Seton Hall University
eRepository @ Seton Hall

Student Works | Seton Hall Law

2023

The Digital Services Act: Does it Respect the Freedom of Expression, and Is It Enforceable?

Terrell Paige

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

 Part of the Law Commons

Table of Contents

I. RESEARCH SUMMATION AND THESIS

This research analyzes the European Union's recently adopted regulation, the Digital Services Act ("DSA").[1] The DSA is the world's first significant attempt to comprehensively address illegal online content and institute corporate accountability structures to protect fundamental rights. It reflects a massive change in the regulatory landscape for digital intermediaries.[2] In coordination with its sister regulation, the Digital Markets Act ("DMA"),[3] the DSA aims to facilitate predictability and trust online by harmonizing the rules that govern intermediary services and digital service providers ("DSP").[4]

First, this paper reviews the historical background of digital services regulation in the European Union. It then introduces and evaluates the new regulatory framework established in the DSA. After introducing fundamental rights in the European Union, this paper examines the freedom of expression enshrined in the Charter of Fundamental Rights of the European Union ("CFR") Article 11. This analysis considers whether the new regulations to address illegal content in the DSA comply with legal limitations on the right to freedom of expression. Finally, this paper reflects on some of the implementation challenges the DSA should expect to face.

The research concludes by finding that some of the structures of the DSA restrict online expression. Notably, there is potential for abuse in the new notice and reporting mechanisms for illegal content. However, as understood by relevant legal authorities in Europe, the freedom of expression likely remains unviolated due to ever-expansive criteria by which authorities may limit that freedom.

---

[1] Regulation 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), 2022 O.J. (L. 277). [hereinafter *Regulation 2022/2065*].
[2] *See* Regulation 2022/2065, recital 40-41, 2022 O.J. (L. 277).
[3] Regulation 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), 2022, O.J. (L. 265) [hereinafter *Regulation 2022/1925*] (economic regulation targeting unfair business practices of "gatekeepers" within digital market spaces, discussion of which is beyond the scope of this paper).
[4] *See* Regulation 2022/2065, recital 9, 2022 O.J. (L. 277).

As for the findings about implementation, in crafting the DSA, the EU left many essential details to be determined later either by the new European Board for Digital Services ("the Board") or through delegated and implementing acts. This lack of clarity may have the effect of replicating many of the same issues of the implementation of the GDPR to the DSA, including selective enforcement by member states leading to inconsistent enforcement efforts. Because the DSA mandates cooperation between national Digital Services Coordinators ("DSC") and the Commission but provides insufficient mechanisms for resolving disputes between the two, implementing the DSA will likely carry a level of inefficiency in bridging competing interests and values of member states.

II. INTRODUCTION AND BACKGROUND

The social media revolution changed the very landscape of how our society connects and interacts. The cultural shift toward social networking via internet platforms arguably began in 1994 with the creation of GeoCities by David Bohnett and John Rezner.[5] Since then, social media has become an inescapable facet of everyday life. According to Statista, as of 2022, over 4,590,000,000 people used social media, with the average user having an account on six different platforms.[6]

Within the digital landscape, platforms with social networking functionality take many forms. These forms include but are not limited to: networking and social community websites (e.g., Facebook, LinkedIn), blogs and microblogging services (e.g., Twitter, Tumblr), image-sharing services (e.g., Instagram, Snapchat), video-sharing websites (e.g., YouTube, DailyMotion), collaborative information databases (e.g., Wikipedia), community-based

[5] *See* JEAN BURGESS, THE SAGE HANDBOOK OF SOCIAL MEDIA, at 80 (Alice Marwick & Thomas Poell eds., 1st ed., 2018) (GeoCities was a service allowing users to create webpages that were all categorized together under a digital "city", either topically or geographically categorized, allowing users to find other websites relevant to them).

[6] S. Dixon, *Number of global social network users 2017-2027*, STATISTA (2022), https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (last visited Dec 17, 2022).

discussion boards (e.g., Reddit, 4chan), and intimate connection platforms (e.g., Tinder, Grindr). Many digital interactions take place on privately held platforms that rely on closely guarded trade secrets, providing unique challenges to regulators looking to contain their influence.[7]

In the internet's infancy, free speech thrived due to regulators' lack of foresight concerning the impact that widely accessible digital services could have on society.[8] The United States Communications Decency Act of 1996 ("CDA") [9] signified the first significant shift from free speech in an attempt to regulate illegal or offensive expressions online. Among other things, The CDA establishes that providers are not publishers of the information posted on them.[10] Because of this designation, the CDA also provides a general immunity removal of content the provider considers "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[11]

The CDA sparked a shift toward regulation of online spaces that led European nations to seek similar controls. Thus, in 2000, the European Union issued the Directive on Electronic Commerce, frequently referred to as the e-Commerce Directive ("ECD"). [12] The ECD largely followed the lead of the CDA by creating guidelines to regulate the internal market for online services.[13] This directive sought to create a market that guarantees "the free movement of information society services between the Member States."[14] The ECD allowed Member States

