amazon—termination of contract case, a Swiss retailer of food additives and beauty products filed a complaint against Amazon for deactivating and terminating their account, deleting their offers, and freezing their funds, citing fake reviews.\(^\text{116}\) The plaintiff claimed they could not fulfil Amazon's remedy package without further clarification on the problematic reviews.

The Munich I District Court first sided with the retailer but later reversed its decision in favour of Amazon.\(^\text{117}\) The court acknowledged Amazon's market dominance but found no abuse in this specific case since the plaintiff was a repeat offender. The court referred to Article 4(5) of Regulation (EU) 2019/1150 (P2B-Regulation) to establish the standards for terminating the provision of online services.

Podszun notes several institutional aspects in this case as worthy: 1) The case demonstrates the "David versus Goliath" situation, with a small company challenging a GAFA-company through the court system, despite the risks and efforts involved, 2) Amazon's willingness to take the case to the German Constitutional Court, a rare step, highlights the company's ability and willingness to mobilize resources, 3) the summary proceedings stand out for their speed and

\(^{113}\) Ibid. p. 3.
\(^{114}\) Ibid.
\(^{115}\) Ibid.
\(^{116}\) Ibid. p. 4.
\(^{117}\) Ibid.
efficiency, allowing for quick decisions and reviews 4) the case lacks references to economics, focusing instead on legal interpretation and precedents 5) the court lowered the standard of proof in accordance with the requirements of a summary proceeding, considering the information asymmetry between the parties, 6) the court integrated the P2B-transparency regulation into antitrust standards, skilfully using the toolkit of digital regulation in a coherent and effective manner.118

The Immoscout—tipping case involved a leading German real estate platform, Immoscout, offering two rebates to customers: a "list-all-rebate" for listing 95% of offers on the platform and a "list-first-rebate" for exclusive listings for the first seven days.119 A competitor filed an application for injunction against these rebates.

The Berlin District Court prohibited the list-first-rebate, while the list-all-rebate was seen as lawful.120 The decision was based on a new provision in German abuse law,121 section 20(3a) of the competition act, which aims to keep markets contestable by preventing undertakings with superior market power from hindering competitors gaining network effects. The court reasoned that the list-first-rebate reduced the availability of fresh offers in the crucial first phase of property marketing, while the list-all-rebate allowed for multi-homing and was unproblematic.

Podszun notes that he case demonstrates the efficient application of a new rule by the court and the remarkable speed of case resolution (two months).122 The court's analysis focused on practical implications rather than economic theory, examining the impact of the rebates on multi-homing and competition between platforms. The case highlights the power of new legislation that remains loyal to competition law principles while addressing potential excesses.

As we can see, these three cases illustrate the power of private enforcement in ensuring fair competition and addressing potential excesses in the digital marketplace. They also demonstrate the ability of courts to decide quickly and efficiently, even in cases involving powerful companies such as Google and Amazon. The courts' focus on practical implications and legal interpretation, rather than economic theory, highlights the importance of adapting competition law to the digital age while remaining loyal to its core principles. The comparison of three cases highlights the effectiveness of private enforcement in competition law. While not making any

118 Ibid. p. 4-5.
119 Ibid. p. 5.
120 Ibid. p. 6.
121 GWB.
122 Podszun (2021)(a) p. 6.
claims about the correctness of the decisions, it is clear that the parties received relatively quick decisions that impacted the market.

In his comparison to public enforcement of competition law, Podszun writes that the Munich I District Court has a remarkable track record when compared to the European Commission's handling of companies like Google and Amazon.\(^{123}\) The Munich court's decisions are short, published quickly, and maintain transparency. Furthermore, there is no evidence of fundamental unfairness towards any of the parties. In contrast, the European Commission took more than six years to conclude the Google Search (Shopping) case, and the remedies have been criticized as ineffective. Publication of decisions can also take years, and the Commission's decisions are much lengthier compared to the Munich courts.

Podszun further states that private enforcement has a different legitimacy than public enforcement. Public agencies enforce the law primarily to pursue the public good, such as protecting competition for wider economic aims.\(^{124}\) Private parties enforce competition law to protect their individual interests in the competitive process. Competition law has a dual nature, protecting both public good and private individual rights. Depending on the enforcement path, one aspect may be in focus over the other. Private enforcement cases often focus on the experiences of the claimants, while public enforcement cases, like the Commission's Google Shopping case, take a broader perspective on markets, structures, and aggregated effects.

Finally, Podszun points out that private enforcement has its limitations: cases are strictly related to the parties involved and have no binding force beyond that.\(^{125}\) Courts are essentially in the hands of the parties, and judges may lack expertise in competition law due to their career paths. If taken to extremes, court cases may take a long time before they are finally decided.

Despite these limitations, private enforcement has proven effective in the three cases analysed by Podszun. The confrontational, formal proceedings at courts appear more effective and no less convincing than similar cases in public enforcement.\(^{126}\) Podszun therefore points out that strengthening private enforcement may lower the bar for finding violations of competition law in general and raise the role of individual harm of competitors and consumers.

\(^{123}\) Ibid.
\(^{124}\) Ibid. p. 7.
\(^{125}\) Ibid.
\(^{126}\) Ibid.
Podszun identifies three main features in his case analysis contributing to the success of private enforcement in competition cases: an attractive legal framework, the interplay of public and private enforcement, and different adjudicating standards.\footnote{Ibid. p. 7-10.}

An attractive legal framework includes a clear competition law basis, a procedural framework that allows for speedy resolution, and the removal of barriers to sue for private parties.\footnote{Ibid. p. 7-9.} German law provides a clear rule in the competition act for bringing infringement proceedings, giving legal certainty to claimants. The procedural framework allows for fast decisions by courts and has the necessary resources and judicial independence. The system also takes precautions against mistakes in fast-track proceedings, with decisions open to appeal and review. To encourage private enforcement, barriers to sue should be considered, such as the financial and informational asymmetry between parties, and efforts should be made to address these barriers.

The interplay of public and private enforcement is crucial for the effectiveness of competition law.\footnote{Ibid. p. 9.} Public enforcement can establish important elements that can be built upon by courts, such as market definition, dominance, and the analysis of business models. Private enforcement, in turn, can contribute to the development of competition law through court decisions, which may serve as precedent or inspiration for agencies and courts in other countries. To maximize this potential, it would be beneficial to create an accessible database of national cases in private litigation. This has already been achieved with EU level judgements and implementing use of better and more capable AI could make this job easy with regard to translation to several different languages.

In private enforcement, adjudicating standards differ from those in public enforcement.\footnote{Ibid.} The standard of proof is set with regard to the effectiveness of the proceedings, taking into account information asymmetries and the possibilities within the chosen forum. This approach contrasts with the evidentiary requirements in Commission proceedings. It may be necessary for the European Court of Justice to scale back these requirements to avoid overburdening the Commission, the affected parties, and the complainants.

The courts in the analysed cases do not rely on complex economic models and instead fulfil the requirements of the law through traditional legal analysis.\footnote{Ibid. p. 9-10.} This approach may prompt
reconsideration of the role of economics in competition law. Lastly, the integration of antitrust law into the broader regulatory framework is essential. The Amazon case demonstrates the interplay of competition law with other areas, such as the P2B-regulation. Judges, who often have a broader legal perspective than competition authorities, may find it less problematic to integrate different legal regimes. Agencies should be more open to other fields of law that intersect with competition rules and coordinate better with other agencies.

Podszuns analysis should be taken for what it is. Three cases from Germany can hardly on their own make an argument that private enforcement is the preferable path in Competition law; Podszun states as much. Podszun however continues by stating that these cases "indicate that private enforcement from time to time manages to solve cases effectively, and that potentially some institutional learnings may be drawn from this." Indeed, as we have seen, the option of private enforcement doesn't eliminate the possibilities of public enforcement. These enforcement approaches can serve as two different avenues both leading both contributing to optimal enforcement of law. Even though Podsuzns analysis isn't broad, we will carry his conclusions and findings over to or discussions on optimal enforcement of the Digital Services Act package.

2.4.3 E-commerce directive

The E-Commerce Directive133 "seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States" pursuant to Art. 1 (1). It is "the foundational legal framework for online services in the EU" and "aims to remove obstacles to cross-border online services."134 The Directive sets out to create a Digital Single Market pursuant to Art. 3 (2). The directive doesn't outline concrete obligations on providers of online services, rather imploring the Member States to do so by approximating certain national provisions on such services pursuant to Art. 1 (2). For instance, the Directive obliges Member States to ensure that a service provider is not liable for illegal information/activity stored on an information society service if the provider has no knowledge of the illegal activity and information and is not aware of circumstances or facts from which the illegal activity/information is apparent pursuant to Art. 14 (1)(a). Such limitations of liability do not however affect the possibility of other injunctions, including the removal of illegal information.135

132 Ibid. p. 13.
133 Directive 2000/31/EC.
134 European Commission (2022)(e).
Even though the Directive doesn't contain its own enforcement mechanisms, one of its four main pillars is promotion of smart regulatory techniques and enforcement.\footnote{Policy Department for Economic, Scientific and Quality of Life Policies (2020) p. 8.} This is evident in the Directives Art. 16 encouraging creation of easily accessible codes of conduct at Community level and Art. 18 on court actions obliging Member States to ensure that court actions are available under national law concerning information society services' to allow for the rapid adoption of measures designed to terminate alleged infringements and prevent further impairment of the interests involved. Art. 20 also obliges Member States to "determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and […] take all measures necessary to ensure that they are enforced." The Directive is therefore rather a call for regulation and subsequent private and public enforcement ensuring compliance. Since the adoption of the Directive, EU has adopted several new rules and enforcement tools pertaining to providers of online platforms.\footnote{Ibid.} The same goes for the Member States, which have adopted measures that online platforms should implement to tackle illegal content in particular.\footnote{Ibid.}

A study requested by the IMCO committee has found that implementation of national laws regarding areas of the E-commerce Directive has led to a situation where these laws "carry serious risk of undermining the completion of the Digital Single Market."\footnote{Ibid.} A concrete example is adoption of variations of ineffective Notice-and-Takedown\footnote{See Directive 2000/31/EC Art. 14.} procedures conducted by only some of the Member States in the Directives implementation stage.\footnote{Policy Department for Economic, Scientific and Quality of Life Policies (2020) p. 31.} Furthermore, "][a]doption or proposals of recent laws in the Member States, in particular regarding hate speech, further increased the risks of Internal Market fragmentation."\footnote{Ibid.} The study gives a specific example:

"[…] Germany adopted the Network Enforcement Act (NetzDG) which requires in particular online platforms with more than two million subscribers in Germany to set up a system for users to complain against hate speech and to remove or block access to within 24 hours from the user's notification; for content that is not obviously illegal, platforms have seven days to remove it or must delegate a self-regulatory body to assess it. In case of repeated incompliance, they face fines up to €50m."\footnote{Ibid.}
In hindsight, the lesson to take from the E-commerce Directive is that broad EU legislation open for interpretation by the Member States in decisions on execution and enforcement, is capable of fragmenting that same legislation. The aforementioned study lists priorities in its assessments of the E-commerce Directive reform, which directly focus on alleviating the fragmentation of the regulatory framework, such as maintaining the Internal Market Clause.\textsuperscript{144} The study goes to state that “cooperation and mutual assistance between Member States […] should be strengthened by providing specific procedures and deadlines.” Moreover, the study goes on, “a separate and more EU-based enforcement mechanism could be foreseen for the systemic platforms when the ability and/or the incentives of the authorities of the Member States where the platform is established are insufficient to guarantee an effective law enforcement”, interesting point bearing in mind the discussions we previously had on the GDPRs ineffective “one-stop-shop”.\textsuperscript{145} A question we however ought to ask ourselves is why it is so important to alleviate fragmentation and thus protect the Digital Single Market.

