Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 73

New Rules for Digital Platforms in the EU and the US: Opening Pandora's Box

Nikolaos I. Theodorakis & Dimitra Tzeferakou

2023

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Authors

Nikolaos Theodorakis is Of Counsel in the London and Brussels offices of Wilson Sonsini Goodrich & Rosati, where his practice focuses on privacy and cybersecurity. Nikolaos regularly counsels on matters of EU data protection law, GDPR compliance, UK GDPR preparedness, cybersecurity, advertising, and marketing and offers a full cycle of services that includes both non-contentious matters and investigations with supervisory authorities. In addition, Nikolaos is an associate professor of law at the University of Oxford (UK), an assessor at the University of Cambridge (UK), and a TTLF Fellow at Stanford Law School, focusing on technology and intellectual property issues. Previously, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. He also gained professional experience at the U.S. Committee on Capital Markets Regulation, the Kluge Center at the U.S. Library of Congress, and the UK Ministry of Justice. Nikolaos has received awards from several bodies, including the State Council of the People's Republic of China, the UK Economic and Social Research Council (ESRC), British Academy, and the Greek Parliament. He has been widely published and frequently receives invitations for public engagements, including guest lectures across the world, international symposia, and TEDx conferences.

Dimitra Tzeferakou is an Attorney-at-Law and owner of a boutique law firm. Ms. Tzeferakou focuses on issues of contracts, torts, investment, medical law, intellectual property and data protection. She represents companies of all sizes and sectors, with a particular focus on technology companies. Ms. Tzeferakou has prior work experience at the Council of Europe, the Greek Parliament, a healthcare company, and a leading law firm in Greece. Ms. Tzeferakou holds a bachelor’s degree in politics, a bachelor’s degree in law, as well as an LL.M. and an M.Sc. degree. She has published several research papers, has participated in numerous conferences and round tables around the world as a convenor or a moderator, and has received several awards. Ms. Tzeferakou is currently a Ph.D. candidate.

General Note about the Content

The opinions expressed in this paper are those of the authors and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF’s partner institutions, or the other sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
Nikolaos I. Theodorakis & Dimitra Tzeferakou, New Rules for Digital Platforms in the EU and the US: Opening Pandora’s Box, Stanford-Vienna European Union Law Working Paper No. 73, http://ttlf.stanford.edu.

Copyright

Abstract

Recently, the European Commission published a set of proposals geared to, inter alia, regulate digital platforms. The relevant package included the Digital Markets Acts (DMA), addressing primarily antitrust-related requirements, and the Digital Services Act (DSA), addressing primarily regulatory matters. In particular, the DSA attempts to regulate long-debated topics such as (i) the liability of online platforms; (ii) the platforms' obligations regarding content moderation and (iii) transparency of advertising. These proposals are intended to apply to all digital services, including social media, online marketplaces, and other online platforms. As such, EU companies and US companies active in the EU will need to consider how these rules may affect their operations and the respective obligations they may have. The working paper will discuss the history behind the DMA/DSA proposal, including the e-Commerce Directive, and will further dive into the DSA and how the obligations that it envisages for online platforms may have a significant impact on how EU and US technology companies do business.

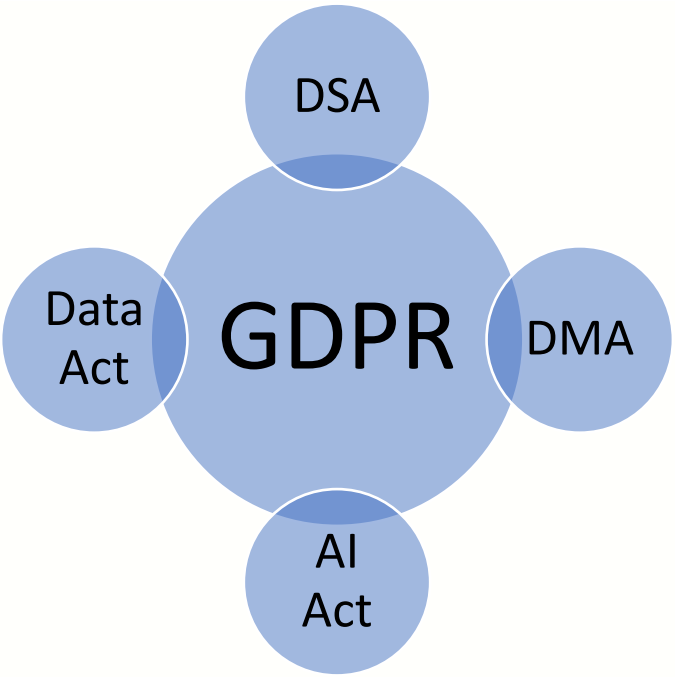
Keywords: Digital Services Act, DSA, Digital Markets Act, DMA, e-Commerce Directive

Table of Contents

1. Introduction

During 2020, the European Commission published a set of proposals geared to, inter alia, regulate digital platforms. The relevant package included the Digital Markets Acts (DMA), addressing primarily antitrust-related requirements, and the Digital Services Act (DSA), addressing primarily regulatory matters.

The DMA/DSA package is added to a new ecosystem that is being created to complement the General Data Protection Regulation (GDPR) and regulate online service providers as long as they target EU consumers. Companies subject to the DSA/DMA include several US companies, making this a matter of interest on both sides of the Atlantic. Apart from the DMA and the DSA, European institutions are now in the process of drafting/finalizing two more initiatives, the AI Act and the Data Act. Once finalized, these four new acts will create a new regulatory landscape that companies will need to comply with depending on the nature and scope of their services.



The interplay of the different acts is not yet entirely clear, particularly since some of them are work in progress, however what is already clear is that the data landscape will change radically over the next years.

In particular, the DSA attempts to regulate long-debated topics such as (i) the liability of online platforms; (ii) the platforms' obligations regarding content moderation and (iii) advertising transparency to avoid user manipulation. The DSA/DMA apply to digital services, subject to scoping conditions, including social media, online marketplaces and other online platforms. As such, EU companies and US companies active in the EU will need to consider how these rules may affect their operations and the respective obligations they may have.

The paper will discuss the history behind the DSA/DMA proposal, including its predecessor, the e-Commerce Directive, and will further dive into the DSA and how the obligations that it introduces for online platforms may have a significant impact on how EU and US technology companies do business.

2. The e-Commerce Directive as the predecessor of the DSA

The e-commerce Directive is the precursor of the Digital Services Act. It was created in the 1990s, at a time when the general public started using the internet on a mass scale, and it became apparent that the lack of regulation was exposing individuals to significant risks. The European Commission therefore set up a framework related to cross-border online services. The e-Commerce Directive was adopted in the dawn of the 21st century, with the primary aim to create economic efficiencies between EU member states, and eliminate any trade protectionist measures implemented on an ad hoc basis. Despite the fact that the e-Commerce Directive, as most of the Commission directives and regulations,

was technology neutral, with the aim of making it timeless, the evolving nature of technology has been calling for a regulatory facelift for a long time. Few things have remained the same since 2000 in terms of electronic commerce, which called for a comprehensive overhaul of this framework in a meaningful way that is fit for purpose.

Overall, the e-Commerce Directive is the foundational legal framework for online services in the EU. It aims to remove obstacles to cross-border online services. The Directive harmonizes rules regarding transparency and information requirements for online service providers; commercial communications; and electronic contracts and limitations of liability of intermediary service providers.