---

[7] *See generally* BURGESS, *supra* note 5, at 129-30 (discussing the impact that trade secrets, such as the algorithms that underly these platforms, have on efforts of researching and regulating these companies).
[8] *See id.*, *at 254-56.*
[9] Communications Decency Act of 1996, 47 U.S.C.A. § 230.
[10] *See* 47 U.S.C.A. § 230 (c)(1).
[11] *See* 47 U.S.C.A. § 230 (c)(2)(A).
[12] *See* 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'), 2000 O.J. (L. 178) [hereinafter *e-Commerce Directive*].
[13] *See id.*, at recital 40.
[14] *See id.*, art. 1(1).

to enact laws compelling providers to coordinate with law enforcement and inform proper authorities of unlawful activities or information from users.[15]

Like the CDA, the ECD prohibits liability for intermediary service providers who only act as a "mere conduit" for the data sent on their platforms.[16] For platforms that host content, so long as they do not know of illegal content or, upon obtaining awareness, remove any illegal content, they are free from liability.[17] Another similarity to the CDA is that the ECD does not require providers actively monitor their platforms for illegal activity by third-party users.[18] Similar policies in the E.U. and U.S. have created comprehensive protection for most digital service providers against liability for content on their platforms.

Policymakers of the late 20th century would be hard-pressed to foresee how social media exploded not only in popularity but in its impact on almost every facet of life, including but not limited to commerce, social discourse, politics, and popular culture. Unlike in the United States, European regulators focused on overall consistency by regulating internet companies similarly to existing telecommunications companies.[19] Since adopting the ECD, European policymakers have shifted their attention toward controlling illegal and harmful content on social networking platforms.[20] In March 2021, the European Commission issued a communication outlining a unified European approach to the future of digital space and pledging that the next would be "Europe's Digital Decade."[21] The foundation of this strategy

---

[15] *See id.*, art. 15(2).
[16] *See id.*, art. 12.1 (a); art. 12(1)(b); art. 12(1)(c).
[17] *Id.*, art. 14(1)(a); art. 14(b).
[18] *See id*., art. 15(1).
[19] *See generally* Johannes M. Bauer, Michel Berne & Carleen F. Maitland, *Internet access in the European Union and in the United States*, 19 Telemat. Inform. 117, 124 (2002).
[20] *See* European Commission, *Illegal content on online platforms | Shaping Europe's digital future*, EUROPEAN COMMISSION, https://digital-strategy.ec.europa.eu/en/policies/illegal-content-online-platforms (last visited Dec 20, 2022) ("The Commission is concerned that the removal of illegal content online is not effective enough").
[21] *See* European Commission, *Europe's Digital Decade: Digitally empowered Europe by 2030*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983 (last visited Oct 30, 2022).

is harmonizing the obligations placed on internet service providers to protect the rights of users of these services and facilitate the removal of illegal content.[22]

III. MEET THE DIGITAL SERVICES ACT

A cornerstone of the "Europe's Digital Decade" initiative is a new regulation, the Digital Services Act. After a period of input from stakeholders from July to September 2020, the European Commission introduced the proposed DSA on December 15, 2020.[23] The DSA focuses on protecting the rights of individual users by establishing obligations for intermediaries to remove illegal content and protect private user data. [24] The introduction of the proposal opened another period of public feedback and comment on the anticipated regulations from December 16, 2020, through March 31, 2021, in which 138 respondents across businesses, trade unions, NGOs, and citizens submitted positions on the proposal.[25]

The European Commission, Parliament, and Council entered a trilogue to consider and incorporate this feedback.[26] A political agreement was reached on April 23, 2022, allowing the legislation to move to final approval by the European Parliament and Council.[27] On October 19, the Parliament and the Council signed the Act into law.[28] Most provisions of the regulation will apply from February 17, 2024.[29] On November 16, 2022, the three-month deadline for

---

[22] *See* European Commission Press Release, Europe fit for the Digital Age: Commission proposes new rules for digital platforms, (December 15, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347.
[23] See *Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC,* COM (2020) 825 final (December 15, 2020).
[24] *See* Regulation 2022/2065, recital 52, 2022 O.J. (L. 277).
[25] *See* European Commission, *Digital Services Act – deepening the internal market and clarifying responsibilities for digital services*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services_en (last visited Oct 31, 2022).
[26] *See* European Parliament, *Interinstitutional negotiations*, EUROPEAN PARLIAMENT, https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations (last visited Dec 20, 2022) ("Negotiations between the institutions on legislative proposals generally take the form of tripartite meetings ('trilogues') between Parliament, the Council and the Commission").
[27] *See* European Commission Press Release, DSA: Commission welcomes political agreement (April 23, 2022) https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.
[28] *See* European Council, *Timeline - Digital Services Package*, EUROPEAN COUNCIL, https://www.consilium.europa.eu/en/policies/digital-services-package/timeline-digital-services-package/.
[29] *See* Regulation 2022/2065, art. 93(2), 2022 O.J. (L. 277).

platforms to report their active number of users began.[30] After February 17, 2023, the Commission will begin to designate which platforms are impacted by specific provisions which apply only to large platforms.[31] Upon receiving such a designation, these platforms have four months to comply.[32]

The DSA is a trailblazing regulation that seeks to harmonize discordant national laws by creating a single internal market with uniform rules for providers of intermediary services.[33] This regulation is a horizontal instrument that will coexist with any existing regulation it does not amend.[34] Because it is a regulation, unlike the ECD, the DSA is directly applicable in all member states with no need for adoption at the national level.[35]