The global economy is increasingly digital, with Information and Communications Technology (ICT) forming the foundation of modern economic systems.\textsuperscript{146} The Internet and digital technologies are transforming various aspects of our lives, offering vast opportunities for innovation, growth, and jobs. However, these changes also present policy challenges that require a coordinated EU response.

To address these challenges, the European Commission has prioritized creating a Digital Single Market, which ensures the free movement of goods, people, services, and capital.\textsuperscript{147} This market allows individuals and businesses to access and participate in online activities under fair competition and with strong consumer and personal data protection. Achieving this will help Europe maintain its position as a world leader in the digital economy and support the growth of European companies globally.

Currently, fragmentation and barriers within the EU are holding back its potential.\textsuperscript{148} Eliminating these barriers could contribute an additional €415 billion to European GDP. A Digital Single Market can provide new opportunities for startups and help existing companies grow in a market of over 500 million people.

\textsuperscript{144} Ibid. p. 47.
\textsuperscript{145} Ibid.
\textsuperscript{146} COM/2015/192 p. 3.
\textsuperscript{147} Ibid.
\textsuperscript{148} Ibid.
The Digital Single Market Strategy, developed through input and dialogue with various stakeholders, focuses on key interdependent actions that can only be taken at the EU level. The strategy is built on three pillars: better access for consumers and businesses to online goods and services across Europe, creating the right conditions for digital networks and services to flourish, and maximizing the growth potential of the European digital economy through investment in ICT infrastructures and technologies. Each action will undergo consultation and impact assessment, in line with Better Regulation principles.

Coherence in law entails not only application of same material rules, but also same procedural rules of enforcement as well as willingness and ableness to act upon them. As the Commission points out with regard to consumer protection “having a common set of rules is not enough [...] there is also a need for more rapid, agile and consistent enforcement of consumer rules for online and digital purchases to make them fully effective.” The Commission continues with regard to combating of illegal content on the internet, “[d]ifferences in national practices can impede enforcement and undermine confidence in the online world.” Granted, this doesn’t help us in determining whether such enforcement should be private or public, though the argument could be made that idyllic enforcement in this case could be centralised EU public enforcement. This does however introduce a new important dimension to our coming discussions on the DMA the DSA; the importance of harmony in law and enforcement for ensuring a stronger digital market for businesses and consumers alike.

2.4.4 USA Legislation of interest
We have so far looked at legislation of interest regarding Big-Tech and VLOPs within the EU. As far as taming the Big-Tech and protection of fundamental and consumer rights in digital spaces, it should be safe to say that Europe is ahead of the game compared to the USA; the country is after all yet to receive a positive adequacy decision with regard to transfer of personal data to third countries pursuant to GDPR Art. 45. Two bills introduced in 2021 are however notable in our discussions on the Digital Services Act package: The Open App Markets Act and The American Innovation and Choice Online Act. Before discussing these Bills proposed by EUs friend across the Atlantic, it should be noted that they have merely been introduced and are far from Presidential Action in the Legislative Process.

149 Ibid.
150 See European Commission (b).
151 See European Commission (2022(f) – All though an adequacy decision has been drafted, it yet to be adopted.
154 The Legislative process in the USA is complex and often long. Introduction is one of the first steps. Getting to Presidential Action entails among other things a House and Senate vote See i.e. Congress.gov Legislative Process Video.
The Open Market Act bears a resemblance to the DMA. Section 3 of the Act aims to protect a competitive app market. It prohibits covered companies from requiring developers to use specific in-app payment systems or favoring their own app store's terms and conditions. They cannot take punitive action against developers who use different pricing terms on other platforms. Covered companies cannot restrict communication between developers and users or use non-public business information from third-party apps for competition. They must allow users to choose, install, and delete third-party apps or app stores and avoid self-preferencing in search rankings. Access to operating system interfaces and other resources should be provided to developers on equal terms.

Section 4 focuses on user security and privacy. Covered companies are not in violation of Section 3 if their actions are necessary for user privacy, security, digital safety, preventing spam or fraud, protecting intellectual property, or complying with the law. To qualify, the company must consistently apply these actions to their own apps and others, avoid using them as pretexts to exclude third-party apps, and ensure their actions are narrowly tailored and non-discriminatory.

Pursuant to Section 5, the enforcement of this Act falls under the responsibility of the Federal Trade Commission (FTC), the Attorney General, and state attorneys general, following the same procedures and powers as specified in other relevant antitrust laws. If the FTC believes a covered company violated the Act, it can commence a civil action to recover penalties and seek relief. State attorneys general may also file civil actions on behalf of residents for violations of the Act and secure any available relief, in line with the parens patriae Doctrine. Developers who have been infringed by violations of the Act can sue in a U.S. district court, regardless of the amount and potentially recover triple the damages they sustained and the cost of the suit, including attorney's fees. The court may award simple interest on actual damages, considering factors related to the parties' conduct during litigation. Developers can also seek injunctive relief against threatened loss or damage caused by violations of the Act, following the same principles and conditions as courts of equity. If the plaintiff substantially prevails, the court shall award the cost of the suit, including attorney's fees. However, app developers owned or controlled by a foreign state are not allowed to bring an action under this subsection.

The American Innovation and Choice Online Act also resembles the DMA. Section 3 outlines unlawful conduct for covered platform operators, making it illegal to engage in activities that would materially harm competition. Examples include favouring their own products, services, or lines of business over others, limiting the competitive abilities of other businesses, and applying discriminatory terms of service. Additionally, covered platform operators cannot restrict access or interoperability, condition access on purchasing unrelated products or services, or use non-public data to compete with other businesses on the platform. They also cannot impede
access to data generated on the platform or restrict users from uninstalling preinstalled software applications, unless necessary for security or functionality. Favourable treatment in user interfaces, search, or ranking is prohibited, as is retaliation against users who report violations to law enforcement.

Affirmative defences for actions under this section are allowed if the defendant can prove their conduct was narrowly tailored, non-pretextual, and reasonably necessary to comply with the law, protect safety, privacy, data security, or maintain core functionality. In cases where the conduct has not resulted in and would not result in material harm to competition, the defendant may establish an affirmative defence if the conduct meets specific conditions, such as being narrowly tailored, non-pretextual, and reasonably necessary for legal compliance, safety, privacy, data security, or maintaining core functionality.

Section 3 (c) outlines the enforcement mechanisms of the Act, stating that the Federal Trade Commission (FTC), the Attorney General, and state attorneys general will enforce it in the same manner as other relevant acts. The FTC has independent litigation authority to commence a civil action if they believe a person violated the Act. State attorneys general can bring civil actions on behalf of natural persons residing in their state. Enforcement can only occur through civil actions brought before a United States district court.

The remedies provided in this paragraph are additional to any other remedies under federal or state law. Civil penalties for violators can be up to 15% of the total US revenue during the violation period. Injunctions and temporary injunctions can be sought by the Assistant Attorney General, FTC, or state attorneys general, with the court determining whether they are necessary or in the public interest. For repeat offenders, the court may require forfeiture of the CEO's or other corporate officers' compensation.

Even though the primary enforcement approach enshrined in these bills is of public nature, the nature of the law in mind would surely be covered by The Clayton Antitrust Act Section 4 stating that “any person who shall be injured in his business or property by reason of anything forbidden in the antitrust laws may sue therefore in any district court of the United States in the district in which the defendant resides or is found or has an agent, without respect to the amount in controversy, and shall recover threefold the damages by him sustained, and the cost of suit, including a reasonable attorney’s fee.” Furthermore, subject to Clayton Act Section 16 “[a]ny person, firm, corporation, or association shall be entitled to sue for and have injunctive relief, 15 U.S. Code § 15 - Suits by persons injured.

in any court of the United States having jurisdiction over the parties, against threatened loss or damage by a violation of the antitrust laws”.

What this shows is that one of EUs counterparts is willing to address the same issues as EU. In their approach, they do this by opening possibilities for both private and public enforcement. We have no way of concluding how exactly this would play out, as the bills are currently only proposed, so there is little to be gained. A point that this thesis already has addressed however, is that use of class action lawsuits is very much prevalent in the USA, making the option of private enforcement rather less costly for the infringed parties. There is certainly something to gain from this side of the American legal system, and it would seem the EU has concluded as much.

2020 marks the entry into force of the Representative Action Directive (RAD)\textsuperscript{157}, which sets out rules to ensure that representative action mechanisms for the protection of collective interests of consumers are available in all Member States pursuant to Art. 1 (1). Indeed, the EU states that lack of procedural mechanisms for collective actions "diminishes consumers' and businesses' confidence in the internal market and their ability to operate in the internal market."\textsuperscript{158} EUs devotion to making available mechanisms for collective action is furthermore very apparent; Christ writes that "[o]n 27 January 2023, the European Commission launched infringement proceedings against no less than 24 Member States for failing to transpose" the Representative Action Directive.\textsuperscript{159}

There is no conclusive data that points that EUs efforts are meant to reflect the traditions and successes of the American legal system pertaining to class action mechanisms. However, looking towards the American solutions, both proposed and in play, can give us insight in the potential successes and failures of the solutions we have implemented through the DMA/DSA.

2.5 Final thoughts

We have discussed private and public enforcement pertaining to legislation on Big-Tech companies and VLOPs, be that enforcement of competition rules or rules stemming from fundamental rights. By looking at general analyses of effectiveness of both types of enforcement as well as specific legislation, certain things should be noted going into our discussions on enforcement of the Digital Services Act package.

\textsuperscript{157} Directive (EU) 2020/1828.
\textsuperscript{158} Ibid. Preamble (6).
\textsuperscript{159} Christ (2023).
Firstly, private and public enforcement both have their strengths and flaws as outlined in Section 2.3 of this thesis. In choice of enforcement, we should look to the type of law being enforced, the potential harm caused by violations and the available resources for enforcement. Optimal enforcement doesn’t necessarily entail use of only one type of enforcement; optimality can be achieved with viability and harmony of both.

Secondly, even though public enforcement has been more prevalent in the fields of law pertaining to Big-Tech companies, such enforcement has often been slow and costly. There has in turn been a rise in private enforcement, in some cases showing greater procedural success.

Thirdly, there are examples of legislative proposals outside of the EU pertaining to similar issues of those covered by the Digital Services Act Package opening possibilities for both public and private enforcement. On the other hand, an outright dismissal of private enforcement of past EU legislation is hardly supported by any research.

Finally, in discussions on enforcement of The Digital Services Act package, we should always bear in mind the positive effects of the Digital Single Market. Fragmentation of the law could deter these positive effects in turn leading to distortions in the market as well as inequity in enforcement of fundamental rights of EU citizens depending on their Member State.
3 Enforcement of the Digital Services Act Package

3.1 Introduction
In this chapter we will briefly take a look at the DMA and the DSA. The chapter will focus on the objectives, subject matter, scope, definitions, obligations and the enforcement approach of the regulations. The chapter will not look at all the obligations the regulations impose in depth. Some of the obligations will however be processed more so than others, with the goal of achieving adequate familiarity, making the later discussions on enforcement easier to comprehend.