The Directive sets out basic requirements regarding mandatory consumer information, steps to follow for online contracts and rules on commercial communications. Examples of services covered by the Directive include: online information services; online selling of products and services; online advertising; professional services; entertainment services and basic intermediary services, including services provided free of charge.[1]

To the surprise of many, the DSA did not invalidate the e-Commerce Directive, but rather builds on it through amending it. The, still in force, e-Commerce Directive applies to information society services, defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual

[1] Article 2 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

request of a recipient of a service".[2] The e-Commerce Directive therefore applies to any provider that offers specific activities, for instance any provider of online hosting, anyone providing access to a communication network etc.

Recital 18 of the e-Commerce Directive adds more color with respect to the particulars of its applicability, since it clarifies that payment for the service does not affect its scope:[3] "*Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service; television broadcasting within the meaning of Directive EEC/89/552 and radio broadcasting are not information society services because they are not provided at individual request; by contrast, services which are transmitted point to point, such as video-on-demand or the provision of commercial communications by electronic mail are information society services; the use of electronic mail or equivalent individual communications for*

[2] Article 2 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[3] Recital 18 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

instance by natural persons acting outside their trade, business or profession including their use for the conclusion of contracts between such persons is not an information society service; the contractual relationship between an employee and his employer is not an information society service; activities which by their very nature cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services."

2.1. Scope of application

The e-Commerce Directive applies to information society providers established in the European Union (EU). The question of establishment is, ultimately, a question of pursuing an economic activity using a fixed establishment for an indefinite period of time. As such, simply having equipment within the EU does not amount to an establishment.[4] The e-Commerce Directive also does not apply to the field of taxation, the field of data protection, questions regarding agreements or practices of cartel law, and certain other activities (e.g. notaries, legal representation, and gambling activities).[5] It is therefore clear that the e-Commerce Directive does not want to create an overlap/complication with respect to other fields of law, such as data protection and competition law. Virtually, every commercial website is covered by the e-Commerce Directive. Every country that adopted the e-Commerce Directive did so

[4] Recital 19 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[5] Art. 1(5) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

in different terms; for instance, the UK said prior to Brexit that, in its view, it is not restricted to buying or selling online.[6]

There has been extensive case law trying to decipher what is considered as an information society provider. For instance in Google France SARL, Google Inc. v. Louis Vuitton Malletier SA and others (2010), the Court of Cassation (France) asked the Court of Justice of the European Union (CJEU) whether Google Search fell within the definition of an 'information society service'.[7] The Court ruled that "*An internet referencing service constitutes an information society service consisting in the storage of information supplied by the advertiser*". The court also emphasized that for a service to fall within the definition of an information society service, there must be evidence that "*service features all of the elements of that definition*".[8]

Also, The UK High Court in 2009 asked the CJEU to provide a preliminary ruling on a number of questions in L'Oreal v eBay (2011).[9] L'Oreal commenced litigation against eBay and sellers on eBay for selling L'Oreal products without L'Oreal's consent. One question that the court considered

[6] United Kingdom Government Guidance, The e-Commerce Directive and the UK, last accessed on 23 November 2022 at: https://www.gov.uk/guidance/the-ecommerce-directive-and-the-uk

[7] Judgment of the Court (Grand Chamber) of 23 March 2010. Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08). ECLI:EU:C:2010:159, available at: https://curia.europa.eu/juris/liste.jsf?num=C-236/08

[8] Judgment of the Court (Grand Chamber) of 23 March 2010. Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08). ECLI:EU:C:2010:159, available at: https://curia.europa.eu/juris/liste.jsf?num=C-236/08, para. 106

[9] Judgment of the Court (Grand Chamber) of 12 July 2011. L'Oréal SA and Others v eBay International AG and Others. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. ECLI:EU:C:2011:474, available at: https://curia.europa.eu/juris/liste.jsf?num=C-324/09

concerned eBay's potential liability. The UK High Court accepted that eBay as the operator of an online marketplace was an information society service.

As discussed below, the internal market clause is a key principle of the e-Commerce Directive since it ensures that the service providers are subject to the Member State where they are established, but not where the service is being provided. As such, if a service provider is, e.g. based in Portugal, it can offer its services throughout the EU without the specifics of each Member State. The Directive also exempts intermediaries from liability to the extent they can fulfil certain requirements, in particular that they did not have an actual knowledge of the contents. Overall, the liability exemption, as mentioned below, only covers services that play a neutral, merely technical and passive role towards the hosted content.[10]

2.2 Internal Market

The e-Commerce Directive includes an internal market clause,[11] which establishes a country of origin principle, similar to the passporting principle in financial services, meaning that there is freedom of providing online services across the members of the European Union. The principle provides that online service providers are subject to the rule of the Member State where they are established rather than the rules of the Member State where the service is accessible. Member States must therefore avoid applying national legislation since the service provision relates to EU law. This principle is similar to

[10] Judgment of the Court (Grand Chamber) of 12 July 2011. L'Oréal SA and Others v eBay International AG and Others. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. ECLI:EU:C:2011:474, available at: https://curia.europa.eu/juris/liste.jsf?num=C-324/09, paras. 106-124.

[11] Art. 3 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

the concept of the national treatment principle under World Trade Organization rules, meaning that a foreign product or a service should not be treated more or less favorably than a domestic product or service (e.g. through the imposition of additional taxes or duties, etc.).[12] This clause is imperative in preserving market cohesion and allowing service providers to offer their services across the EU, without needing to worry about specific protectionist policies.

In its simplest form, the "country of origin" principle means that as long as a business complies with the provisions of the e-Commerce Directive, it can ignore the laws of other member states that touch upon the same subject matter.

It is common practice for EU legislation to offer a derogation from the general principle, and this is no exception, since it allows EU member states to derogate from the general principle if the measures are:

(1) necessary for reasons of public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,

(2) the protection of public health,

(3) public security, including the safeguarding of national security and defense,

[12] For a general description of the World Trade Organization practices see: https://www.wto.org/english/tratop_e/tariffs_e/tariffs_e.htm

(4) the protection of consumers, including investors.

Copyright and certain other intellectual property rights are also excluded from the scope of the country of origin. The same applies to real estate transfers and unsolicited commercial emails (e.g. spam).[13]

The e-Commerce Directive also provides for freedom of establishment for information society service providers (Art. 4), and lays out the basic rules that apply to e-Commerce and online services, including electronic contracts and general obligations towards consumers.[14]

2.3. Service Providers

However, the Directive does not provide for liability for service providers no matter what; rather, it recognizes limited liability exemptions, meaning that certain intermediary service providers are exempted from liability for thirty party content. The e-Commerce Directive provides specific types of activities that may, under certain conditions, be exempted from liability, in particular: mere conduit; caching; and hosting. These service providers are also relevant in the Digital Services Act, as we will discuss later on in the working paper.