Though the DSA is a European Union regulation, it will have global ramifications as non-European-based companies must comply with the regulations if they do any business in the Union, a market of over 450,000,000.[36] These ramifications include potentially severe penalties for non-compliance. The obligations introduced in the DSA come from general duties applicable to all companies and special obligations imposed on "very large" companies. Failure to comply with an obligation set by the DSA can result in fines of up to 6 percent of an intermediary's annual global revenue.[37] For violations, this could mean fines as costly as eleven billion dollars for a company such as Google.[38]

---

[30] *See* European Commission, *DSA: landmark rules for online platforms enter into force*, EUROPEAN COMMISSION, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6906.
[31] *Id.*
[32] *Id.*
[33] *See* Regulation 2022/2065, recitals 2-4, 2022 O.J. (L. 277).
[34] *See id.*, at recital 110
[35] *See id.*, at art. 93.
[36] *See id.*, at recital 76; recital 110.
[37] *See id.*, at art. 52(3).
[38] *See* Anna Schiffrin, *The hard work of implementing the Digital Services Act has begun*, COLUMBIA JOURNALISM REVIEW, (2022) https://www.cjr.org/analysis/digital-services-act-european-union.php.

A. Regulations Applicable to Companies Irrespective of Size

The DSA introduces a tiered system of gradual obligations on intermediaries. At the broadest level, the DSA has general obligations that apply to all intermediary services.[39] The DSA lays out the framework for these intermediaries in three categories. These categories are "mere conduits," "caching services," and "hosting services" and are differentiated by the nature of the interaction between the provider of the service and the data transmitted.[40]

The liability regime established in the ECD remains where "mere conduits" have no liability as long as they do not control the transmission.[41] Intermediaries that "cache" information are not liable so long as they comply with storage and access requirements and remove cached data that is flagged for removal or removed from the network.[42] While "hosting" intermediaries are not liable for illicit content as long as they have no actual knowledge of the content and act with haste to remove it upon obtaining knowledge of unlawfulness.[43] One variation from the existing system is that the DSA includes a safe harbor provision wherein providers are not liable when conducting investigations into illegal content or actions taken to comply with national law or the DSA itself.[44] The ECD's restriction on general monitoring obligations remains intact.[45]

The DSA has various general due diligence obligations found in Chapter III. Some of the broadest responsibilities are contingent on the intermediary's location. All intermediaries must have a point of contact.[46] E.U. companies must designate a company contact for the national Digital Service Coordinator, the Commission, and the Board.[47] Finally, foreign

---

[39] *See* Regulation 2022/2065, arts. 5-7, 2022 O.J. (L. 277).
[40] *See id.*, at art. 3 (g)(i)-(iii)
[41] *See id.*, at art. 4 (a)-(c)
[42] *See id.*, at art. 5(1)(a)-(e)
[43] *See id.*, at art. 6(1)(a)-(b)
[44] *Id.*, at art. 7; *see also* Taylor Wessing, *Digital Services Act - an overview*, LEXOLOGY (2022), https://www.lexology.com/library/detail.aspx?g=fd2c6982-8174-4b8d-860d-fb98513b6780 (last visited Dec 20, 2022) (discussing safe harbor provision).
[45] *See* Regulation 2022/2065, art. 8, 2022 O.J. (L. 277)
[46] *I*d., at art. 11
[47] *See id.*, art. 12

companies must appoint a legal representative to establish liability for non-compliance with the DSA.[48] All intermediaries must explain how they moderate third-party content, whether this process is automated, and how they handle complaints.[49]

At the second level, hosting services have additional requirements on top of the general due diligence obligations imposed on all intermediaries. Hosts are required to implement a comprehensive and accessible notice and action mechanism to allow users to notify the provider of suspected illegal content.[50] The DSA also establishes an obligation on hosting service providers to provide a specific statement of reasons when they restrict a user on a platform, such as via suspension, content removal, or demonetization.[51] The DSA requires hosts to notify law enforcement about any suspected criminal offense involving a threat to life or safety.[52]

At the third level, online platforms not classified as a "micro or small enterprise" receive an even higher level of obligations. The DSA defines online platforms as a hosting service that "stores and disseminates information to the public" as one of its primary features.[53] These online platforms are required to implement special content moderation procedures. These procedures include certifying trusted content flaggers, who get priority when highlighting illegal content. [54]

The DSA introduces a host of transparency requirements on online platforms, requiring clear labeling of advertisements and who funds them.[55] Additionally, the DSA establishes new internal complaint and out-of-court dispute mechanisms for handling decisions that negatively

---

[48] *Id.*, art. 13
[49] *Id.*, art. 14
[50] *See id.*, art. 16
[51] *See id.*, art. 17
[52] *See id.*, art. 18
[53] *See id. art. 3(i)*
[54] *See id.*, art. 22.
[55] *See id.*, art. 26

impact a user, such as a decision to remove content or suspend a user's access to a service.[56] These platforms must also report how many complaints they receive in their internal system and how many disputes out-of-court settlements resolve.[57] Finally, the DSA requires transparency from online providers in how systems that recommend things to users decide what to recommend.[58] Section IV of the DSA introduces special regulations for online e-commerce platforms, which center on transparency, such as the accessibility of information collected on consumers, and creates a right for customers to access information when they have purchased an illegal product.[59]