3.2 The DMA
3.2.1 General Information and Objectives
The Digital Markets Act was proposed to combat the negative consequences of the largest online platforms controlling most of the digital market. The DMA was proposed by the Commission in 2020 and agreed by the European Parliament and the Council in March 2022, with the rules starting to apply in May 2023 and the application of obligations first starting in March 2024.\textsuperscript{160}

The objectives and envisioned benefits of the DMA have been stated under Section 1.2. The DMA will undoubtedly change the landscape of EUs digital market as the Executive President of the European Commission Margrethe Vestager has stated:

\begin{quote}
“The DMA will change the digital landscape profoundly. With it, the EU is taking a proactive approach to ensuring fair, transparent, and contestable digital markets. A small number of large companies hold significant market power in their hands. Gatekeepers enjoying an entrenched position in digital markets will have to show that they are competing fairly.”\textsuperscript{161}
\end{quote}

3.2.2 Subject matter, scope and definitions
The DMA lays down harmonized rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present pursuant to DMA Art. 1 (1). Gatekeeper means a provider of core platform service, core platform services being online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services and advertising services pursuant to Art. 2 (1) and (2). Gatekeeper platforms are in other words “digital platforms with a systemic role in the internal market that function as

\textsuperscript{160} European Commission (2022)(g).
\textsuperscript{161} Kent (2023).
bottlenecks between businesses and consumers for important digital services.” The Regulation "shall apply to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service" pursuant to Art 1 (2). An end user is defined as "any natural or legal person using core platform services other than as a business user" pursuant to Art. 2 (20), whilst a business user is defined as "any natural or legal person acting in commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users" pursuant to Art. 2 (21).

A provider of core platform services shall be designated as gatekeeper if a) "it has a significant impact on the internal market", b) "it operates a core platform service which serves as an important gateway for business users to reach end users", and c) "it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future" pursuant to Art. 3 (1). A provider of core platform services shall be presumed to satisfy the requirement in Art. 3 (1)(a) where the undertaking to which it belongs "achieves an annual EEA turnover equal to or above 7.5 billion in the last three financial years, or where the average market capitalization or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 75 billion in the last financial year, and it provides a core platform service in at least three Member States" pursuant to Art 3 (2)(a). Furthermore, a provider shall be presumed to satisfy the requirement in Art. 3 (1)(b) "where it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year" pursuant to Art 3 (2)(b). Lastly, a provider shall be presumed to satisfy the requirement in Art. 3 (1)(c) "where the thresholds in [Art. 3 (2)](b) were met in each of the last three financial years" pursuant to Art. 3 (2)(c). Designation of gatekeepers falls within the power of the Commission pursuant to Art. 3 (4) of the regulation.

3.2.3 The obligations

The goal of the regulation being to secure a contestable and fair market by evening out the scale between the largest providers of core platform services and the SMEs, requires material rules capable of ensuring it. DMAs approach is regulating the practices of gatekeepers that limit contestability or are unfair, which it does in Chapter III.

Pursuant to Art. 8 (1) of the regulation, "the gatekeeper shall ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7" of the regulation ensuring "that the implementation of those measures comply with applicable law" in particular the GDPR,

---

162 European Commission (2023)(a).
Directive on privacy and electronic communications\textsuperscript{163}, legislation on cyber security, consumer protection, product safety and accessibility requirements. The DMA in so far not only imposes a new set of rules for the Big-Tech, but also reiterates older legislation that must be respected under the implementation of the measures prescribed under the regulation. This is understandable seeing that the obligations pursuant to Article 5, 6 and 7 without a doubt could present problems pertaining to protection of personal data, consumers and cyber security.

The obligations under the DMA cover a wide range of measures, some pertaining to cessation of gatekeeper practices such as the obligations pursuant to Art. 5 (2)(c) obliging gatekeepers to not cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper including other core platform services, and vice versa or Art. 5 (3) stating that gatekeepers shall not prevent business users from offering the same products or services to end users through third-party online intermediation services or through their own direct online sales channel at prices or conditions that are different from those offered through online intermediation services of the gatekeeper. Prohibitions are not unfamiliar in legislation pertaining to Big-Tech.\textsuperscript{164}

Other provisions pertain to measures gatekeepers must implement and allow. Such an obligation can be found in Art. 6 (3)(1) stating that gatekeepers shall allow and technically enable end users to easily un-install any software application on the operating system of the gatekeeper. Further we have the obligation pursuant to Art. 6 (4)(1) stating that gatekeepers shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of the gatekeeper. These types of measures have been heavily discussed during the past few years, often deemed too risky by providers of services with regard to cyber security, a notable example being the calls for option of installation of the Google App Store on the iPhone, where Apple has reiterated their response in connection to proposal of new rules such as the DMA and the DSA, stating that the proposed changes would turn iOS, Apples operative system, into an "Android clone".\textsuperscript{165} It should however be noted that the DMA in fact takes the views of potential gatekeepers such as Apple into consideration, by for instance stating in Art. 6 (4) that gatekeepers shall not be prevented from taking, to the extent that they are strictly necessary and proportionate, 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 are duly justified by the gatekeeper.

\textsuperscript{163} Directive 2002/58/EC.
\textsuperscript{164} See TFEU Art. 102 see also GDPR Art. 6.
\textsuperscript{165} Emmanuel (2023).
Interoperability of number-independent interpersonal communication services is another example of an obligation demanding that the gatekeepers implement measures which allow certain practices, in this case interoperability between the systems of the gatekeeper and those of a third party pertaining to basic functionalities in communication cf. Art. 7. The provision obliges the gatekeepers to make basic functionalities such as end-to-end text messaging between two users cf. Art. 7 (2)(a)(i) or end-to-end voice calls between two individual users cf. Art. 7 (2)(c)(i) interoperable with the services of another provider, providing that the gatekeeper itself provides those functionalities to its own end users. A good example is end users being able to conduct calls between two people using two different social media platforms like Instagram and Snapchat, both of whom provide the function on their own.\(^{166}\)

DMAs obligations are diverse and far reaching and reading them certainly emphasizes Commission signals; unfair practices are indeed practices-non-grata or the main enemy in layman's terms. We will revisit these obligations in discussions of possibility, viability and effectiveness of private enforcement under the DMA in section 3.4 of this thesis.

3.2.4 Enforcement approach

The enforcement approach of the DMA is centralized. Pursuant to Art. 1 (5) of the Regulation, Member States shall not impose further obligations on gatekeepers by way of laws, regulations or administrative measures for the purpose of ensuring contestable and fair markets in order to avoid fragmentation of the internal market. Furthermore, pursuant to Art. 1 (7), national authorities shall not take decisions which run counter to a decision adopted by the Commission under the Regulation. The Commission is solely empowered to designate gatekeepers pursuant to Art. 3. The Commission is also solely empowered to open Market investigations pursuant to Chapter IV as well as given the sole power to investigate, enforce and monitor pursuant to Chapter V, based solely off the legislative text, begging the question of whether private enforcement of the DMA at all is possible as well as putting the powers of the Member States in question. We will return to these questions under Section 3.4 of this thesis.

\(^{166}\) Snapchat and Instagram are ideal examples as number-independent interpersonal communication services are communication services which do not connect with publicly assigned numbering resources, that being numbers or international numbering plans, and do not enable communication with numbers in national or international numbering plans \textit{see} Directive (EU) 2018/1972 Art. 2 (7).
3.3 The DSA

3.3.1 General Information and Objectives
The Digital Services Act was proposed as a means to “create a safer digital space where the fundamental rights of users are protected”. The Regulation was proposed by the Commission in 2020, entered into force November 2022 and will apply for all regulated entities on 17 April 2024.

The objectives of the DSA have also been stated under Section 1.2 of this thesis. The DSA will ensure a higher protection of fundamental rights online, its focus being a safe digital environment for all Union citizens. Executive President of the European Commission Margrethe Vestager has stated the following on twitter: "The Digital Services Act will make sure that what is illegal offline is also seen [and] dealt with as illegal online – not as a slogan, as reality! And always protecting freedom of expression!" This is also reflected in the preamble: "In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of "illegal content" should broadly reflect the existing rules in the offline environment.”

3.3.2 Subject matter, scope and definitions
The DSA aims to contribute to "the proper functioning of the internal market for intermediary services by setting out harmonized rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected" pursuant to Art. 1 (1), intermediary services being one of the following information society services: I) “a ‘mere conduit’ service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network”, II) “a ‘caching’ service consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients upon their request” or III) “a ‘hosting’ service, consisting of the storage of information provided by, and at the request of, a recipient of the service” pursuant to Art 3 (g). In particular, the regulation establishes, a) “a framework for the conditional exemption from liability of providers of intermediary services”, b) “rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services” and c) “rules on the implementation and enforcement of [the] Regulation, including as

---

168 Regulation 2022/2065 Preamble (12).
169 Charter of Fundamental Rights of the European Union.
regards to cooperation and coordination between the competent national authorities” pursuant to Art. 1 (2).

The DSA applies to all “intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment” pursuant to Art 2 (1). This thesis will however focus on DSAa impact on VLOPs which pursuant to the Regulation are "online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million and which are designated as very large online platforms pursuant to paragraph" pursuant to Art. 33 (1). These platforms must follow additional obligations pursuant to the Regulation, which we will discuss under the following subsection. Even though the criterions for designating a VLOP pursuant to the DSA differ from those for designating a gatekeeper pursuant to the DMA, the reasoning follows the same lines; they are the biggest actors in the digital market. In case of DSA, it is argued that VLOPs "may cause societal risks, different in scope and impact from those caused by the smaller platforms" and they "should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact". It should here be noted that it isn't given that a VLOP is a gatekeeper, seeing that VLOPs also can be SMEs. Their influence is however notable, and they are therefore also the subject of this thesis alongside the Big-Tech enterprises operating digital services.

3.3.3 The obligations

The obligations under the DSA are largely sorted into regulations third chapter on due diligence obligations for a transparent and safe online environment. The chapter is divided in several sections: 1) provisions applicable to all providers of intermediary services, 2) additional provisions applicable to providers of hosting services, including online platforms, 3) additional provisions applicable to providers of online platforms, 4) additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders, 5) additional obligations for providers of very large online platforms and of very large online search engines to manage risks and 6) other provisions concerning due diligence obligations. As it stands, all sections of Chapter III are applicable to VLOPs, and will therefore be briefly discussed.

Section 1 of Chapter III includes obligations applicable to all providers of intermediary services. Of interest is Art. 13 stating that "[p]roviders of intermediary service shall include information on any restriction that they impose in relation to the use of the service in respect of information provided by recipients of the service in terms and conditions" pursuant to paragraph 1 following

---

170 Regulation 2022/2065 Preamble (76).
up with "[p]roviders of very large online platforms and very large online search engines shall provide recipients of services with a concise, easily-accessible and machine readable summary of the terms and conditions, including the available remedies and redress mechanisms" and "shall provide their terms and conditions in the official languages of all the Member States in which they offer their services" pursuant to paragraphs 5 and 6.