Service providers, whether involved in e-commerce or not, must provide certain minimum information. The requirements vary from one country to the other, however in general service providers are required to provide the following in the form of a notice to individuals:

---

[13] Art. 5-11 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[14] Art. 5-11 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

- The name of the service provider, easily accessible;
- The geographic address of the service provider;
- The details of the service provider including his/her email address, or an alternative means of communication;
- Details of a register, including any registration number;
- The company's registration number;
- The particulars of a supervisory authority;
- Details of a professional body or similar institution with which the service provider is registered;
- A VAT number;
- Clear and unambiguous pricing.[15]

With respect to service providers in particular, the e-Commerce Directive makes reference to mere conduit, caching, and hosting providers:

Mere Conduit. The e-Commerce Directive defines a mere conduit as an "*information society service is provided that consists of the transmission in a communication network of information provided by*

[15] Art. 5 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted".[16] To qualify as a mere conduit, the provider most not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission. The acts of transmission include the automatic, intermediate and transient storage of the information transmitted with respect to carrying out the transmission in the communication network.[17]

Caching. The e-Commerce Directive also exempts caching service providers from liability. Caching is defined as the process whereby "*an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for 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 of the service upon their request*".[18] The liability exemption again comes under certain conditions, in particular that the provider does not modify the information; that the provider complies with conditions on access to the information; the provider complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry; the provider does not interfere with the lawful use of technology; and the

[16] Art. 12 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[17] Art. 12 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[18] Art. 13 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

provider acts expeditiously to remove or disable access to the information it has stored upon obtaining actual knowledge of the fact.[19] Overall, for the liability exception to apply, caching services must have a hands off approach, meaning that they do not actively make any decisions or otherwise define how and why data is being processed, and further that once they become aware and obtain knowledge, they act expeditiously in line with legal requirements.[20]

Hosting. The e-commerce Directive also includes exceptions regarding hosting, which is probably the most discussed provision of the directive. The directive defines hosting as the instance where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service. There are certain conditions attached to this, in particular that (1) the provider does not have an actual knowledge of illegal activity or information and, regarding claims for damages, is not aware of factors or circumstances from which such illegal activity is apparent; or (2) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.[21]

The key issue with these exceptions is that the notions of "actual knowledge", "reasonable expectation" etc. are terms of art, meaning that they have often led to extensive case law that tries to

[19] Art. 13(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[20] Art. 13(2) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[21] Art. 14(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

define them in a meaningful way. In a notable difference compared to the DSA, the e-Commerce Directive does not set out specific procedural obligations of notice and takedown, even though the Member States can separately establish their own conditions.[22]

2.4 No general monitoring obligation

Article 15 of the e-Commerce Directive is one of the most debated ones since it prohibits that the Member States impose any general monitoring obligations on online intermediaries.[23] In practice, this means that it is prohibited to require from intermediaries that they seek facts or circumstances regarding illegal activity. Service providers are not supposed to be in a fact-finding mission to actively find illegalities. However, the Member States may ask information society service providers to inform the public authorities of alleged illegal activities undertaken or information provided by recipients of their service.

In practical terms, it is normally accepted that if website operators monitor the content on their servers, they are at greater risk that they will be treated as publishers for that information. Extensive case law has provided that service providers do not have the obligation to monitor the content of their services.

[22] Art. 14(2) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[23] Art. 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

3. Relevant legislation in the US

The US has limited, and relatively fragmented regulation about the topic of online platform regulation. For instance, the US Code S. 230 on the protection for private blocking and screening of offensive material acknowledges the importance, potential and contribution of the internet, while stressing the importance for efficient policy that promotes development and preserves the free market character of the Internet. As such, S. 230 introduces certain principles, for instance:[24]

- Treatment of publisher or speaker: No provider/user of an interactive computer service is to be treated as the publisher/speaker of any information provided by another information content provider;
- Civil liability: No provider/user of an interactive computer service shall be held liable if:
    - It takes any action in good faith to restrict access/availability of material that the provider or user considers inappropriate; or
    - Any action taken to enable or make available to information content providers the technical means to restrict access to material.

Section 230 also introduces certain provisions on obligations of interactive computer services, namely that a provider of such service shall provide the service in a manner that the provider considers appropriate, notify customers about parental control protections, and otherwise limit harmful access to minors.

[24] Section 230, Protection for private blocking and screening of offensive material, available at: https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)

While certain proposals are geared towards expanding the scope of applicability, certain alternatives exist in other jurisdictions. The DSA for instance uses co-regulatory mechanisms to achieve its goals, and tailors the mechanisms to large platforms.[25]

In the road to regulation, the US Digital Trust and Safety Partnership (DTSP) was founded in 2020 as an industry initiative that aims to build best practices (similar to codes of conduct) and subsequent internal and third party assessments. DTSP is primarily industry-based, and it has released its first iteration of best practices that were designed as five commitments to product development, governance, enforcement, improvement and transparency. As such, with or without legislation, institutions like DTSP can build these mechanisms, or be partners in co-regulatory mechanisms.

In May 2020, former President Trump issued an executive order on the Communications Act of 1934, as amended (Section 230). Section 230 creates federal immunity for providers and users of "interactive computer services", generally preventing said platforms from being held liable for hosting content that someone else created.[26] The provision has allowed the growth of online platforms that host user-generated content. Certain policymakers also argue that Section 230 has allowed social media platforms to exert political bias. In October 2020, the Chairman of the Federal Communications Commission expressed an interest to move forward to clarify Section 230. [27]

---

[25] Wheeler, T. (2022). "US regulatory inaction opened the doors for the EU to step up on internet", available at: https://www.brookings.edu/blog/techtank/2022/08/23/the-digital-services-acts-lesson-for-u-s-policymakers-co-regulatory-mechanisms/

[26] Executive Order 13925, (2020). "Preventing Online Censorship," 85 *Federal Register* 34079-34083.

[27] Brannon, V.C. et al., (2020), Congressional Research Service Legal Sidebar LSB10484, *UPDATE: Section 230 and the Executive Order on Preventing Online Censorship*.

In December 2020, the Federal Trade Commission (FTC) launched a study of social media and streaming platforms, specifically focusing on how such platforms "collect, use, and present personal information, their advertising and user engagement practices, and how their practices affect children and teens".[28]

In July 2021, President Biden signed the "Executive Order on Promotion Competition in the American Economy". The Congress has also acted towards this direction: the Senate introduced the American Innovation and Choices Online Act, geared towards regulating big tech companies.[29]

Separately, Members of the US Congress and other stakeholders are scrutinizing the role that social media played in recent civil justice and political protests. As a result of this investigation, several bills have been introduced to reform Section 230 (e.g. H.R. 277, S. 299).[30]

A noteworthy element is that the United States has recently limited the liability of internet service providers and information content providers in recent trade agreements, for instance the US-Japan Agreement on Digital Trade and the US-Mexico-Canada Agreement. This is in line with Section 230.76. This will probably have an impact on future trade agreements as well between the US and its trading partners. At the same time, the modernization of certain multilateral trade agreements, including the General Agreement on Trade in Services (GATS) will be largely affected by the US's

[28] Federal Trade Commission, (2020), *FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information*.

[29] Tracy, R. (2022), Senate Panel Approves Antitrust Bill Restricting Big Tech Platforms, available at: https://www.wsj.com/articles/senate-panel-approves-antitrust-bill-restricting-big-tech-platforms-11642701487.

[30] Frenkel, R. (2021), "The storming of Capitol Hill was organized on social media," *New York Times*, available at: https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html

stance, particularly in the current World Trade Organization (WTO) landscape that is facing a deadlock as the result of the Dispute settlement Mechanism Appellate Body paralysis.

The USTR also annually reports on markets that facilitate substantial trademark counterfeiting and copyright piracy. In 2020 for instance, the report focused on the growth of digital platforms, particularly in facilitating trade in counterfeit and pirated goods, and how such platforms have made it more difficult to direct such goods.[31]

4. Time for a Change: the DSA

Several things have changed since 2000, including the scope and nature of the services that online platforms provide. Also, new types of services do not fit the description of a service provider, for instance online advertising services. Further, the fact that the e-Commerce Directive is a directive, meaning that it has a minimum harmonizing effect, has led countries to significantly diverge and impose stricter, or more lenient, standards for service providers depending on their domestic priorities.

The Digital Services Act (DSA), initially proposed by the European Commission, was designed in a way that builds on the e-Commerce Directive to address new challenges online. The DSA is structured to address the changes and challenges that have arisen over the past years, particularly regarding online intermediaries.