B. Provisions Applicable Only to Very Large Online Platforms and Search Engines

At the fourth and most narrow level, the DSA imposes strict new obligations on "very large online platforms" ("VLOP") and "very large online search engines" ("VLOSE"). Platforms and search engines with active members greater than forty-five million E.U. citizens, or around ten percent of the population, have additional obligations because of their potential impact on many E.U. citizens.[60] These special obligations reflect the recognition of a concentration of influence on the internet among a small number of large and powerful companies such as Alphabet, Amazon, Apple, Meta, and Microsoft. For these VLOP and VLOSE, the European Commission is directly responsible for oversight and enforcement of these obligations and for designating platforms as VLOP or VLOSE.[61]

The first of these special VLOP and VLOSE obligations are obligatory yearly risk assessments for threats on their services, including but not limited to the dissemination of illegal content, threats to fundamental rights, threats to the electoral process and civil discourse,

---

[56] *See id.*, art. 20; art. 21.
[57] *See id.*, art. 24.
[58] *See id.*, art. 27.
[59] *See generally id.*, art. 30; art. 31; art. 32.
[60] *See id.*, art. 33(2).
[61] *Id.*, art. 65

and threats of discriminatory violence.[62] The DSA pairs these assessments with the required mitigation of risks, requiring VLOP and VLOSE to implement measures to mitigate previously identified risks.[63] This mitigation includes making changes to design and functionality, adjusting the content moderation process, and taking specific steps to protect children, among other efforts.[64]

The following significant obligation imposed on VLOP and VLOSE is that they must establish "crisis response mechanisms." These mechanisms dictate that these companies assess how their services may contribute to a severe threat when "extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it."[65] Upon the Commission making such a determination, they may require VLOP and VLOSE to "prevent, eliminate or limit any such contribution to the serious threat."[66] This obligation would almost certainly require companies such as Twitter or Facebook to flag misinformation about a public health crisis or electoral crisis or even downright remove information deemed to contribute to the threat upon being ordered by the Commission.

The DSA imposes a host of transparency requirements on large companies based on prioritizing access to data in drafting the regulation. These requirements include advertising transparency, requiring companies to make available data on all advertisements they present for at least one year.[67] Companies must provide access to their data to allow monitors to ensure compliance with the DSA and for research purposes.[68] To ensure compliance with these regulations, VLOP and VLOSE must appoint a compliance officer[69] and conduct yearly audits

---

[62] *See id.*, art. 34
[63] *See id.*, art. 35(1)
[64] *See id.*, art. 35(1)(a)-(k)
[65] *Id.*, art. 36(1); art. 36(2).
[66] *Id.*, art. 36(1)(b)
[67] *See id.*, art. 39(1)
[68] *See id.*, art. 40(1); art. 40(8)
[69] *See id.*, art. 41

at their expense.[70] Finally, the DSA imposes a to-be-determined annual supervisory fee against VSOP and VLOSE to cover the costs of the Commission implementing the regulations.[71]

The DSA leaves many specifics of how the bill will work in practice to future action, as detailed in Section 6. These specifics include critical areas such as standards for the collection of notices, audits, transparency obligations, and protection of minors;[72] establishing codes of conduct when applying the regulations, codes of conduct for online advertising, and codes of conduct for commitments to accessibility;[73] drawing protocols to address crisis protocols and how the crisis powers of the Commission mentioned above will work in practice.[74] The lack of specificity in these areas leaves many questions about how essential parts of the DSA will work in practice.

This new regulation creates the most impactful and expansive reconfiguration of the landscape for digital services since the ECD went into effect over twenty years ago. Many of the DSA's structures come directly from the existing system, including the continued limitation of liability for intermediaries so long as they avoid active knowledge of illegal content. Nevertheless, the new obligations imposed on intermediaries, particularly those set on VLOP and VLOSE, have unique and extraordinary implications for how these businesses will conduct their operations and the rights of customers who use these services, particularly the right to freedom of expression online.

IV. FREEDOM OF EXPRESSION IN THE EUROPEAN UNION: ITS CREATION AND CONSTRAINTS.

The general principles of law among nations are the foundation of the entire international law system, a concept that the European Union's governing documents

[70] *See id.*, art. 37
[71] *See id.*, art. 43
[72] *See id.*, art. 44
[73] *See id.*, art. 45; art. 46; art. 47.
[74] *See id.*, art. 48

recognize.[75] The Treaty on the European Union ("TEU") identifies several sources of laws that create a framework for protecting the political, social, and economic rights of EU citizens. This framework includes the constitutional traditions common to the Member States, the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), and the 2000 Charter of Fundamental Rights of the European Union ("CFR").[76] The TEU enshrines the historical constitutional traditions of the EU member states as a primary source of the European Union's laws to guarantee fundamental rights, allowing EU courts to draw from the constitutional heritage and jurisprudence of the 27 Member States when making decisions.[77]