Section 2 of Chapter III includes additional provisions applicable to providers of hosting services, including online platforms. Of interest is Art. 16 which states that "[p]roviders of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content" cf. paragraph 1 following up with "provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the possibilities for redress in respect of that decision" pursuant to paragraph 5.

Section 3 of Chapter III includes additional provisions to providers of online platforms. It should be noted that micro and small enterprises are excluded these obligations pursuant to Art. 19. The reasoning behind this is to "avoid disproportionate burdens". The section does however apply to providers of online platforms that have been designated as very large online platforms pursuant to Art. 33 of the regulation pursuant to Art. 19 (2) whether they qualify as micro or small enterprise or not because "very large online platforms or very large online search engines have a larger reach and a greater impact in influencing how recipients of the service obtain information and communicate online." In the following paragraph we will look at some obligations of interest.

Pursuant to Art. 20 under Section 3 of the Regulation, "[p]roviders of online platforms shall provide recipients of the service […] with access to an effective internal complaint-handling system that enables them to lodge complaint […] against the decision taken by the provider of the online platform upon the receipt of a notice or against […] decisions taken by the provider […] on the grounds that the information provided by the recipient constitutes illegal content or is incompatible with its terms and conditions." Recipients "shall be entitled to select any out-of-court dispute settlement body that has been certified in accordance with [Art. 21 (3)]" pursuant to Art. 21 (1). Pursuant to Art. 22 "[p]roviders of online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers […] are given priority and are processed and decided upon" pursuant to paragraph 1, the status of "trusted flagger" being awarded to applicant with a) "a particular expertise and competence for

171 Ibid. Preamble (57).
172 Ibid.
the purpose of detecting, identifying and notifying illegal content", b) "is independent from any provider of online platforms" and c) "carries out its activities for the purposes of submitting notices diligently, accurately and objectively" pursuant to paragraph 2. Pursuant to Art. 23 (1) "[p]roviders of online platforms shall suspend, for a reasonable amount of time […] the provisions of their services to recipients of the service that frequently provide manifestly illegal content. Pursuant to Art. 25 (1) "[p]roviders of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipient of their service to make free and informed decisions." Pursuant to Art. 26 (3) "[p]roviders of online platforms shall not present advertisements to recipients of the service based on profiling as defined" under the GDPR "using special categories of personal data referred to" in the GDPR. Finally, pursuant to Art. 28 (2) "[p]roviders of online platform shall not present advertisements on their interface based on profiling as defined" under the GDPR "using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is minor."

Section 4 of Chapter 3 includes additional provisions applicable to providers of online platforms allowing consumers to conclude distance contracts with traders. As with section 3, the section does not apply to micro and small enterprises pursuant to Art. 29 (1). The section does apply to very large online platforms pursuant to Art 29 (2). The reasoning behind this is the same as the one under section 3.173 Of interest, Art. 30 (1) states that "[p]roviders of online platforms allowing consumers to conclude distance contracts with traders shall ensure that traders can only use those online platforms to promote messages on or to offer products or services to consumers located in the union if" they previously have obtained information about the consumer. Further, pursuant to Art. 31 (1), "[p]roviders of online platforms allowing consumers to conclude distance contracts with traders shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding precontractual information, compliance and product safety under applicable Union law." Finally. Pursuant to Art. 32 (1), the provider shall inform consumers who have purchased an illegal product or a service about the fact that the product or service is illegal, the identity of the trader and any relevant means of redress, if the provider finds out that a trader is offering illegal products/services to consumers within the Union.

Section 5 of Chapter 3 includes additional obligations for providers of very large online platforms and of very large online search engines to manage systemic risks. Obligations include in-depth rules on risk assessment pursuant to Art. 34, mitigation of risks pursuant to Art. 35, crisis

173 Ibid.
response mechanisms pursuant to Art 36, additional online advertising transparency pursuant to Art 39 and data access and scrutiny pursuant to Art 40.

Section 6 of Chapter 3 includes other provisions concerning due diligence obligations. The obligations under this section largely tackle standards and codes of conducts imposed by the Commission and the Board, which have little to do with private enforcement and are therefore not of interest for this dissertation.

DSAs obligations are many and at times very specific. The preamble states that "[i]n order to achieve the objectives of this Regulation, and in particular to improve the functioning of the internal market and ensure a safe and transparent online environment, it is necessary to establish a clear, effective, predictable and balanced set of harmonised due diligence obligations for providers of intermediary services." The viability and effectiveness of private enforcement pertaining to these obligations will be further discussed under Section 3.3 of this thesis.

3.3.4 Enforcement approach
The enforcement approach of the DSA is very much the exact opposite of the DMA. Whereas DMA seemingly gives the power to enforce solely to the Commission, the DSAs enforcement approach is far more Member State based. This is very well reflected in chapter IV of the Regulation on implementation, cooperation, penalties and enforcement. For instance, Art. 49 (1) states that Member States shall designate one or more competent authorities to be responsible for the supervision of providers of intermediary services and enforcement of this Regulation ("competent authorities"). These competent authorities have enforcement powers pursuant to Art. 51 (2). It is further stated under Art. 56 (1) that the Member State in which the main establishment of the provider of intermediary services is located shall have exclusive powers to supervise and enforce this Regulation. This does however exclude enforcement of Section 5 of Chapter III on additional obligations for VLOPs and very large online search engines to manage systemic risks pursuant to Art. 56 (2), as well as the power to enforce other obligations pertaining to VLOPs pursuant to Art 56 (3). This will be the topic of discussion under section 3.4.2 and onward of this thesis.

\[174\] European Board for Digital Services.
3.4 Enforcement under DMA and DSA

3.4.1 Is private enforcement under the DMA possible?

3.4.1.1 The preparatory work and Commission signals
Looking at the preparatory work of the DMA, it is unclear whether the intention with the Regulation is to allow private enforcement pertaining to its obligations. Preamble paragraph 6 states that the Regulation "aims to complement the enforcement of competition law" further stating that the Regulation therefore should apply without prejudice to corresponding national rules and Art. 101 and 102 of the TEFU, but that "application of those rules should not affect the obligations imposed on gatekeepers under [the] Regulation and their uniform and effective application in the internal market." The goal of the Regulation, as we will see under the discussions of the legislative text under section 3.3.1.2 of this thesis, is to work in harmony with those rules already present in EU and national competition law but also other rules which the Regulation touches upon, like those of the GDPR. The preamble states as much in paragraph 37 (2), "The regulation is without prejudice to Regulation (EU) 2016/679, including its enforcement framework, which remains fully applicable with respect to any claims by data subjects relating to and infringement of their rights under that Regulation” as well as Art. 5 (2)(3).

The preamble further on goes to state in paragraph 80 that the Commission "should have strong investigative and enforcement powers, to allow it to investigate, enforce and monitor the rules laid down in [the] Regulation" in order to ensure effective implementation and compliance with the Regulation. The paragraph doesn’t mention national courts or authorities, however paragraph 86 states that "[t]he Commission, and the relevant national authorities should coordinate their enforcement efforts" pertaining to fining of illegal activity in accordance with the principles of ne bis in idem\textsuperscript{175} and proportionality. It should be noted that paragraph 86 emphasizes that respect of these principles is prevalent where national authorities have imposed penalties relating to an infringement of other Union or national rules. In doing so the paragraph illustrates a legal framework where DMA, other Union law and national law coexist in harmony, rather than joint empowerment of Member States and the Commission pursuant to the Regulation. This is further cemented in paragraph 90 stating that "[t]he coherent, effective and complementary enforcement of available legal instruments applied to gatekeepers requires cooperation and coordination between the Commission and national authorities within the remit of their competences."

Finally, paragraph 90 of the preamble outright states that "[t]he Commission is the sole authority empowered to enforce this Regulation", but that "it should be possible for Member States to

\textsuperscript{175} See Oxford Reference "the right not to be prosecuted or tried twice for the same criminal conduct.”
empower their national competent authorities enforcing competition rules to conduct investigations into possible non-compliance by gatekeepers with certain obligations under [the] Regulation” in order to support the Commission. The curious mind would wonder how this is to be interpreted against paragraph 92 which states that "[in] order to safeguard the harmonized application and enforcement of [the] Regulation, it is important that national authorities, including national courts, have all necessary information to ensure that their decisions do not run counter to a decision adopted by the Commission under [the] Regulation.” One way to interpret this possible collision is that national courts in fact are empowered to enforce the Regulation. Another, and semantically more correct way to interpret this, is that national courts in application of rules stemming from other Union and national law, must bear in mind Commissions application of the DMA, so as to not rule in favor of decisions which might run counter to decisions made by the Commission under the DMA.

The uncertainty pertaining to possibilities of private enforcement under the DMA stems in part from the utter lack of mention of such enforcement in its preamble. The preamble on the other hand mention rights and obligations vigorously, for instance paragraphs 29, 33 and 54. Paragraph 6 states that "it is necessary to provide in a clear and unambiguous manner [rules] with regard to […] [gatekeepers] services" so as to "safeguard the contestability and fairness of core platform services provided by gatekeepers". Clear and unambiguous obligations, resulting in enforceable rights, yet with no discussion on how the infringed party is supposed to enforce them and preamble statements such as "the Commission is the sole authority empowered to enforce this Regulation".

Looking at the Commissions press releases, one ought to ask oneself; does the Commission itself know whether private enforcement under the DMA is possible? One source on the Commissions website states that "[t]he DMA will be enforced through a robust supervisory architecture, under which the Commission will be the sole enforcer of the rules, in close cooperation with authorities in EU Member States"\(^\text{176}\) whilst another states that "[t]he DMA is a Regulation, containing precise obligations and prohibitions for the gatekeepers in scope, which can be enforced directly in national courts" that same article stating that "[t]he Commission will be the sole enforcer of the rules laid down in the Digital Markets Act."\(^\text{177}\) Which statement is correct, or are all of them correct at the same time? Perhaps the robust supervisory architecture the Commission is solely empowered to enforce pertains to designation of gatekeepers, opening of market investigations and imposing of fines, etc., whilst legal remedies sought by infringed parties can be awarded by national courts. Nonetheless, it cannot be said that the preamble nor

---

\(^\text{176}\) European Commission (2022)(g).

\(^\text{177}\) European Commission (2023)(b).
the Commissions statements give us a clear picture of private enforcement under the Regulation, so let us take a look at the concrete provision.

3.4.1.2 Lack of provisions pertaining to private enforcement in the legislative text

The legislative text of the DMA is without a doubt ambiguous pertaining to possibilities of private enforcement under the Regulation. As mentioned, Art. 1 (7) states that "[n]ational authorities shall not take decisions which run counter to a decision adopted by the Commission under [the] Regulation" and that "[t]he Commission and Member States shall work in close cooperation and coordinate their enforcement actions on the basis of the principles established in Articles 37 and 38." Art. 37 further goes on to state that the cooperation and coordination of enforcement between the Commission and the Member States is meant to "ensure coherent, effective and complementary enforcement of available legal instruments applied to gatekeepers within the meaning of [the] Regulation" with Art. 38 more precisely describing the principles of such cooperation. Pursuant to Art. 38 of the Regulation, the cooperation and coordination between the Commission and the Member States regards mostly obligations on Member States to inform the Commission when the national authorities are intending to enforce rules and impose obligations pursuant to Art. 1 (6) of the Regulation, that being national competition rules etc., on gatekeepers. The provisions therefore don’t describe rules of joint enforcement of powers and obligations pursuant to the Regulation, but instead give a clarification on when and how national competition rules etc. can be used as a complementary means to the DMA. The provisions also don't give any clarification pertaining to use of private enforcement.