[31] Executive Order 13960, (2020), "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," 85 FR 78939 *Federal Register* 78939-78943.

The DSA is therefore aimed at modernizing the e-Commerce Directive regarding illegal content, transparent advertising, and disinformation. It was submitted at the same time as the Digital Markets Act (DMA), notably striking the first significant nexus between data protection and competition law. The DSA/DMA were first submitted on 15 December 2020.

On 5 July 2022 the European Parliament approved the DSA along with the DMA, whereas in September 2022, the Council of the European Union adopted the DSA. The rules are expected to apply fifteen months after coming into force, or on 1 January 2024. Online platforms and search engines, among others, will need to comply with their obligations four months after the European Commission has designated them as such.

The expressed purpose of the DSA is to update the EU's legal framework for illegal content on intermediaries, in particular by modernizing the e-Commerce Directive adopted in 2000. The DSA tries to harmonize different national laws in the EU that have emerged at a national level to address illegal content. In practice, it is expected that the DSA will set new rules regarding illegal content, transparent advertising and disinformation.

The Digital Services Act (DSA) was published in the official journal of the European Union on Thursday 27 October 2022, and entered into force 20 days afterwards, i.e. on 16 November 2022.[32] In the meantime, the European Commission has already been preparing on how the new rules will apply to the companies in-scope.

[32] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

Time is of the essence when complying with the DSA, particularly for the so-called very large online platforms and very large online search engines, that need to disclose the number of their active EU users by February 2023. To the extent that a platform or search engine has more than 45 million users in the EU, they will need to follow certain rules regarding illegal content, disinformation, and algorithm adaptation. Timing is less strict for smaller online platforms and digital companies like cloud services, which have until 2024 to prepare.

The DSA introduces a legal framework for content, products, and services offered by intermediary services providers. It steps up the compliance requirements since it creates new obligations for all intermediary service providers, including online platforms. The regulatory burden imposed by the DSA overall varies depending on the type of services offered. In its first significant draft of December 2020, the DSA followed a layered approach with building blocks of obligations, depending on the size and function of an intermediary service. The DSA in particular covers four types of service providers: (1) intermediary services, including "mere conduit" and "caching" services; (2) hosting services (e.g. cloud and web hosting services); (3) online platforms (e.g. online marketplaces, app stores, and social media platforms); and (4) "very large" online platforms, which are defined as platforms reaching more than 10 percent of the then current EU population, currently estimated at 45 million users. Since the DSA obligations are working in building blocks, the more data heavy a company is, the more steps it will need to take to comply, while having complied with all the previous steps.[33]

4.1. DSA Background

[33] See Section 1, 2, 3, 4 and 5 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN that work in building blocks

The Digital Services Act largely builds on the Commission Recommendation 2018/314, which had signaled that a relevant EU regulatory initiative was in the works, at the same year when the GDPR entered into force in the EU, another landmark legislation for the EU. The European Commission launched a public consultation to gather evidence in the course of 2020. The European Commission also published an impact assessment, which is customary for this type of legislative acts.

The DSA is aimed at enhancing content moderation on social media platforms, pursuant to increasing calls regarding illegal content. Key innovations of the DSA include new obligations on intermediaries, content moderation obligations, and the cooperation and enforcement between the European Commission and national authorities.

The DSA is inheriting the e-Commerce Directive's provisions regarding liability, meaning that companies which host other's data, and intermediaries are not liable for the content of the information they host, unless they have actual knowledge that the content is illegal, or if they do not act in accordance with the law once they are alerted to the fact that they host illegal content. This notion is known as "conditional liability exemption", meaning that intermediaries and hosting services are not always exonerated from liability, but rather under specific conditions.[34]

The DSA also introduces far-reaching new obligations on platforms, including certain that aim to disclose to regulators the rationale and modus operandi of their algorithms, in the context of

[34] Recital 16 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

transparency. On the same note of transparency, related obligations are aimed at explaining how decisions to remove content are taken and why certain advertisements are directed to specific users.

The DSA is structured in a layered manner, meaning that the most detailed obligations only apply to platforms with a significant number of users in the European Union (i.e. more than 45 million users). However, even smaller platforms will have obligations, it is just that they will not be as onerous/detailed as the requirements prescribed to large platforms. The building block approach is therefore a proportionate way to avoid "one-size-fits-all" compliance, but rather to comply in accordance with the actual strength/size of the company's presence in the EU. It is noteworthy that European policymakers felt a greater sense of urgency to move the legislation forward in a call to ensure that major tech platforms were transparent and properly regulated.

The DMA and DSA fit in the broader European Digital Strategy announced by the European Commission. The Commission's intention was primarily to review the rules applicable to digital platforms and propose a new framework that ultimately aims to booster the single market for data and ensure Europe's global competitiveness. These initiatives, taken together, want to ensure that data can flow in accordance with the principles of competition law and data protection. The DMA therefore outlines a new enforcement framework, whereas the DSA regulates the liability of platforms and imposes new obligations with respect to content moderation, due diligence of illegal content, and transparency of advertising.

The European Commission called particularly on the importance to modernize/substitute the e-Commerce Directive in key issues that were not adequately defined and regulated, for instance how platforms should exercise content moderation, the taking down of illegal or harmful content, and the

exercise of due diligence to their services. Also, the European Commission's antitrust framework, albeit extensive, was drafted a while ago, and therefore was not tailored to challenges pertinent to the digital economy, or otherwise in line with large digital platforms.

It is noteworthy that the rise in prominence of acts like the DSA/DMA does not go unnoticed in countries. For instance, Germany is waiting the parliamentary adoption of a competition code regarding undertakings, whereas the UK is contemplating, through the Online Harms proposal, significant fines to companies of up to 10 percent of their global revenue if they fail to stop illegal and harmful content from reaching their online users.[35]

4.2. Evolution of the DSA: The First Draft

Obligations for every service provider. The initial draft of the DSA recognized certain obligations that would apply to every service provider:

(1) Publish annual reports on any content moderation they engage in. This adds to the reporting requirements that companies already have since they will need to explain and detail any relevant content moderation activity that happens as part of the service provision;[36]

[35] In latest update, the UK government has said that the Online Safety Bill will be introduced "as soon as possible" (February/March 2022), available at: https://commonslibrary.parliament.uk/research-briefings/cbp-8743/#:~:text=The%20Paper%20proposed%20a%20single,enforce%20compliance%20with%20the%20duty.

[36] Art. 15(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

(2) Enforce their terms and conditions including regarding content moderation. The DSA imposes a stricter obligation with respect to content moderation since it is requiring companies to diligently enforce their terms and conditions. This is, ultimately, a word of art and remains to be seen how it will play out in practice. However, at a high-level, this is particularly important for cases of fake news, which on its own is an increasing and aggravating force.[37]

(3) Cooperate with national authorities and follow orders to act against illegal content (e.g. take down orders for hate speech or illegal content). The cooperation requirement is way more detailed than what was previously the case under the e-Commerce Directive. Also, the DSA requires that service providers react expeditiously in take down orders for hate speech or illegal content.[38]

(4) Have a point of contact and, where necessary, and EU representative. Providers with no presence in the EU are required to appoint an EU representative- unlike with EU representatives under the General Data Protection Regulation (GDPR), regulators can hold the EU representative liable for any breach of the DSA. [39]

Hosting services. Hosting service providers have certain obligations on top of the general obligations, in particular to put online mechanisms in place when needed so that users and companies can notify

[37] Art. 14 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[38] Art. 14-15 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[39] Art. 13 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

them of any illegal content. This is a step up from the existing regime under the e-Commerce Directive, since these mechanisms will arguably increase enforcement and also complaints from individuals. Having an easy-to-access and user-friendly mechanism will likely lead to more individuals raising complaints. Hosting service providers must also inform users and states of the reasons for taking down any content or when they suspend a user's account as a result of repeated spread of manifestly illegal content.