The TEU also codifies the rights found in the ECHR as a part of the general principles of Union law and mandates EU ascension to the treaty.[78] The ECHR, inspired by the Universal Declaration of Human Rights, was the first widespread European agreement to prevent further human rights abuses.[79] It remains an essential tool for understanding the extent and nature of fundamental freedoms in the EU as the Courts often look to its history of interpretation.[80] Though accession to the ECHR has yet to occur once negotiations conclude and an agreement is reached, it will mean individuals will be able to directly bring a claim against the EU in the European Court of Human Rights ("ECtHR").[81] The Council of Europe drafted the ECHR,

---

[75] *See* Consolidated Version Of The Treaty on European Union, art. 6(3), October 26, 2012, 2012 O.J. (C-326) 15 [hereinafter *TEU*] (also referred to as the Treaty of Lisbon); *see also*, ZIEGLER S KATJA, NEUVONEN J PÄIVI & MORENO-LAX VIOLETA, RESEARCH HANDBOOK ON GENERAL PRINCIPLES IN EU LAW: CONSTRUCTING LEGAL ORDERS IN EUROPE 2-3 (2022) (discussing the incorporation of fundamental rights in art. 6 TEU).
[76] *See* TEU, art. 6(1)-(3).
[77] *See* TEU, art. 6(3); *see also*, ROBERT SCHÜTZE, EUROPEAN CONSTITUTIONAL LAW 18-20 (2012) (introducing the ideas of supranationalism and the intersection between that and national law).
[78] *See* TEU, art. 6(2)-(3).
[79] *See generally* WILLIAM A. SCHABAS, THE EUROPEAN CONVENTION ON HUMAN RIGHTS: A COMMENTARY, at 2 (2015).
[80] *See* Allan Rosas, *The Court of Justice of the European Union: A Human Rights Institution?*, 14 J. HUM. RIGHTS PRACT. 204, 208 (2022).
[81] *See* Council of Europe, *European Union accession to the European Convention on Human Rights - Questions and Answers*, COUNCIL OF EUROPE, https://www.coe.int/en/web/portal/eu-accession-echr-questions-and-answers.

giving the ECtHR responsibility for its interpretation, and all forty-six members of the Council are parties to the treaty.[82]

For almost half a century, the ECHR was the principal instrument for European human rights. This changed with the 2009 reforms to the TEU, which beyond recognizing general principles of law and the ECHR as sources for the principles of EU law, also gives legal effect to the CFR with the same legal primacy as the governing documents of the European Union.[83] Unlike the ECHR, the CFR is a European Union document limiting its scope to the 27 Member States.

The TEU points to the CFR to interpret the guaranteed rights, freedoms, and principles of E.U. citizens.[84] The CFR then points to the ECHR to understand the rights enshrined in the Charter.[85] This chain of references gives the Court of Justice of the European Union ("CJEU") the ability to issue rulings based on the CFR or general principles of law that it takes from the ECHR.[86] This interconnected web of agreements and frameworks enhances the complexity of assessing the rights of EU citizens and provides a starting point to determine how the CJEU may interpret whether the application of the new provisions of the DSA complies with the freedoms enshrined in either treaty or found in general principles, specifically the freedom of expression.

Article 11(1) of the CFR protects the freedom of expression and information: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." [87] Because the Charter recognizes that freedom exists

---

[82] *See* Council of Europe, 46 Member States, COUNCIL OF EUROPE, https://www.coe.int/en/web/portal/46-members-states.
[83] *See* TEU, art. 6(1)
[84] *See* Consolidated version of the Treaty on European Union, *supra* note 76., art. 6
[85] *See* Charter of Fundamental Rights of the European Union, art. 52, 2012 O.J. (C 326) 391. [hereinafter CFR],
[86] *See generally* Rosas, *supra* note 80.
[87] CFR, art. 11(1), 2012 O.J. (C 326) 391.

"regardless of frontiers," the freedom of expression covers all forms of speech, oral and written, irrespective of the means of communication, such as print, radio, television, and most relevantly to the DSA, the internet.[88]

Like the other rights and freedoms recognized by the Charter, any limitation of the freedoms of expression and information must meet three conditions: (1) the goal of the limitation must reflect a legitimate interest recognized by the Union or necessary to protect the rights and freedoms of others; (2) the limitation must be provided for by law; (3) the limitation must be necessary to avert a specific threat, and the limitation must be proportionate to the threat from the expression.[89] This system of negative obligations is the primary means of analyzing the freedom of expression. Negative obligations contemplate what a state may not do instead of establishing a more general duty to take affirmative action.

Several areas of concern arise from the new regulations in the DSA. Among these are the standards by which moderators judge illegal content, the removal process of online expressions due to a finding of illegality, and questions about a lack of due process in automated content moderation systems.[90] The Digital Services Act, on its face, limits users' expressions. Requiring DSPs to remove content the Union or Member States deems illegal will inevitably remove the expressions people post online in a limiting fashion. Thus, the question becomes whether the structures established in the DSA comport with the conditions imposed on limiting expressions.