Art. 39 of the Regulation deals with cooperation with national courts. Art. 39 (1) states that national courts "[i]n proceedings for the application of [the] Regulation, […] may ask the Commission to transmit to them information in its possession or its opinion on questions concerning the application of [the] Regulation." The second paragraph goes on to state that "Member States shall forwards to the Commission a copy of any written judgment of national courts deciding on the application of [the] Regulation." Inclusion of Art. 39 is in line with Art. 1 (6) of the Regulation stating that the DMA is without prejudice to the application of Art. 101 and 102 of the TFEU, meaning that the provisions of the DMA create obligations and rights for individual entities, as was the case in Guérin Automobiles v Commission. This however begs the question of what exactly the national courts are empowered to rule on.

As previously stated, the powers granted under the Regulation are granted to the Commission. The Commission is solely empowered to designate gatekeepers pursuant to Art. 3 (4), suspend certain obligations pursuant to Art. 9 (1), exempt from certain obligations pursuant to Art. 10 (1), update obligations pursuant to Art. 12 (1), open market investigations pursuant to Art. 16,

178 Case C-282/95 P (39).
open proceedings pursuant to Art. 20, adopt interim measures pursuant to Art. 24 and impose fines pursuant to Art. 30. National courts and authorities have no leeway to take steps or rule on the provisions of the Regulation, based solely on the legislative text. Furthermore, pursuant to Art. 39 (5) "[n]ational courts shall not give a decision which runs counter to a decision adopted by the Commission under [the] Regulation", further stating that the courts "should avoid giving decisions which would conflict with a decision contemplated by the Commission in proceedings it has initiated under [the] Regulation", effectively removing any power from the national courts where the Commission rules the other way.

As it stands, DMAs current provisions in no way offer clear and distinct procedures for national courts to rule on, leaving us with the ambiguous text in Art. 39. The Regulation does however include provisions on clear obligations pertaining to gatekeepers, which in turn give rights to the victims of gatekeeper's illegal conduct. The missing pieces are provisions dedicated to procedural rules on how disputes are to be settled and the available remedies in case of disputes.

As is the case with the preamble and Commissions statements, the provisions of the DMA give us no clear concrete answer on DMAs private enforcement due to the lack of procedural rules. There is however enough evidence to support that private enforcement should be available under the Regulation. The question we are left with is how exactly we are to fill the gaps in the provisions, and in that sense, if the gaps at all can be filled.

3.4.1.3 Filling the procedural gaps in the DMA
There are two main natural ways to fill the procedural gaps in the DMA: through use of other EU Law and trough use of national law. In our discussions on EU Competition Law under Section 2.4.2, we encountered both of these. Let’s start by looking at EU Competition Law.

Much like the proposed US legislation we encountered in Section 2.4.4 of this thesis where the Bills themselves only mention public enforcement, relying on the Clayton Act for the private aspect of enforcement, an argument on filling the procedural gaps in the DMA with EU Competition Law firstly depends on viewing the DMA as anti-trust legislation in line with other EU competition rules. This would open the door for applying the procedural rules of the Damages Directive and Regulation 2003/01 on the DMA itself. This begs the question of whether the DMA can be viewed in such a way, and on this matter, the experts and the Commission agreed; the DMA holds no such position. Our examination shows as much; the DMA operates

\[179\] Podszun (2021)(b), Podszun states, in line with Commission remarks, that the DMA is not a piece of competition law legislation, despite the wishes of many. Legislation pertaining to the enforcement of TFEU Art. 101 and 102 can therefore not be applied.
without prejudice to TFEU Art. 101 and 102 pursuant to DMA Art. 1 (6) and the procedural apparatus enshrined in the Damages Directive and Regulation 2003/01 therefore don't apply *de jure*.

Even though the DMA isn’t to be viewed as traditional anti-trust legislation, an argument can still be made that there is a lot to learn from battles fought and won in this area of law within the EU. Amaro suggests exactly this, stating that TFEU and Court of Justices’ case law regarding the Treaties, here especially *Manferdi*, can be used to “provide useful lessons”. Following Amaro’s argument, we arrive at the second set of rules DMAs procedural gap can be most naturally filled with; national law, more precisely “in application of the principle of procedural autonomy, subject to the usual limits set out by the principles of effectiveness and equivalence.”

Even at such an early stage as this, we are so lucky to view this in action.

Carugati reports that Germany in recent years has implemented several antitrust measures and initiated cases to regulate major technology companies. The German Competition Act has been amended, strengthening the Bundeskartellamt (B KartA), which has identified Meta, Alphabet, Amazon, and Apple as within German competition law's scope. Crugati states that the B KartA is seen as a leading digital antitrust authority, causing concern in Brussels. Crugati continues:

“Germany thus competes with Brussels in overseeing big tech. But Brussels has a card Germany does not have and will never have. Brussels is the sole enforcer that can tame big tech in Europe, whereas B KartA can do it only within Germany in areas unregulated by Vestager through the DMA. EU legislators adopted this card with Germany in mind to avoid market fragmentation arising from a patchwork of national legislation.

Conscious of this limit, the German government (and Mundt) stated that they would assist Brussels in enforcing the DMA and that Section 19a would complement it rather than compete with it. The latest amendment to the German Competition Act empowers Mundt to help Vestager with the DMA. But the amendment also enables the B KartA to open a market investigation in any market and force market players to change their behaviour, and even how they operate structurally by breaking them up. Brussels

---

180 Amaro (2021).
181 Carugati (2023)(a) – Carugati outlines Germanys efforts to tame the Big-Tech in an article.
182 Ibid.
183 Gesetz gegen Wettbewerbsbeschränkungen – GWB.
184 Federal Cartel Office of Germany.
contemplated this power with a proposal for a new competition tool, but finally rejected it in favour of the DMA.”

However interesting, not much is to be gained from discussing Germanys efforts to tame the Big-Tech itself, at least pertaining to possibilities for private enforcement of DMAs obligations. The willingness to regulate on national level is on the other hand imperative in establishing possibilities for such private enforcement. Not bearing in mind Germanys approach, it is therefore important to establish the limits of such regulation, which brings us back to Amaros argument; the limits are set by the DMA itself.

We have already covered that since DMAs obligations seem “sufficiently precise and unconditional to create rights, they may therefore be invoked before national courts.”\(^{185}\) Amaro continues this notion:

“Moreover, the DMA also contains several rules modelling the exclusive competence of the European Commission (Articles 3, 8 and 29 to 33 – see also Recital 91: “The Commission is the sole authority empowered to enforce this Regulation”). When, read a contrario, these rules can also tell us about the competence of national courts: they would not be empowered to classify a company as a gatekeeper under article 3, to apply the suspension system under article 9, and even to rule on violations to articles 5, 6 and 7. If this interpretation is correct, it would make private litigation a minimalist form of litigation: exclusively follow-on damages actions.”

Amaro ends with “Is that what we want?” Podszun on the other hand, opposes Amaros conclusion, citing Art. 288 TFEU in conjunction with the judgement in Van Gend & Loos:

"Independently of the legislation of Member States, Community law not only imposes obligations on individuals, but it also intended to confer upon them rights which become part of their legal heritage. These rights arise not only where they are expressly granted by the Treaty but also by reason of obligations which the Treaty imposes in a clearly defined way upon individuals as well as upon the Member States and upon the institutions of the Community.”\(^{186} 187\)

Amaros and Podszuns points of view differ with regard to concreteness of the obligations. Podszun approaches the discussion by looking at the obligations specifically.

\(^{185}\) Amaro (2021).
\(^{186}\) CJEU Case 26-62.
Podszun notes that Art. 5 contains specific obligations for gatekeepers that are directly applicable, allowing business and private users to rely on these rules as rights.\(^{188}\) Even though Podszun's remarks are based on the DMA draft, we can gather as much by analysing how Art. 5 (3) of the current version of the DMA for instance states that the "gatekeeper shall not prevent business users from offering the same products or services to end users through third-party online intermediation services". Such violations of Art. 5 can therefore be enforced in private litigation, such as seeking injunctive relief, as long as the Commission has reached a decision that the violator is a gatekeeper subject to the obligations of the Article. Podszun notes that Art. 5 does however contain many vague terms but rebuts that such ambiguity negates its direct applicability in private enforcement, stating that "the legal concept matters, not the factual difficulties in determining legal obligations – all words are subject to ambiguity, but that does not take them out of the Van Gend & Loos rules."\(^{189}\) Podszun's remarks don't include Art. 7 as this provision was added later, but an analysis of the obligations leads us to suspect that the same remarks applicable to Art. 5 obligations apply for Art. 7 as well.\(^{190}\)

With regard to Art. 6, Podszun's opinion is that this Article has less private enforcement possibilities due to the obligations being less specific, mainly because these obligations are susceptible of being further specified under Art. 8 of the Regulation.\(^{191}\) Initiating private litigation proceedings based on this Article could open to arguments by the gatekeeper stating that the rule is not specific enough, which in turn would lead to the plaintiff having to drop the case because "there is no procedure under existing law to stay the proceedings and involve the Commission." Podszun notes that Art. 6 therefore becomes directly applicable in private enforcement after the Commission establishes concrete specifications with the specific gatekeeper, because "[o]nly where a rule is self-executing and where the competence to assess this character of the rule lies with a national court, such claim can be brought."

An important note with Podszun's assessment of Art. 6 is that it is based on the DMA draft. This version of the DMA doesn't include Art. 39 on cooperation with national courts which we have discussed. As we have noted Art. 39 (1) states that "[i]n proceedings for the application of [the] Regulation, national courts may ask the Commission to transmit to them information in its possession or its opinion on questions concerning the application of [the] Regulation". An argument can be made that this provision mends the problems Podszun identifies with private enforcement.

---

\(^{188}\) Ibid. p. 11.
\(^{189}\) Ibid.
\(^{190}\) Art. 7 as we have discussed entails gatekeepers allowing end-to-end messaging between two individual end users using different number-independent interpersonal communications services. This should be regarded as a specific and concrete obligation, where failure to comply could result in private litigation seeking injunctive relief or compensation.
\(^{191}\) Podszun (2021)(a) p. 11.
enforcement of Art. 6 by allowing the courts to involve the Commission in the proceedings helping them understand the specifications regarding obligations of potential violators.

As we can gather, a case can be made for private enforcement under the DMA. Pdoszun states that "[i]f the draft DMA remains unchanged, private enforcement will be burdensome." The draft has been changed to include Articles on cooperation with national authorities and courts, but as we have discussed, the Regulation still lacks concrete mechanisms which would strengthen private enforcement. This leads us back to Amaros question; is this what we want?

3.4.1.4 Final thoughts
We have established certain ambiguities pertaining to private enforcement under the DMA. Our conclusion is however that the Regulation opens possibilities for such enforcement, to a certain extent. The question that remains is whether the outlined enforcement of the Regulation is optimal. This question invites us to dissect DMAs overall enforcement apparatus holding it up against the goal of taming or reining in Big-Tech companies in the EU, bearing in mind all we have learned about private and public enforcement, both generally and connected to specific past legislation. Before we do so, we will first look at the possibilities for private enforcement under the DSA, mainly pertaining to enforcement of VLOP obligations.