Online platforms. The online platforms will need to comply with the general obligations and the hosting services obligations, and on top of that establish an internal complaint-handling system where users can contest the platforms' decisions. In practice, this means that users can disagree with a specific take down of fake news action, and they must have a means to complain accordingly.

Online platforms would also need to establish the so-called "trusted flaggers", which are entities that can flag any illegal content to the online platforms. These trusted flaggers will be able to alert the platform of illegal content, and add a flair to grassroots approach since the control of illegal content will not only be from top to bottom, but vice versa as well. The online platforms would need to take measures against misuse, for instance suspending a user's account for a reasonable period of time if the user repeatedly transmits "manifestly illegal content" through the platform, such as the sale of counterfeit goods.[40]

[40] Art. 22 and Art. 23 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

Online platforms also need to maintain a "Know Your Business Customer" (KYBC) registry before allowing other companies to offer goods and services on the platform, as well as notify the authorities about any suspicion of criminal offense.[41]

Online platforms will also have to provide detailed information about the ads shown to users. This includes ensuring that users are aware and can easily recognize sponsored content, as well as detailed information about the ads shown to users. Similar to a nutrition label, consumers should be able to clearly recognize whether an ad is sponsored, which is the responsible entity, and any other meaningful information about the specific variables for showing the ad to a specific user.[42]

Very large platforms. In addition to all the requirements mentioned above, very large platforms would further need to conduct annual risk assessments about the use of their services. They would also be subject to annual audits from independent auditors with respect to their compliance with the DSA. They would further need to appoint company officers who are dedicated to DSA compliance, and provide access to data that is necessary to prove compliance with the DSA upon request from national authorities or the European Commission.[43]

---

[41] Art. 24 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[42] Art. 26 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[43] Art. 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

Finally, very large platforms will be required to provide a publicly available list of advertisements along with information for each ad and the specific parameters used to target specific groups of individuals.

Other significant points.

The DSA does not establish a general monitoring requirement, in line with the e-Commerce Directive, or a relevant fact-finding obligation for intermediary service providers. However, if providers become aware or are otherwise alerted to the fact that there is illegal content, they must act without undue delay to remove or disable access to the illegal content. The DSA also includes provisions aimed to incentivize intermediary services to conduct voluntary investigations and detect illegal content- it does so by shielding them from liability for findings that come as a result of these investigations.[44]

The DSA also creates a one-stop-shop mechanism for intermediary service providers with an EU establishment or an EU representative. National authorities are responsible for supervising the EU operations of companies established in their territory. The DSA also creates the European Digital Services Board, which will be responsible for ensuring enforcement of the DSA across the EU. The European Commission may also impose fines for very large platforms of up to 6 percent of the company's total turnover, or periodic penalty payments of up to 5% of the average daily turnover.

[44] Art. 7 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

Penalties imposed by national authorities could also be similar. Finally, civil society organizations and NGOs can lodge class action lawsuits in cases of DSA infringements, based on the EU Collective Redress Directive.

4.3. The EU Parliament and EU Council Versions

The EU Parliament and EU Council adopted their own versions of the DSA and the DMA, which led to the trilogues (negotiations between the EU Commission, Parliament and Council) to agree on the final version of these laws.

Changes to the DSA in the European Parliament's version:

- *Certain targeted advertising activities prohibited*. The European Parliament's version prohibits (i) the display of targeted advertising to minors and (ii) the targeted advertising by using sensitive personal data. This means that online platforms would need to review their age-gating procedures and ensure that no targeted ads are shown to minors, as well as ensuring that the advertising mechanisms are not using any sensitive data.

- *Due diligence in enforcing T&Cs.* The European Parliament's version requires online platforms to use due diligence to identify traders offering illegal products and services, including through random checks.

- *Obtain GDPR consent*. Where platforms need to obtain GDPR consent, the European Parliament prohibits the use of dark patterns, meaning methods that are designed to manipulate

the user into agreeing to certain terms (e.g. by using a bold font or more attractive colors).

Changes to the DSA in the Council's version:

- *Online search engines are expressly in DSA's scope*. To avoid any confusion, the Council's draft clarifies that online search engines fall within the scope of the DSA, whereas under certain criteria they are considered very large search engines.

- *Centralized enforcement in the EC*. The Council's draft recognizes that the European Commission is primarily responsible for enforcing the DSA for very large online platforms and search engines.

4.4. Final Version

On 27 October 2022, the DSA was published in the Official Journal of the European Union. The final legislation spans 102 pages and introduces a comprehensive framework for regulating digital services in the EU. Key obligations that were introduced in the initial drafts made it all the way to the final version, including regarding content moderation, online advertising, and trader transparency.

Based on the published timeline, companies will have until February 17, 2024 to comply with the DSA. Very large online platforms (VLOPs) and very large online search engines (VLOSES) will need to step up their compliance processes since the DSA will apply four months after their respective designation, which would take place as early as in the first half of 2023. The DSA is complementing the Digital Markets Act (DMA) which entered into force on 1 November 2022.

Key requirements

The DSA complements, but does not replace, other legislation that introduces moderation and transparency requirements. For instance, the regulation on terrorist content requires platforms to remove terrorist content within one hour of receiving a removal order.[45] Other relevant laws include regulations on political advertising and child sex abuse material. It also does not replace the existing eCommerce Directive, but rather builds on it. It adds to the trader transparency requirements in the eCommerce Directive.

The scope of the DSA has remained the same as in the initial drafts since it applies to "intermediary services", a catch-all term that includes providers of conduits, caching services, and hosting services (including online platforms and search engines).[46] It is based on a building block mode, meaning that the obligations that a company will need to observe are commensurate to its size, and how data heavy it is. For instance, online platforms or search engines that have more than 45 million users in the EU may be designated as VLOPS or VLOSEs by the European Commission, which would bring them to the highest degree of regulation directly by the European Commission.

The final draft also maintains the extra-territorial reach of the DSA, meaning that if a company is not established in the EU but offers its services to individuals or companies in the region, it will need to comply with the DSA requirements and appoint a representative. The DSA representative is different

[45] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM/2018/640 final

[46] Art. 3(g) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

than the GDPR representative since he/she can be held liable for noncompliance with the DSA, and therefore this is a significant role.

Core obligations. Intermediary service providers are subject to some minimum requirements irrespective of their size:

- *Respond to take down orders.* Service providers must diligently respond to orders issued by national judicial or administrative authorities, such as take down orders, or information regarding individual recipients of a service to be provided.[47]

- *T&Cs.* Every service provider must enforce its T&Cs, including with respect to content moderation activities, algorithmic decision making. They must also provide details of complaint procedures. Transparency is key under the new regime, meaning that any changes must be communicated to users.[48]

- *Annual reports.* Service providers must publish reports on their content moderation on an annual basis. The reports should be publicly available and easily accessible also in connection with the nature of the service that is being offered.[49]

---

[47] Art. 13 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[48] Art. 15 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[49] Art. 14 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

- *Notice and takedown.* Every hosting service[50] must implement a means for users to flag illegal content. The notifier must be made aware of the result of a notice once it's been reviewed, and the affected user must also be informed about the specific action taken, and the reason for this.