A. Legitimate Goals: The Court Rarely Finds Impermissible Constructions.

The first element of the freedom of expression analysis requires the Court to consider whether the States goal in limiting the expression reflects a legitimate purpose. Courts do not

---

[88] *See* STEVE PEERS ET AL., THE EU CHARTER OF FUNDAMENTAL RIGHTS: A COMMENTARY 352-53 (2021).
[89] CFR, art. 52(1)-(2), 2012 O.J. (C 326) 391.
[90] *See generally* Karen Gullo and Christoph Schmon, *DSA Agreement: No Filternet, But Human Rights Concerns Remain*, ELECTRONIC FRONTIER FOUNDATION (2022), https://www.eff.org/deeplinks/2022/04/dsa-agreement-no-filternet-human-rights-concerns-remain (last visited Dec 20, 2022) (considering some of the human rights challenges with the DSA, including some mentioned in this paper, and some not addressed.)

give much time to asking whether a goal is legitimate, spending more time determining if it is necessary.[91] Art. 52(1) allows for limitations of the rights in the CFR "only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[92] To understand what these objectives of general interest comprise concerning freedom of expression, one can look to Article 10(2) of the ECHR due to the CFR's reliance on it to interpret its nearly identical provisions. The freedom of expression in Article 10(2) of the ECHR allows for restrictions:

> In the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[93]

The CFR holds the meaning and scope of the rights it guarantees are the same as their corresponding rights in the ECHR.[94] When assessing whether a limitation meets one of these legitimate aims, the Court, on a case-by-case basis, weighs the limitation on freedom against the reason for the limitation presented by authorities.[95] For example, arguments for a limitation predicated on the protection of public morality may be more complicated than those to protect the judiciary or national security due to the clear governmental interest in those areas. Thus, the analysis of any limitation must occur considering the objective given by the government.

---

[91] *See infra*, Section IV(C), for a discussion on necessity.
[92] *See* Charter of Fundamental Rights of the European Union, *supra* note 75, Art. 52.1.
[93] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, art. 10(2), Nov. 4, 1950, Council of Europe Treaty Series 005 [hereinafter *ECHR*].
[94] Charter of Fundamental Rights of the European Union, *supra* note 75, Art. 52.3.
[95] *See e.g.*, Case C-71/02, Herbert Karner Industrie-Auktionen GmbH v. Troostwijk GmbH, 2004 E.C.R. I-03025, ¶ 51, ("It is common ground that the discretion enjoyed by the national authorities in determining the balance to be struck between freedom of expression and the abovementioned objectives varies for each of the goals justifying restrictions on that freedom and depends on the nature of the activities in question").

The DSA states that it aims to "contribute to the proper functioning of the internal market for intermediary services by setting out harmonized rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected."[96] The ECtHR also allows limitations based upon the protections of Article 17 ECHR, which prohibits any enumerated right from being used to destroy or limit any other enumerated right.[97] In *Norwood*, the ECtHR held that Article 10 did not protect the applicant's expressions as they discriminatorily abridged others' enjoyment of their rights and freedoms in violation of ECHR Article 14.[98]

The stated objective of the DSA, more likely than not, would fall under the enumerated exception to protect the reputation and rights of others. The regulation aims explicitly to protect the fundamental rights in the CFR. As outlined above, the Court has consistently held the position of allowing limitations of some rights to protect others.[99] Thus, the CJEU will likely allow this limitation on freedom of expression if it is prescribed by law and compliant with the criteria of necessity and proportionality.

B. The Deference to States in Whether a Restriction is "Prescribed By Law."

As a starting point, Courts find few laws improperly prescribed by law. The ECtHR has a long-used test to determine whether a limitation is "prescribed by law," best laid out in the

---

[96] *See* Regulation 2022/2065, art. 1(1), 2022 O.J. (L. 277).
[97] *See* ECHR, *supra* note 83, art. 17. ("Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention."); *see also*, Joined cases C-244/10 and C-245/10, *Mesopotamia Broadcast A/S METV (C-244/10) and Roj TV A/S (C-245/10) v. Bundesrepublik Deutschland*, 2011 E.C.R. I-08777 (AG Opinion ¶ 68)
[98] *See Norwood v. the United Kingdom (dec.)*, no. 23131/03 (2004) (discussing a case where a neo-Nazi, who displayed a poster in the window of his apartment with a photograph of the Twin Towers on fire with the words "Islam out of Britain – Protect the British People.", had it forcibly removed by the police and was charged with displaying hostility toward a racial or religious group.)
[99] *See also,* ALEXANDRE DE STREEL ET AL., ONLINE PLATFORMS' MODERATION OF ILLEGAL CONTENT ONLINE: LAW, PRACTICES AND OPTIONS FOR REFORM 15 (2020).

seminal freedom of expression case *The Sunday Times v. United Kingdom*.[100] In that case, the court expressed the requirements for a limitation to be "prescribed by law" as a two-part test focusing on accessibility and foreseeability, stating:

> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[101]

In *The Sunday Times*, the ECtHR found that the paper had a "more than adequate indication" of the legal rules applicable to their conduct due to the "mass of authority" on the relevant case law.[102] The law was "precisely detailed" in that it was contempt for a newspaper to report on proceedings in any way likely to prejudice the trial and even provided examples comparable to their current circumstances. Thus, the court held that the law had enough precision to allow a person to foresee the consequences of their actions.[103] Applying this standard to the DSA may lead to a different result due to the disparities between the Member States and what content is considered illegal. These discrepancies may preclude reasonable citizens from properly comporting their behavior regarding online expressions.