3.4.2 The power of the national courts under the DSA
Pursuant to Art. 54 of the DSA, recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect to any damage or loss suffered due to an infringement by those providers of their obligations under the Regulation. This provision of the DSA undoubtably ratifies the infringed parties right to take infringers of the DSA to court, making private enforcement under the DSA possible.

The enforcement apparatus of the DSA nonetheless can be compared to that of the GDPR. After all, Member State are to appoint competent enforcement authorities. Where GDPR has Data Privacy Coordinators, the DSA has Digital Services Coordinators. Art. 53 of the DSA states that recipients of services covered by the DSA shall have a right to lodge a complaint with the Digital Services Coordinator alleging infringements against providers of intermediary services. In turn the Digital Services Coordinator may for instance order cessation of infringements or impose fines pursuant to Art. 51 (2) (b) and (c) respectively. The competence of the Member States is however modified under Art. 56 of the Regulation.

---

192 Ibid. p. 12.
Art. 56 (1) states that Member States have exclusive powers to supervise and enforce the Regulation, however not pertaining to infringements of Chapter III Section 5 on additional obligations for VLOPs to manage systemic risks pursuant to Art. 56 (2) and other obligations pertaining to VLOPs pursuant to Art. 56 (3). Art. 56 (4) states that where Commission has not initiated proceedings for the same infringement, the Member State in which the main establishment of the provider of VLOP or of very large online search engine is located, shall have powers to supervise and enforce the obligations under this Regulation, other than those laid down in Section 5 of Chapter III, with respect to those providers. Art. 56 (4) therefore states that a Member State has competence to enforce obligations pertaining to VLOPs where the Commission has not itself started proceedings, however not pertaining to infringements of Section 5 of Chapter III.

Seemingly, we stand in front of a legal ambiguity; every recipient of a service has the right to seek compensation in case of infringement pursuant to Art. 54, but Member States don’t have the power to enforce certain obligations pertaining to VLOPs pursuant to Art 56. Is it at all possible to interpret these provisions in harmony, and if so, what exactly are the national courts competent to decide pertaining to VLOP infringements under the DSA?

Firstly, we ought to look closer at what exactly Art. 54 entails. The provision only mentions compensation, which begs the question of whether courts at all can order cessation of infringements. If we look at Art. 51, we can gather that Digital Services Coordinators may exercise their powers under paragraph 2 (a)-(e) or request the national judicial authority in their Member State to do so. For instance, they may order cessation of infringements or request the judiciary to do so pursuant to Art. 51 (2)(b). This wouldn't constitute private enforcement as the recipients of the service do not themselves request the judiciary to rule on their behalf, even though we do find ourselves in an area between public and private enforcement.

It is uncertain whether the recipients of a service pursuant to the Regulation may take matters into their own hands and take them to court to request injunctive relief for instance. The provisions of the Regulation do not explicitly provide for this. The natural conclusion would be that any act of power conducted by the Digital Services Coordinator may be contested in court alike the GDPR, but this is not clearly stated. Unlike the GDPR, seeking civil remedies from courts other than compensation as the first step, is not however clearly defined in the Regulation. Alike DMA, one could here argue the Courts view in Van Gend & Loos; if the obligations are clearly defined, then they too constitute rights which may be brought before the courts. In the matter of DSAs obligations, this argument can, apart from Section 5 under Chapter III, be made for an array of obligations. We can however anticipate that this will not be so prevalent, as we have seen with the GDPR.
The seemingly right conclusion pertaining to private enforcement of the DSA, especially regarding VLOP obligations, is that while an argument can be made for it, EU sure hasn't been clear on the matter. Same goes for the DMA as we have seen. The general feeling is that the framework of the Digital Services Act package pertaining to private enforcement, requires jumping through hoops and digging up old precedents. The answer to why this seems to be the case is not plain. We can however look at the enforcement of the Digital Services Act package as it stands and discuss whether it is optimal.

3.4.3 Optimality of DMA/DSA enforcement

3.4.3.1 Designation of gatekeepers and VLOPs

It seems only obvious to begin a discussion on efficiency and viability of enforcement under the DMA and DSA, by examining the mechanisms for designation of gatekeepers and VLOPs. These are after all the instruments for ensuring a company/service provider is obliged to comply with the obligations set out in these regulations, making them subject to both private and public enforcement mechanisms. As we have discovered, this power lies in the hands of the Commission, which is solely empowered to designate gatekeepers and VLOPs.

As we have seen with regard to the DMA, designation of gatekeepers will under every circumstance hinder private enforcement of the Regulation, in so far as the possibilities of private litigation based on obligations in Art. 5 and 7 are dependent on a designation which cannot be decided on by the national courts. The same argument can be made for VLOPs pursuant to the DSA: enforcement against them may only find place if they are designated as such. This doesn't make the enforcement of the regulatory framework less efficient nor unviable. As Podszun puts it, "[t]he designation of digital gatekeepers is certainly a legal act that requires the authority of the Commission."\(^ {193}\) The obligations of both regulations are comprehensive. As they are meant to only concern the biggest actors holding entrenched positions in the market and having a special role and reach, the designation shouldn't be taken likely, and the mechanisms certainly should be strict so as not to lead to overenforcement.

Centre on Regulation in Europe (Cerre) has conducted a paper on certain problems pertaining to designation of gatekeepers in the DMA.\(^ {194}\) They identify three issues which are yet to be clarified: I) whether it is sufficient for a gatekeeper providing several services only to be designated once, II) standards to be applied to rebut presumptions based on quantitative thresholds, and III) the application of anti-circumvention rules. We will take a short look at all these issues.

\(^ {193}\) Ibid. p. 10.

\(^ {194}\) Feasey (2022), Note on Designation of Gatekeepers in the Digital Markets Act.
Pertaining to sufficiency of only one designation per gatekeeper, the paper states that the DMA defines a gatekeeper as a firm providing a designated core platform service (CPS).\textsuperscript{195} This entails that there are two interpretations to this definition: 1) a single firm can have multiple gatekeeper designations for different CPSs, and 2) once a firm is designated as a gatekeeper for one CPS, any other CPSs provided by the firm would be added to the list without needing a new designation. It is unsure which of the two definitions is correct. Looking at Art. 3 (9) we can gather that for each undertaking designated as a gatekeeper the Commission shall list in the decision the relevant CPSs that are provided, and which individually are an important gateway for business users to reach end users. Such ambiguity is unhelpful according to the paper, especially since market power in one service doesn't automatically imply market power in another, which also makes the first definition the fairest. Cerre therefore recommends that the text be made clearer to reflect this reality. The point is also touched upon by Carugati with example:

"For instance, Google Search displays Google Maps when a user searches for restaurants. In this context, Google Maps and Google Search are used for the same purpose; end-users and/or business users cannot use Google Search independently as they cannot perform a search without a map being displayed. In that case, it is doubtful that Google Maps is a distinct service from Google Search, as they might be substitute services. They might therefore be considered part of the same CPS in online search engine services. However, Google also offers Google Maps on a standalone basis through an application or from the web. In that case, Google Maps is likely a distinct service from Google Search and might be a complementary service to Google Search, as a user can perform a search on Google Maps without using Google Search. For instance, users can make location-related searches on Google Maps, whereas they make general queries on Google Search. Accordingly, Google Maps and Google Search might be considered two distinct CPSs – Google Search in online search engine services and Google Maps in online intermediation services. In this case, it will be thus difficult to distinguish CPSs. This point matters as considering a service distinct might make it subject to the DMA if it fulfils the other criteria."\textsuperscript{196}

Pertaining to standards for rebuttal, the paper notes that Art. 3 (5) allows firms to submit arguments for why they should not be designated as a gatekeeper despite meeting quantitative thresholds under Art. 3 (2).\textsuperscript{197} On the other hand Art. 3 (8) enables the Commission to designate a gatekeeper despite the form/service not meeting the same thresholds. What is unclear,

\textsuperscript{195} Feasey (2022) p. 7 see also DMA Art. 2 (1).
\textsuperscript{196} Carugati (2023)(b).
\textsuperscript{197} Feasey (2022) p. 8-9.
according to Cerre, is whether the same evidential thresholds and relevant factors apply in both situations. The issue is grounded in Art. 3 (5) considering exemptions as "exceptional", whilst Art. 3 (8) doesn't mention this. As regards evidential standards, Article 17 would seem to envisage the European Commission undertaking a similar form of market investigation when arguments for exemption have been accepted under Art. 3(5) and when the Commission proposes to designate under Art. 3(8). Once the Commission has decided to proceed to a market investigation then it would seem appropriate that the assessment would be undertaken by the Commission adopting the same evidential standard as it would apply to any other market investigation, including an investigation undertaken pursuant to Art. 3(8).

Finally, with regard to the application of anti-circumvention rules, the paper states that the provision in Art. 13 aims to address strategic behaviour by firms and prevent them for evading regulation by dividing services.\(^{198}\) The problem, according to Cerre, is that Annex A allows firms to offer different commercial services with the same CPS provided they are used for different purposes. Cerre states that the Commission needs to either show that services within the same CPS class are not used for different purposes and should be aggregated, or that the motive for disaggregating services was to evade regulation rather than legitimate commercial purposes, to address such strategic behaviour. This can however prove to be challenging according to Cerre due to the complexity of motivations for changing commercial practices and the potential for firms to influence the perceived purpose of a given service.

Cerre's identified issues concern the material side of rules on designation. It is unclear what effects these issues would have on the optimal enforcement of the Regulation if they indeed became prevalent and consistent. Furthermore, the effects would not be as prevalent under the DSA regime, as DSA only concerns providers of intermediary services. A far bigger potential blow to the enforcement efforts under the Digital Services Act package is rooted in the body executing the designation decisions, more specifically, their willingness to execute their power. As Andrijchuk writes, "while the competence of the Commission to designate appears to be justiciable, the competence not to designate looks very unlikely to be subject to judicial review."\(^{199}\) So what if the Commissions political agenda changes, or as Podsuzen puts it, "[w]hat if a successor of Margrethe Vestager is less keen on taming the tech titans?"\(^{200}\) As we have discussed, this is always a potential problem with public enforcement, and in the case of the DMA/DSA, it hinders not only enforcement by the Commission, but also eliminates the possibilities of private enforcement which are dependent on designation made by the Commission. This blow is of course lesser as pertains to the DSA, seeing that it only hurts the efforts of

\(^{198}\) Ibid. p. 9-10.

\(^{199}\) Andriychuk (2022) p. 126.

\(^{200}\) Podsuzen (2021)(b).
enforcing those provisions applicable to VLOPs. Andrijchuk puts it like this, "[s]uch flexibility is incompatible with an entitlement-based logic whereby the rights of business users under the DMA would have to be protected irrespective of the discretionary designation."\(^{201}\) Then again, as we have mentioned, the obligations in the DMA/DSA are comprehensive, and designation decisions should not be taken lightly.

A possible solution that maintains the severity of designation decisions whilst also attending to Commissions eventual changes of heart, is giving the designation powers to the Member States. Here we would have to avoid what we have learned from the "one-stop-shop" in the GDPR and equip all the Member States with the power to designate gatekeepers which operate within their borders without necessarily having their place of establishment in that Member State. A problem far more prevalent would be potential inequitable execution of power leading to fragmentation of the Digital Single Market. In case of Commissions abstention from its designation duties, some enforcement would however be better than no enforcement. If the Commission still executes its power alongside Member States, the problems with fragmentation become less prevalent.