Online platforms

Online platforms are also required to:

- *Comply with advertising requirements.* The DSA prohibits targeted advertising based on profiling of sensitive data or children's data, therefore onboarding the recommendations of the European Parliament. Additionally, online platforms need to display details about the ad, including who paid for it, and the main variables that determine who sees the ad.[51]

- *Use of recommender system*. Online platforms that use automated systems, even partly to recommend content, must explain how is content recommended, including the criteria used to determine what information is being presented. Online platforms must also disclose relevant options for the user to modify these parameters.[52]

[50] Art. 16 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[51] Art. 26(3) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[52] Art. 27 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

- *Taking onboard the European Parliament's suggestion*, the DSA prohibits that online platforms design and organize their interface in a way that seeks to shape user behavior in a particular way, for instance by using a different font size or color for one option, or for using bold language.[53]

- *Complaint mechanism and dispute settlements*. Online platforms must also offer a complaint mechanism so that flaggers and other affected users can challenge content moderation decisions (e.g. decisions leading to remove or disable access to content). The online platforms have even further flexibility in the sense that if they find a user repeatedly providing clearly illegal content, or submitting unfounded notices or complaints, they can issue warnings to these individuals and, if the issue persists, eventually to suspend the user from the service.[54]

- *Know your customer requirements*. Online marketplaces must collect background information from traders before permitting them to use their service. Similarly, traders will need to provide information such as payment account details before they can offer goods on the online marketplace.[55]

[53] Art. 25 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[54] Art. 21 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[55] Art. 30 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

- *Notify customers of illegal products*. Taking onboard one more recommendation of the European Parliament, the final text of the DSA requires online marketplaces to take reasonable steps to check official online databases to ensure that products/services on offer on their platforms are not illegal. If they become aware of any illegal products/services, they will need to promptly notify the users. Where this is not possible, they need to display a public notice to that effect.[56]

- *Comply by design*. Online marketplaces will need to design their interface to allow traders to comply with their respective obligations, and clearly identify products and services that they offer to EU customers.[57]

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs).

On top of all the previously mentioned requirements, the final version of the DSA recognizes that VLOPs ad VLOSEs need to boost their transparency requirements by creating an accessible ad search function on their user interface. This tool should be searchable, with multicriteria functions, allowing users to discover information including the content of the ad, how long it was presented for, whether the ad is targeting a specific group or not, and what are the respective criteria for excluding/including groups from viewing the ad accordingly. The information must remain available to the users for at

[56] Art. 30(2) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[57] Art. 31 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

least one year, meaning that users should have access to all the information they need for a reasonable period of time.[58]

VLOPs must also offer users at least one option for a non-personalized service, which means a recommender system that is not based on profiling of personal data, but is more a "plain vanilla" version of the service.

VLOPs and VLOSEs must provide the users with a concise, easily accessible, and machine readable format summary of their T&Cs. The terms should be published in the official language of each EU country where they offer services, which would add even further to the complexity of the issues that they would need to navigate as part of the DSA requirements.

National regulators will regulate intermediary services, coordinated by one Digital Services Coordinator in each Member State. VLOPs and VLOSEs will be regulated directly under the European Commission. The DSA also creates a European Board for Digital Services designed to help ensure consistent enforcement of the DSA across the EU. Finally, fines for non-compliance can reach up to a maximum of six percent of a company global revenue.

4.5. The US angle to the DSA

The US has overall been following these latest regulatory/legal developments in Europe, while assessing the ramifications for US businesses. At the same time, the US government is exploring its options, including if the US will launch similar regulatory initiatives. At the core of the debate, the US

[58] Art. 32 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

is contemplating whether such regulations will instigate growth, or whether they will halt innovation and deter entrepreneurs from kicking off new initiatives.

For instance, at a letter directed to President Biden, the Co-chairs of the Digital Trade Caucus urged him to work with the EU to "ensure non-discriminatory treatment for firms on both sides of the Atlantic."[59] In particular, the co-chairs raised the concern that the DSA and the DMA would heavily regulate large technology firms, and levy significant fines for non-compliance. Based on their estimates, up to 19 million American workers could be impacted by these regulatory changes. When the DSA was still a draft, members of the Congress had asked President Biden to raise these concerns with the EU before the legislation got finalized.[60]

Notwithstanding the above, the US is generally in favor of further regulating online platforms, the key question being the level and depth of such regulation. In the vein of regulatory enforcement, President Biden, in his State of the Union address, declared that "*we must hold social media platforms accountable for the national experiment they're conducting on our children for profit*".[61]

From the outset, the DSA and DMA are another example of EU regulations that practically enjoy extraterritorial application due to their nature and scope of application. The GDPR kicked off this trend since it required companies that may have no corporate presence in Europe to comply with

[59] Hellmann, A. (2021), "Biden must push back against EU's discriminatory digital policies", available at: https://www.atr.org/biden-must-push-back-against-eus-discriminatory-digital-policies/

[60] Hellmann, A. (2021), "Biden must push back against EU's discriminatory digital policies", available at: https://www.atr.org/biden-must-push-back-against-eus-discriminatory-digital-policies/https://www.atr.org/biden-must-push-back-against-eus-discriminatory-digital-policies/

[61] Alegre, S. (2022), "Biden may change the game in Big Tech regulation", available at: https://techonomy.com/biden-may-change-the-game-in-big-tech-regulation/

European data protection laws if they process EU personal data. It recognized the changing nature of service provision and introduced an extraterritorial element that practically led every company that offers services in Europe to be subject to European regulations. The same principle applies to the DSA/DMA since Europe is requiring companies that are either gatekeepers, or otherwise provide their services as online platforms, to comply with EU-made rules irrespective of their location. As such, in practice this ends up being an EU regulation that has a heavy US focus as well given the nature of the services it regulates. In a way, the EU has moved swiftly to regulate activity taking place over the Internet, irrespective of the physical location of the service provider.[62] The de facto compliance with the GDPR by US companies is a solid indication/predictor of how the DSA/DMA will also be welcomed in the region. The EU is therefore generally considered to hold the first-mover advantage in policy matters, and in this particular case the DSA and the DMA. [63]

In practice, the EU has a competitive advantage of exporting its legal institutions and standards to the rest of the world, due to its advance regulatory infrastructure. Companies that want to do business with the EU must therefore adjust their practices, or forego entry to the EU market altogether.[64] It is often easier and less costly to adjust/standardize the global practices according to the EU standards, rather

[62] Wheeler, T. (2022). "US regulatory inaction opened the doors for the EU to step up on internet", available at: https://www.brookings.edu/blog/techtank/2022/03/29/u-s-regulatory-inaction-opened-the-doors-for-the-eu-to-step-up-on-internet/

[63] Wheeler, T. (2022). "US regulatory inaction opened the doors for the EU to step up on internet", available at: https://www.brookings.edu/blog/techtank/2022/03/29/u-s-regulatory-inaction-opened-the-doors-for-the-eu-to-step-up-on-internet/

[64] Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1, 1 (2012).

than creating different buffer zones based on various geographies. This means that, in practice, the EU standard becomes a de facto global standard.

5. The Digital Markets Act (DMA)

The Digital Markets Act has been approached as a package agreement along with the Digital Services Act, and has primarily focused on the "gatekeepers". In contrast to the DSA which includes service providers irrespective of their size, the DMA only regulates the largest platforms. This is good news for several companies that do not need to comply with the DMA, however its complicated rules mean that certain service providers may need to comply indirectly because of their service provision/dependency with regulated gatekeepers. Ultimately, the DMA regulates the conditions and processes for gatekeepers to share data with their partners, meaning that certain restrictions will flow down to companies that are collaborating with large online platforms.