---

[100] The Sunday Times v. the United Kingdom (no. 1), 6538/74 (1979) https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57584%22]} (holding that an injunction by the UK government prohibiting the paper from publishing an article related to a settlement for mothers of children with congenital disabilities violated their freedom of expression).
[101] *Id.*, at ¶ 49.
[102] *Id.*, at ¶ 51.
[103] *Id.*

A core goal of the Digital Services Act is to harmonize laws between offline and online illegal content.[104] Nonetheless, the fractured landscape of laws defining illegal content creates questions concerning whether the E.U. crafted the DSA per the principles of legality as they pertain to freedom of expression. The E.U. defines crimes such as illegal terrorist content, online hate speech, and child pornography at the National level; outside of this, the Member States may draft criminal laws.[105] However, the DSA does not define what content is manifestly illegal and defines illegal content broadly as:

> Any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.[106]

Tying the definition of what is illegal under the DSA to the definitions of what is unlawful across any Member State creates twenty-seven different standards by which online platforms may consider content unlawful. This definition puts a great deal of power in the hands of the Member States to determine whether specific content is illegal, ostensibly counter to the goal of harmonizing laws. The DSA leaves implementation to the Member States, except for the requirements imposed onto VLOP and VLOSE in section 5, where the Commission has sole competency.[107] What this means in practice is that unless a platform has a user base equal to or larger than 10 percent of the Union's population, they are subject to the laws of the member state where its establishment or legal representative exists.[108] However, the VLOP and

---

[104] *See* Regulation 2022/2065, recital 12, 2022 O.J. (L. 277).
[105] *See* DE STREEL ET AL., *supra* note 99, 16.
[106] *See* Regulation 2022/2065, art. 3(h), 2022 O.J. (L. 277).
[107] *See id.*, art. 56.
[108] *See supra,* note 60.

VLOSE are still subject to the Member State they are established in so long as the Commission has not initiated proceedings yet.[109]

For the average user, the E.U. may have needed to formulate the DSA more precisely to allow users to comport their behavior to this incredibly complex system of laws like the principle of legality requires. The billions of social media users within and outside of the E.U. may think themselves covered by local laws when posting online. However, under the framework outlined above, conduct could be legal where a consumer resides only to be illegal where the provider exists for DSA purposes and thus become censored.[110] The immediately global nature of online expressions magnifies this challenge because any person or entity across the globe can access the information published online and submit a report alleging illegality.[111]

For American companies and consumers, for instance, small or large, an E.U. national court or the CJEU can order the takedown of content globally, even when it is legal under US law or the law of one of the Member States. The DSA, like the ECD before it, does not limit the jurisdiction of Member State courts only to remove or block content within their borders. The CJEU laid this ruling down in *Eva Glawischnig-Piesczek v. Facebook Ireland Limited.*[112] In that case, an anonymous Facebook user shared an article about refugees while commenting that the applicant, an Austrian politician, calling her "miese Volksverräterin" (lousy traitor), "korrupter Trampel" (corrupt bumpkin), and her party a "Faschistenpartei" (fascist party).[113] The applicant requested that Facebook delete the comment, but they would not, so she sued

---

[109] *See* Regulation 2022/2065, art. 56(4), 2022 O.J. (L. 277).
[110] *See generally* Kaie Rosin & Markus Kärner, *The Limitations of the Harmonisation of Criminal Law in the European Union Protected by Articles 82(3) and 83(3) TFEU*, 26 EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND CRIMINAL JUSTICE 315 (2018) (discussing the ramifications of discordant criminal law due to the limits imposed by the Union's founding documents).
[111] *See* Regulation 2022/2065, art. 14, 2022 O.J. (L. 277) (notice and action mechanisms)
[112] Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Limited, ELLI:EU:C:2019:458, (2018)(Opinion of Advocate General Szpunar delivered on 4 June 2019) [hereinafter *Glawischnig-Piesczek*] *(* Facebook Ireland Ltc. ("Facebook") is the European holding company for Facebook, now known as Meta.)
[113] *See id.*, at ¶ 12.

Facebook in the Austrian Commercial Court in Vienna.[114] The court ordered Facebook to stop the publication and dissemination of photographs of Glawischnig-Piesczek so long as the aforementioned defamatory comments or any "equivalent content" accompanied them.[115]

Facebook proceeded to block access to the content within Austria; however, on appeal, the Higher Regional Court in Austria ordered that the ban be enforced globally rather than just within Austria.[116] Upon further appeal, the Austrian Supreme Court referred the proceedings to the CJEU.[117] In his decision, the Advocate General offered that a Member State court could require Facebook to "seek and identify" all identical information as the defamatory comments and remove them.[118] Concerning expressions that are "equivalent" rather than exact, the Advocate General stated that censorship should be limited only to the expressions of that user which are equivalent instead of all like comments to avoid a violation of the prohibition on a general obligation to monitor.[119] He then goes on to declare that a Member State court may generally order the removal of content extraterritorially, going as far as to refer to their jurisdiction as universal.[120] All the court offers to limit this is that the order must be necessary to protect the injured party.[121]