Only time will tell how well the functioning of designation of gatekeepers and VLOPs will be. It is however clear that there is a need for some refinement in the legislative text already at this stage. It is further undoubtful that the Commission has taken on a huge responsibility. The important thing to remember here is that this responsibility doesn’t only consist of designation of gatekeepers and VLOPs. As Commission has stated, it is the sole, or as we have seen, at least the main enforcer of the DMA and the provisions relating to VLOPs under the DSA, having most of the power. In the following Section we will problematise this.

### 3.4.3.2 Commissions workload

As we have learned with our discussions of the one-stop-shop, effective enforcement demands quick and decisive execution of the enforcement mechanisms. It is probable that the Commission in the implementation of the DMA and the DSA had this in mind, seeing their willingness and morale as strong enough to enforce the complex rules of the regulatory frameworks all by itself, bearing also in mind the disappointment we have seen in certain handlings of GDPR cases connected to tech titans conducted by the Irish DPA for instance. Willingness and morale aren’t however always enough to achieve the goals at hand.

As it stands the Commission at current state of play stands for most of the enforcement of DMA, which entails designation decisions, conduction of market investigations and finally, investigations into and decisions on potential non-compliance. Each of these are complex tasks

---

\(^{201}\) Andriychuk (2022) p. 126.
undoubtedly calling for collection of an abundance of data. This data, naturally being complex, further requires specialized processing towards reaching a decision. The Commission must do all this whilst facing exhaustion and attrition by their tech titan counterparts. Finally, the Commissions only purpose isn’t enforcing DMA. The Commission as the executive branch of the EU has loads of tasks, one of which is enforcement of the DSA as well. As so much of the enforcement of the DMA and DSA lies with the Commission, it is important to ask, will the Commission be able to deliver effective enforcement?

Vergnolle sees this as one of the main issues with DMA enforcement, stating that “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.” This is not impossible, albeit Vergnolle notes that the absence of the latter already has been considered one of the reasons for GDPRs enforcement failures. The reasonable conclusion however is that this is a momentous task, where the chances of the Commission failing to deliver effective enforcement, are high.

With regard to the DSA, it is important to note that Commissions duties do not only concern designation of VLOPs and decisions pertaining to their infringements. The Commission also for instance has the duty to act where a case is referred to them pursuant to Art. 59 (1) of the DSA, making their potential workload even bigger.

Looking past the effectiveness of the enforcement, Vergnolle also makes an argument against its suitability, stating that it puts the European separation of powers at stake. She writes that European Commission's enforcement powers in the Digital Service Act package have expanded its role beyond the executive arm of the European Union. The Commission's influence now extends to the legislative and judicial branches, with limited enforcement roles given to national judiciaries. The Commission can adopt "non-compliance decisions" and impose heavy fines on organizations, similar to the functions of a court. Additionally, procedural rights like the right to be heard and access to the file are granted to services and gatekeepers, further emphasizing the Commission's judicial role. Although this shift towards enforcement out of courts in the digital sector is partly due to courts being understaffed or less specialized, Vergnolle writes:

“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

203 Ibid.
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.  

Circling back to the one-stop-shop, we ought also to consider Member States workload, specifically pertaining to the DSA. As we have seen, Member States are granted exclusive power to supervise and enforce the DSA pertaining to providers of intermediary services which have their main establishment within their borders. This in itself can be regarded as carrying on the one-stop-shop from the GDPR to the DSA. The DSA tries to remedy this by imposing the Digital Services Coordinator with a deadline where the matter concerns cross-border enforcement, stating that the Coordinator shall assess the infringement without undue delay and in any event, not later than two months following receipt of the request pursuant to Art. 58 (5). Where this is not done, the matter may be referred to the Commission pursuant to Art. 59 (1). The Commission in turn must assess the matter within two months following the referral pursuant to Art. 59 (2). The Commission can then where it considers that the assessment or the investigatory/enforcement measures taken/envisaged are insufficient to ensure effective enforcement, refer the case back to the Digital Services Coordinator with their view, giving the Coordinator a new deadline of two months to reach a decision pursuant to Art. 59 (3), effectively making the absolute deadline for cross-border cases six months. This is all in all a welcome change, which would, if functioning properly, ensure the problems of one-stop-shop don’t follow over to the DSA. In the question of optimal enforcement of those provisions regarding VLOPs, this does however yet again give the Commission even a larger task making enforcement harder and subsequently doing so for the DMA as well.

Looking at the DSA, it is also apparent that the overall enforcement apparatus is quite confusing. Where the DMA, although not optimally, has the Commission at its head, the DSA operates with several enforcers splitting the enforcement duties between Member States and the Commission in what Vergnolle denotes as "a maze of responsibilities". Yet, pertaining to the most important and dangerous actors, the VLOPs, the Commission again consolidates its own powers making itself the sole enforcer. Vergnolle argues that providing such a monopolistic role to the

---

204 Ibid.
205 Ibid. p. 106.
Commission may in the end lead to dangerous consequences. We have reviewed one such consequences, a potential change in Commissions sheer will to designate, investigate and sanction. We can now amend this list with potential inertia due to the sheer workload the Commission is going to face.

As it stands, the Commission may have chewed off more than it can bite with regard to enforcement of the Digital Services Act package. The regulatory frameworks do however stem from noble goals which certainly have the power to bring around a positive change in competition in the digital sector as well as the strengthening of fundamental rights of EU citizens, but how do we achieve them? What enforcement do they call for?

3.4.3.3 The goals at hand and the enforcement they call for

This thesis started with a much narrower sight in mind, discussing only the private enforcement of the Digital Services Act package. The possibilities, the effectiveness and the suitability of such enforcement. We have however seen that such discussions demand looking at the whole picture, the delicate interplay between private and public enforcement in determining the optimal enforcement of law. I do however find it funny that what drew me to this subject, the utter lack of provisions on private enforcement in the DMA, is what I will circle back to in discussing the optimal enforcement of the DMA/DSA. In other words, after examining both private and public enforcement more generally, examining past legislation concerning Big-Tech and the DMA/DSA themself, the case I want to make, the case I feel must be made, is one for vigorous private enforcement under the regulatory frameworks.

First and foremost, let's get one thing out of the way; the case being made is not one for exclusive private enforcement. As we have concluded, designation of gatekeepers and VLOPs should fall within the powers of public authorities. The powers of the Commission to designate gatekeepers and VLOPs should however be expanded later if the workload is too big. There is nothing wrong with asking for help. Private parties in competition designating each other as gatekeepers hardly seems to make sense. We are however yet to see how the obligations of DMA will impact the gatekeepers. In the case complying with the obligations is easier than first thought, one could possibly expand the circle of obligers, even by setting a list of terms which if met automatically trigger a designation. One must however have in mind that the main goal is a contestable and fair digital market; obliging companies which do not hold an entrenched position would probably lead to the opposite. Similar goes for the VLOPs under the DSA.

With that out of the way, let's first discuss why private action against violations of gatekeepers is a good idea. In choosing optimal enforcement, we have discovered that we should look to three criteria: The type of law being enforced, potential harm caused by violations and available resources for enforcement. Let’s analyze the DMA with these criteria in mind.
DMA is a comprehensive law, holding a set of complex obligations pertaining to its obligers. As we have concluded, designation is best suited as a power of public authorities because of this. On the other hand, these obligations are concrete rights of other companies competing with the tech giants, meant to level the playing field between them. These companies therefore hold a great interest in the enforcement of these obligations, or rather yet, an immense willingness to litigate. It is to some degree incomprehensible having the goal of tackling competition issues in the digital sector, changing the law for that purpose, but at the same time not arming those suffering at the hands of those with entrenched positions, with the possibility to use the law towards achieving the goal. The point is that this is a law that bears importance both for the society as a whole, but also certain individuals and entities within it which have a personal stake and better information on the issue. We have in the past few years seen environmental groups for instance making use of the legal arsenal pertaining to environmental issues, however small it may be, to take the issue of climate into their own hands because of their own resoluteness. This is therefore positive, both for the society and the individuals/entities within it. As Frédéric Bastiat said, “The worst thing that can happen to a good cause is, not to be skilfully attacked, but to be ineptly defended.”

The goal of the DMA being to promote a competitive digital sector, potential harm caused by violations of its obligation may exude itself on the market and the fundamental rights of Union Citizens. This harm may perhaps not be of the same calibre as pollution, but it would centrally bear negative effects on the EU and its citizens. Preventing such harm is as we have discussed maybe best suited through use of public enforcement measures. In relation to the DMA, making an argument for sole public enforcement because of this is however untenable, mostly because the harm felt is first and foremost felt by the infringed companies and the harm isn’t of criminal nature. Furthermore, equipping these companies to fight their infringers with the DMA alongside public authorities may alleviate and prevent even more harm.

Last in our brigade of criteria is available resources. This point has already been touched upon in the previous Section. It is hard to imagine that the Commission will have enough resources to satisfyingly complete each power granted to it under the DMA besides those granted under the DSA as well etc., much of this pertaining to the mere mass of information gathering and

---

206 See Urgenda Foundation v. State of Netherlands where the foundation argued and won that Netherlands should do more to prevent climate change pursuant to Art. 2 and 8 of the ECHR see also HR-2020-2472-P where Greenpeace and Natur og Ungdom argued a similar case against the Norwegian Ministry for Oil and Energy on the basis of The Norwegian Constitutions § 112, and although not winning the case fully, at least confirmed with the Supreme Court of Norway that the right in § 112 indeed is a material right of Norwegians citizens which the Government must respect (paragraph in the judgement)

207 Past member of the French National Assembly.

208 Bastiat (1845) p. 107.
processing which is needed. On the other hand, the infringed parties of the DMA will certainly have ample knowledge about the violators and their violations concerning them. In turn they will probably in most circumstances be willing to use their resources to launch private litigation efforts. Furthermore, certain violations of the DMA could potentially be far reaching, bringing firms to cooperate in litigation against the infringer, sharing information and resources by doing so. Where this knowledge or means to litigate does not exist, the mechanisms of public enforcement and their executor will have their opportunity to shine.

Finally, much of what we have discovered by examining past legislation relevant for Big-Tech, concerns the slowness, latency and inertia in public enforcement. On the other hand, we have seen some increase in private enforcement of the GDPR and that private enforcement can prevail in Competition Law trough expediting litigation. As we have discovered, building up these procedural mechanisms in competition law has taken years, and it is therefore startling that they are not present to a higher degree in a piece of legislation such as the DMA.

Many things point towards private enforcement being a viable and needed option towards reaching optimal enforcement of the DMA. As we have discovered, the public enforcement apparatus could also benefit from certain changes. Nonetheless, this is the case for private enforcement of the DMA.