In terms of timing, the DMA entered into force on 1 November 2022, and the gatekeepers need to notify the European Commission within two months starting in Spring 2023, which is when the majority of DMA's provisions will become applicable. Gatekeepers will overall have six months to comply with the relevant rules.

The DMA is part of the broader EU digital agenda, and is a pioneer legislation in that it overlaps with other areas of law including data protection.

5.1. Scope

The DMA applies to platforms that are offering Core Platform Services (CPS) and that have been designated as gatekeepers by the European Commission. The fact that the European Commission classifies a platform as a gatekeeper does not mean that a platform cannot argue against such classification.[65] The notion of classifying a platform as a gatekeeper depends on certain metrics, in particular:

- If a company has an annual revenue in the European Economic Area at least 7.5bn in each of the last three financial years, or average market capitalization or fair market value at least 75bn, and provides the Core Platform Services in at least three EU member states;

- Strong intermediary position: if the platform operates a Core Platform Services with at least 45 million monthly active end-users established in the EU, and more than 10,000 yearly active business users established in the EU in the last financial year; and

- Has or is expected to have entrenched a durable position in the market, for instance when the company meats the other criteria in each of the last three financial years.[66]

These thresholds are non-binding, meaning that the European Commission reserves the right to designate gatekeepers even in cases where these criteria are not met. The European Commission

[65] Recital 23 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[66] Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

overall affords itself adequate flexibility to designate and upkeep the classification of gatekeepers as it deems fit.[67]

In terms of the actual CPS, the DMA covers ten core platform services:

- online intermediation services;
- online search engines;
- online social networking services;
- video-sharing platform services;
- number-independent interpersonal communication services;
- operating systems;
- cloud computing services;
- advertising services;
- web browsers;

[67] Art. 3 and Art. 4 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

- virtual assistants.[68]

Out of these ten core platform services, eight were part of the European Commission's initial proposal, and two core platform services (virtual assistants and web browsers) were added to the list initially proposed by the European Parliament.[69]

The inclusion of further providers in the list of CPS is justified based on broader developments, including findings of the sector inquiry into the consumer Internet of Things, which looked into issues of voice assistants, and recent enforcement experience and broader developments related to web browsers.

In terms of the gatekeeper designation, the classification is reviewed regularly, and in any event at least every three years.

5.2. Key obligations

The Digital Markets Act (DMA) establishes a series of obligations that gatekeepers will need to implement in their daily operations to ensure fair and open digital markets. Key obligations imposed on the gatekeepers include:

[68] Art. 2(1) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[69] Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets, 31 October 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349

- Allow end users to easily un-install pre-installed apps or change default settings on operating systems, virtual assistants or web browsers that steer them to the products and services of the gatekeeper and provide choice screens for key services;[70]

- Allow end users to install third party apps or app stores that use or interoperate with the operating system of the gatekeeper;[71]

- Allow end users to unsubscribe from core platform services of the gatekeeper as easy as it is to subscribe to them;[72]

- Allow third parties to inter-operate with the gatekeeper's own services;
- Provide the companies advertising on their platform with access to the performance measuring tools of the gatekeeper and the information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper;

- Allow business users to promote their offers and conclude contracts with their customers outside the gatekeeper's platform;

---

[70] Art. 5-8 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[71] Art. 6 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[72] Recital 63 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

- Provide business users with access to the data generated by their activities on the gatekeeper's platform.[73]

At the same time, the DMA introduces certain prohibitions for the gatekeepers, including:

- Ban on using the data of business users when gatekeepers compete with them on their own platform;
- Ban on ranking the gatekeeper's own products or services in a more favorable manner compared to those of third parties;
- Ban on requiring app developers to use certain of the gatekeeper's services (such as payment systems or identity providers) in order to appear in app stores of the gatekeeper;
- Ban on tracking end users outside of the gatekeepers' core platform service for the purpose of targeted advertising, without effective consent having been granted.[74]

5.3. Practical Implications

The European Commission will assess whether companies active in core platform services qualify as a "gatekeeper" under the DMA. Companies will assess if they meet the quantitative thresholds

[73] Art. 5 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[74] Art. 6-7 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

included in the DMA regarding gatekeepers- once they complete their assessment, they will have to provide the European Commission with information on this; the European Commission will subsequently designate as "gatekeepers" the companies that meet the thresholds in the DMA based on the information that the companies provide and pursuant to a market investigation. Within six months after a company being designated as a gatekeeper, it will have to comply with all the obligations listed in the DMA.[75]

In terms of enforcement action, if a gatekeeper does not comply with the rules, the European Commission can impose fines of up to 10% of the company global revenue or 20% in the event of repeated infringements and periodic penalty payments of up to 5% of the company's global revenue.[76] The European Commission can also impose additional remedies in cases of systematic infringements; where necessary to achieve compliance, and where there is no alternative, other equally effective measures are available, such as structural remedies, obliging a gatekeeper to sell a business or parts of it, or banning a gatekeeper from acquiring a company that provides services in the digital sector.[77]

The Digital Markets Act allows the European Commission to supplement the existing obligations applicable to gatekeepers based on a market investigation, which can also translate into a supplementary act (delegated act), or a review of the DMA. The Commission will also be able to

[75] Art. 3(10) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[76] Art. 30 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

[77] Art. 30 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

designate "emerging" gatekeepers that can make services tip to their advantage. The instrument allows a flexible approach to keep pace with developments in the fast-evolving digital sector.

5.4. Timeline of enforcement

The European Commission will be the enforcer of the DMA. Centralized enforcement matches the Commission's priority regarding competition enforcement. The DMA entered into force on 1 November 2022, and will start applying as of 2 May 2023. Concerned gatekeepers would need to notify their core platform services to the Commission by 3 July 2023. The European Commission must assess whether the undertakings meet the threshold, and designate gatekeepers, by 6 September 2023. Following their designation, gatekeepers will have six months to comply with the DMA requirements, by 6 March 2024.[78]

5.5. The US angle to the DMA

Similarly to the discussion and the concerns raised above regarding the DSA, the DMA has received lukewarm reception in the US, particularly since it appears to be targeting (based on the scoping criteria for a company to be considered a "gatekeeper") primarily US companies. Another relevant concern is that the DMA may create roadblocks for small and medium sized enterprises (SMEs) that assist the big online platforms operate as they do. In other words, the DMA requirements may flow down to service providers that are not in-scope of the Act, but that need to comply notwithstanding so that they can provide their services to their clients who are subject to the law. This may lead to significant enforcement costs for companies in the broader technology ecosystem, and eventually

[78] Art. 3(10) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=EN

contract growth. Instead of facilitating a level playing field that is geared towards a competitive market, these regulations could make it more difficult for small companies to engage with their customers and serve the big online platforms as they are today. As an indication of the US reservations towards the impact that the DMA will have in the technology landscape, the US Chamber of Commerce issued a statement stating that "*Europe is intent on punishing successful companies that have made deep investments in Europe's economic growth and recovery*."[79]

Another key criticism relates to the fact that only a handful of European companies are regulated under the DMA. A related concern that has been raised is whether, in fact, drafting laws such as the DMA constitutes covert protectionism, in the sense that the law may be perceived as targeting primarily foreign companies, therefore introducing certain restrictions/protectionist measures only to said companies.[80] Substantially, the US concern is that only, or primarily, US companies, will be in scope of the DMA. At the same time, however, the EU's argument in favor of the DMA revolves around the fact that it is purposed to regulate the gatekeepers, meaning the largest companies that have a lion share in the digital market. The fact that most of them are based in the US does not necessarily mean that the law is designed in a way to explicitly target US companies. As such, the law is not discriminatory, but based solely on a set of quantitative criteria, as a signpost of market power.