Pertaining to the DSA, much of what regards the DMA can be said here as well. The obligers of the DSA however, in this case VLOPs, will rarely have the same opposing actor as the gatekeepers under the DMA in case of infringements. The DSA intends to safeguard users' fundamental rights. In doing so, the probable infringed party is the union citizen himself. Whereas companies have greater resources to fight against gatekeeper infringements, a lone person would struggle more going against an infringement caused by a VLOP. The mere complicity of the law at hand would certainly demand use of legal counsel furthermore cementing the need for great resources. The optimal enforcement of the DSA therefore demands vigorous public enforcement where public authorities are specialised in dealing with potential issues pertaining to the Regulation and can effectively remedy infringements. With regard to this, we have concluded that the DSA to a degree addresses those problems we have seen with the GDPR, such as the one-stop-shop, but we have yet to see how this works in actuality; if the maze of responsibilities is traversed in an effective way by all those actors empowered to enforce. Of utmost importance for this thesis, however, is the enforcement of VLOP obligations which is centralized, leaving us with the same issues as it does under the DMA. The question is how this should be addressed so as to lead to optimal enforcement of the DSA.

One way of addressing the centralization of enforcement of VLOP obligations under the DSA is giving the Member States the opportunity to address and decide themselves on every VLOP
infringement affecting their citizens. The risk of course is transferring the fragmentation that occurred under the E-commerce Directive to the DSA, with the possible effect of damaging the Digital Single Market. The counter argument is again that some enforcement is better than none in case the Commission can’t complete or in worst case abandons its duties. Setting aside the alarming notions and consequences of centralization of power in the manner the DSA does pertaining to VLOP obligations, amending the powers of the Member States should perhaps come at a later date, firstly because this would give us concrete insight into Commissions effectiveness and willingness to enforce the obligations and secondly because Commissions enforcement efforts then can be used as a precedent possibly averting fragmentation of the rule of law.

The second way of addressing the centralization of power is implementation of possibilities for vigorous private enforcement. It is after all a reasonable assumption that infringements of VLOPs in many cases will affect several people. Here we can draw inspiration from USA for instance, building on principles of the Representative Action Directive as well, and set the stage for specialised litigants which can take infringements of the VLOPs to the courts on behalf of several claimants simultaneously. Indeed, such litigation possibilities would also ensure that the Regulation can be enforced, even where the Commission changes it’s focus.

Even though this thesis holds potential private enforcement of the Digital Services Act package in a high regard, the two abovementioned solutions can work in unity. As discussed, it is important that the DSA has vigorous public enforcement, but, if the system does not meet the goals envisaged, these solutions in unison could perhaps meet them. It is important to note however, that the second solution pertaining to private enforcement of the DSA, can and should be implemented already. Fragmentation of law should not be any issue here, as long as the claimant and the defendant have the opportunity to address potential disagreements at EU level as well. This is the case for private enforcement under the DSA. Let’s now examine how private enforcement under the DMA/DSA could function in the future.

3.4.3.4 The future of private enforcement under the DMA/DSA

Firstly, we must reiterate that the future of the DMA depends on changes to the legislation as it stands right now. Some changes are necessary, but there are several ways to go about this. In the following we will examine this.

One of the changes which may be necessary is described by Podszun, namely establishing a clear legal basis for private enforcement within the DMA.209 This is first and foremost based on establishing a provision that clearly states that infringed parties can litigate based on

violations of Art. 5 – 7, either in national or EU courts. The process for such litigation under Art. 6 must however be further specified due to the nature of the provision, in case Art. 39 (1) isn’t sufficient. Podszun finally notes that national law should ensure a fast-track procedure for infringement claims and a clear legal basis for damages claims, which should be possible in cases of infringement of the abovementioned provisions, or when the Commission has decided on an infringement. The reason these changes are only possibly necessary is because the Regulation as we have discussed already at this point may be capable of ensuring them. The changes would nonetheless make the argument for possibility of private enforcement absolute.

Podszun further points out that the DMA lacks detailed accompanying rules, not only for obligations under Articles 5 and 6 (now also 7) regarding private enforcement, but also for the role of private parties in DMA proceedings, because the Regulation does not mention the involvement of third parties in administrative proceedings, leaving them without official status. Podszun remarks that this is a mistake, as their input is crucial for the efficiency of the rules. He suggests that the DMA should include specific rights for third parties, customers, and competitors, granting them official status in proceedings that allow for judicial review. He finally states that it would be beneficial to apply rules from antitrust proceedings to DMA proceedings to address these issues.

Successful private enforcement relies on the interplay with public enforcement and certain adjudicating standards as we have discussed under Section 2.4.2 of this thesis. Podszun believes that the regulation of gatekeepers through public and private enforcement could involve the Commission’s specific roles, such as designating gatekeepers and specifying obligations, while courts help define terms in Articles 5 - 7. He further suggests that courts can handle the integration of other legal fields, including competition law, but the relationship should be clarified in DMA Art. 1.

Finally, Podszun returns to Art. 6, stating that it can be difficult for courts to adjudicate, as it requires a deep understanding of business models and digital markets. While courts have shown they can handle this, an alternative enforcement path tailored to the DMA could be more efficient. Podszun suggests creating an independent Platform Complaints Panels, which can be approached by private parties claiming violations of obligations. These panels would consist of independent adjudicators who are experts in digital markets and could work similarly to courts in private enforcement. They would have the power to decide on infringement claims and specify obligations. Gatekeepers would be obliged to cooperate with these panels, making them

211 Ibid. p. 13.
212 Ibid.
more accessible than the Commission or courts. A specialized body could act as a neutral adjudicator with in-depth market knowledge, easing the Commission's monitoring burden and providing accessibility for private claims. These are some of the ways of strengthening the private enforcement under the DMA.

As regards the DMA, so regards the DSA. Establishing a clear legal basis for all sides of private enforcement, pertaining to all the obligers, is a necessity. Many of the provisions under the DSA especially pertaining to VLOPs need further refinement to be clearly applicable as concrete rights, here for instance several of the obligations under Section 5 of Chapter III. The main refinement efforts of the DSA must however be dedicated to simplifying the enforcement apparatus which at this stage is quite comprehensive and to a degree centralized when it matters the most.

As it stands, meeting the goals the Digital Services Act package is set out to achieve demands further fleshing out of the public enforcement rules. We will of course get a clearer picture of what exactly needs to change when we actually see the public enforcement in action. With regard to private enforcement, there is a need for an absolute ratification of the private enforcement possibilities pertaining to gatekeepers and VLOPs, as well as clarification of certain obligations making them more prone to private enforcement. Hopefully, we will also get a clearer picture of the private enforcement possibilities at current state, though this is less likely due to the sheer ambiguity of the DMA and VLOP part of the DSA regarding private enforcement. Here we should ask ourselves if anyone is up to task to take such a case on. I sure hope so.
4 Conclusion

This thesis had two main goals: I) Examining what optimal enforcement of legislation pertaining to Big-Tech and VLOPs entails and based on this II) examine whether the enforcement of the Digital Services Act package can be viewed as optimal. The second goal demanded examining whether the Digital Services Act package can be enforced privately and identifying the flaws with the overall enforcement and offering solutions.

We can conclude that optimal enforcement of legislation pertaining to Big-Tech and VLOPs demands use of private and public enforcement in unison. Public enforcement has been the most prevalent approach at tackling such issues, yet it has seemed to fail in many regards. Private enforcement on the other hand has been on a rise and shown that it can supplement public enforcement efforts where they fail.

With regard to the Digital Services Act package, we can conclude that although an argument for possibility of private enforcement can be made, the regulatory framework at play is messy at best. Furthermore, both the DMA and the DSA contain the inherent flaw of centralization which will possibly lead to a feeling of unfulfillment considering the goals of the regulations. The flaws of the regulatory frameworks can possibly be addressed by further affirming the possibilities and procedures for private enforcement in the legislative text and perhaps also amending and expanding the public powers in case of Commissions inertia.

Enforcement of law is crucial in reaching any goal that law sets out to achieve. Why should we have a criminal code if the criminals aren't judged on their criminal deeds? Why should we have contract law if a party can withdraw from a legally binding contract just like that without any consequence? Indeed, enforcement of law should be regarded as one of the main pillars of achieving goals we set as a society, and we should strive to implement optimal enforcement, because our goals deserve as much. If not, why have goals at all?

The underlying goal of the legislation we have discussed is a fair Digital Single Market which the fundamental rights are inscribed on. As we have seen, the EU certainly hasn't taken a backseat with regard to this goal. No, we have in fact seen marvelous pieces of legislation such as the GDPR passed by the EU. Now we also have the Digital Services Act package, and certainly many more regulatory frameworks to come. Still, it is hard not to feel some kind of emptiness discussing all of this, for however good or noble the goal seems to be, the enforcement efforts, those envisaged and those made, just don't seem to be able to hit the mark. Is it too arrogant to state that you cannot play tennis with a birdie? Well, you can always try, but it will probably prove ineffective.
The envisaged enforcement of the Digital Services Act package will probably not be optimal. It will probably not reign in the tech giants. This of course is cause for concern, but things needn’t be so dreary. Law is ever evolving. We have seen as much studying private enforcement efforts under EU Competition Law. DSA is a product of the E-Commerce Directive. We are still trying to fix the problems pertaining to the enforcement of the GDPR and have even seen a rise in private enforcement. The Digital Services Act package is young and will certainly mature throughout the years. Perhaps instead of feeling emptiness, one should look to past victories and present willingness and instead choose hope.
# Table of reference

## Treaties, legislation and soft law

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation 2016/679</td>
<td>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).</td>
</tr>
</tbody>
</table>
Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.


Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Commission Notice 2004/C 101/05 Commission Notice on Handling of complaints by the Commission under Articles 81 and 82 of the EC Treaty.

EDPB Urgent Binding Decision 01/2021 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 – Adopted on 12 July 2021.
ECHR  

National Law  
Gesetz gegen Wettbewerbsbeschränkungen – GWB  

US  
U.S Const.  

S.2710, 117th Congress (2021-2022)  
The Open App Markets Act (Proposed).

S.2992, 117th Congress (2021-2022)  
The American Innovation and Choice Online Act (Proposed).


Case law  

EU  
Case C-645/19.  
Case C-295/04 EU:C:2006:461.  
Case C-282/95 P.  
Case C-26/62.

National  
HR-2021-2403-A  
Norway.
Urgenda Foundation v. State of Netherlands  
Netherlands.

LG München I, 10/02/2021–37 O 15721/20  
*Kooperation Bundesgesundheitsministerium/Google*  
Germany

LG München I, 12/05/2021–37 O 32/21  
*Amazon Kontosperrung II*  
Germany

LG Berlin, 08/04/21–16 O 73/21  
*Kart, Tipping*  
Germany

**Preparatory work**

**EU**

**COM/2020/842**  

**COM/2020/825**  

**COM/2020/264**  
Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition – two years of application of the General Data Protection Regulation.

**COM/2015/192**  
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy.

**COM/2008/165**  
White paper on damages actions for breach of the EC antitrust rules.

**SWD/2013/0203**  
Private litigation as a key complement to public enforcement of competition rules and the first conclusions on the implementation of the new Merger Regulation.

**Literature**

**Books**

Whish (2021)  

Hofmann (2019)  

Polinsky (2007)  

Bastiat (1845)  

**Articles**

Andriychuk (2022)  

Rucz (2022)  

Podszun (2021)(a)  

Web Pages


<table>
<thead>
<tr>
<th>Reference</th>
<th>Source</th>
</tr>
</thead>
</table>


Reports, papers and surveys

Feasey (2022) Feasey, Richard on behalf of Centre on Regulation in Europe. Note on Designation of Gatekeepers in the Digital Markets Act. (November


Polinsky (2005)


Videos

Congress.gov.