[79] Kannengeiser, E. and Fleck, J. (2020). Europe's new legislative proposals mark a big 'first move' on tech-market power, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/europes-new-legislative-proposals-mark-a-big-first-move-on-tech-market-power/

[80] Wheeler, T. (2022). "US regulatory inaction opened the doors for the EU to step up on internet", available at: https://www.brookings.edu/blog/techtank/2022/03/29/u-s-regulatory-inaction-opened-the-doors-for-the-eu-to-step-up-on-internet/

Overall, the EU's approach with the DSA and DMA is in line with the continued EU trend of driving the digital and regulatory agenda by creating new acts and leaving the US to respond/react on an ad hoc basis.[81] This feeds into a criticism that the US is increasingly facing, in that it has fallen behind in driving innovation over the past years, and it has allowed the EU to address/fill-in this regulatory gap by imposing increasingly complicated and burdensome regulations. The failure or unwillingness to develop specific rules has left the field open for other countries to take the lead, while potentially costing the US the claim to regulatory innovation in the technology arena. Also in the field of antitrust reforms, the US has not acted as fast as the EU from a regulatory standpoint.[82]

Interestingly, the US Congress has held several hearings on the power of digital platform companies. However, in terms of actionable steps, there hasn't been much progress to follow suit. Conversely, the EU may claim that it has been forced to take action because the US has not done so until now. It remains to be seen how the US will further react in terms of regulatory initiative. For the moment, certain members of the US Congress are pushing for bipartisan legislation. For instance, the House Judiciary antitrust subcommittee chair has signaled that new laws will be introduced soon.[83] This is an effort to regulate a field that the US has raised concerns regarding the EU's rules disproportionately affecting US businesses. Any such initiative will try to address one of the key concerns, which has

[81] Kannengeiser, E. and Fleck, J. (2020). Europe's new legislative proposals mark a big 'first move' on tech-market power, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/europes-new-legislative-proposals-mark-a-big-first-move-on-tech-market-power/

[82] Nylen, L. and Stolton, S. (2022), "US slow to respond to EU's landmark tech regulation", available at: https://www.politico.com/news/2022/03/25/us-eu-digital-markets-act-00020551

[83] Nylen, L. and Stolton, S. (2022), "US slow to respond to EU's landmark tech regulation", available at: https://www.politico.com/news/2022/03/25/us-eu-digital-markets-act-00020551

also been voiced by the US Chamber of Commerce, in that the new EU rules form a policy of de facto discrimination against US companies.

6. The future of the EU-US Digital Trade based on the latest regulatory initiatives

The US and the EU are top trading partners, whereas their economic partnership has been crucial to the growth and development of the digital economy. For instance, in 2019 the US exported $196 billion worth of information and communications technology (ICT) services to the EU. Similarly, the EU is one of the most prolific and profitable regions, and therefore especially attractive for US companies.[84]

One interesting point of interconnection is whether the recent Privacy Shield invalidation (NB: currently the Data Privacy Framework is subject to review by the European Commission with a view of issuing an adequacy decision, which would make the Framework a valid way to transfer data from the EU to the US moving forward), in combination with the DSA/DMA create an even more burdensome/difficult landscape for US companies to be active in.[85]

The EU recently adopted "A New Transatlantic Agenda for Change", including a proposal for a US-EU tech and trade council to shape global tech standards and solutions. At the same time, the Data Privacy Framework has attempted to create an adequate level of data protection for transatlantic data transfers.

[84] Congressional Research Service (2021). EU Digital Policy and International Trade Report, p. 2.

[85] Kannengeiser, E. and Fleck, J. (2020). Europe's new legislative proposals mark a big 'first move' on tech-market power, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/europes-new-legislative-proposals-mark-a-big-first-move-on-tech-market-power/

At the same time, US and EU government bodies have proposed new bilateral efforts to address digital technology challenges. For instance, in December 2020, the European Commission and the EU's High Representative for Foreign Affairs and Security Policy issued a "*New EU-US Agenda for Global Change*", on the basis of the regions' common values, interests and influence. The proposed joint EU-US tech agenda includes creating a "*transatlantic technology space that can form the backbone of a wider coalition of like-minded democracies that have a shared vision on tech governance*".[86] In doing so, the EU explicitly calls out cooperation on issues of AI, data flows, online platforms, competition, taxation in the digital economy, and standards.

The EU-US Trade and Technology Council (TTC)

The EU-US Trade and Technology Council (TTC) was announced at the US-EU summit in June 2021 for the purpose of leading a "valued-based digital transformation of [Europe]". The major goals for the TTC include seeking common ground and strengthening global cooperation on technology, digital issues, and supply chains. At the same time, the TTC wishes to facilitate regulatory policy and enforcement cooperation.

Key objectives of the partnership include: (i) to ensure that trade and technology serve the EU and US societies and economies; (ii) to strengthen technological and industrial leadership; and (iii) to expand bilateral trade and investment.

[86] Press release, (2022), "EU-US Trade and Technology Council addresses common challenges and responds to global crises", available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7433

In its most recent meeting on 5 December 2033, the TTC reaffirmed the work undertaken by the ten active working groups. It also provided an update on several aspects of ongoing digital projects, including for online platforms. Notably, the US and the EU issued a first joint roadmap on the evaluation and measurement tools for trustworthy AI and risk management (AI Roadmap). The purpose of the roadmap is to inform the EU-US approach to AI risk management and trustworthy AI on both sides of the Atlantic. This initiative is also in line with the OECD and GPAI.[87]

The EU and the US are also in the process of establishing an expert task force to reduce barriers to research and development collaboration on quantum information science and technology, develop frameworks for assessing technology readiness, discuss intellectual property, and export control-related issues, and work together on these international standards.

The TTC also confirmed its plans to launch workstreams on Post-Quantum Encryption and Internet of Things (IoT), along with a preliminary focus on technical and performance standards for cybersecurity.

Another interesting development in the latest TTC meeting is the agreement on the principles of the Declaration for the Future of the Internet (DFI). The next meeting is scheduled for mid-2023 and will likely introduce even further areas of cooperation between the EU and the US.

[87] Press release, (2022), "EU-US Trade and Technology Council addresses common challenges and responds to global crises", available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7433

7. Conclusion

The DSA and DMA are overall some of the most significant developments in terms of regulatory innovation in the recent years in the EU. In combination with other acts that are still in draft form, namely the ongoing Data Act and AI Act, they set the stage for a new era of regulatory oversight for service providers and other companies that are active and data heavy.

The EU-US digital trade collaboration is also key in enhancing the dialogue and introducing regulation on both sides of the Atlantic with a view of bringing consistent and enforceable regulation. As discussed above, the US has been more reluctant in regulating online platforms, and the DSA/DMA have been criticized for targeting US businesses. At the same time, the US recognizes the importance of regulation insofar as it does not stifle innovation. In that regard, the US appears eager to continue exploring its different regulatory options while improving its trade relationship with the EU.

It remains to be seen how the DSA and DMA will be enforced in practice, as well as the ramifications of these regulations on both sides of the Atlantic. Companies have been trying to understand whether they are directly or indirectly in scope, how they can comply, and the consequences these rules will have on their daily operations. If nothing, the increasing web of European regulations makes Europe a highly complicated territory to provide services in. At the same time, these regulations signal Europe's vision to lead by example, and to have the first mover advantage in fields that are still growing, like digital platforms, Artificial Intelligence, and the Internet of Things. Only time will tell whether this regulatory experiment will be successful, or whether it will create an overly burdensome compliance landscape that will ultimately make Europe unattractive for service providers.