One such area where this will be problematic is laws that have different standards in one nation than another. Defamation, for instance, the exact phrase may be defamatory in one country and not defamatory in another.[122] However, under the *Glawischnig-Piesczek* ruling, the CJEU does not find this problematic. While the CJEU does not mention the principle of margin of appreciation, one should infer that these differences between states fall within the

---

[114] *See id.*, at ¶ 14.
[115] *See id.*
[116] *See id., at* ¶ 17.
[117] *See id., at* ¶ 22.
[118] *See id., at* ¶ 58
[119] *See id., at* ¶ 72
[120] *See id., at* ¶ 86
[121] *See id., at* ¶ 100.
[122] *See* SCOTT GRIFFEN, OUT OF BALANCE: DEFAMATION LAW IN THE EU, 10 (2015) (illustrating the different statements considered defamatory among different Member States).

nature of this allowance. Though the DSA does not specify what laws will be applicable in every instance, in *Glawischnig-Piesczek,* the CJEU made allowance for circumstances wherein there is discord between the implementation of Member State law. Due to this, though an average citizen may have difficulty foreseeing how to comport their behavior, it is unlikely the CJEU would invalidate the DSA due to a lack of being "prescribed by law."

C. Necessity is Subjective, But an E.U. Court May Disagree.

To determine if a limitation on freedom of expression is necessary, courts primarily examine whether a nation needs this restriction to protect a demanding social need with great deference to national governments.[123] When analyzing whether an action unjustly limits a human right, the ECtHR often allows limitations utilizing a principle referred to as the margin of appreciation. The margin of appreciation is a judicial doctrine wherein the court defers to differences in how various nation-states actualize the enumerated rights.[124] This deference allows for regional differences in the applications of certain rights and freedoms. Clarifying their position on the margin of appreciation in *Dickson,* the ECtHR offered that when a widely accepted and "important facet of an individual's existence or identity" is a concern, there is less margin of appreciation for how necessary a restriction is.[125] In this same vein, subjective values have a different standard, with the *Dickson* court holding:

> Where, however, there is no consensus within the Member States . . . either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider. This is particularly so where the case raises complex issues and choices of social strategy: the authorities' direct knowledge of their society

---

[123] *See Handyside v. the United Kingdom*, no. 5493/71, ¶ 48 (December 7, 1976), http://hudoc.echr.coe.int/eng?i=001-57499 ("it is not possible to find in the domestic law of the various Contracting States a uniform European conception of morals. . . it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context.)
[124] *See* DR ANDREW LEGG, THE MARGIN OF APPRECIATION IN INTERNATIONAL HUMAN RIGHTS LAW: DEFERENCE AND PROPORTIONALITY 3-5 (2012).
[125] *See Dickson v. the United Kingdom*, No. 44362/04 ¶ 78 (April 12, 2007), https://hudoc.echr.coe.int/eng#{%22appno%22:[%2244362/04%22]}.

> and its needs means that they are in principle better placed than the international judge to appreciate what is in the public interest. In such a case, the Court would generally respect the legislature's policy choice unless it is "manifestly without reasonable foundation."[126]

However, the court previously made clear in the *Handyside* case that this is not an "unlimited power of appreciation."[127] Instead, courts leave the necessity determination to the nation-state but give special attention to the protection of principles necessary to a "democratic society."[128] In that case, the court held that content that may "offend, shock, or disturb" deserves protection as without "pluralism, tolerance, and broadmindedness," there can be no democratic society.[129] However, since then, the CJEU has given greater weight to the need to limit speech in favor of protecting rights.[130]

It is difficult to argue against the fact that European nations have substantial consensus regarding regulating "illegal" speech in digital spaces. Not only is this evident by the passage of the DSA, which required the consent of all the Member States, but the actions leading up to it, such as the harmonization of rules concerning terrorist content, child sexual abuse material, racist and xenophobic hate speech, and violations of Intellectual Property.[131] To assess whether necessity exists, the court considers if the means were proportionate to one of the "legitimate aims" which the limiter of the freedom of expression must have enumerated. Whether the means are proportionate is a case-specific analysis weighed against the aim; here, as stated above, the DSA seems to aim to protect the reputation and rights of others. Traditionally, the rights of politicians weigh less favorably against the value of allowing freedom of expression

---

[126] *Id.*
[127] *See Handyside v. the United Kingdom*, *supra* note 123., ¶ 49
[128] *Id.*
[129] *Id.*
[130] *See, e.g.*, *Glawischnig-Piesczek*, *supra* note 100 (confirming the reach of companies to remove content globally).
[131] *See* DE STREEL ET AL., *supra* note 99.

concerning matters of political interest.[132] However, the recent judgment by the CJEU in the Facebook case indicates a shift may occur here toward restricting speech in the EU. The rights of others provide another legitimate aim for limiting freedom of expression. For instance, in the case *Otto-Preminger-Institute v Austria*, the applicant showed a film that depicted religious figures in a highly disparaging manner that the government seized.[133] Defending this, the ECtHR found the film violated the guarantee of respect for the religious feelings of believers, and thus this limitation was proportionate.[134]

Within the past two decades, for the first time, people can impart and receive information without limit and nearly instantaneously. This societal shift has an enormous impact on the freedom of expression.[135] The DSA appears to incentivize platforms to over-censor content due to the liability limitations of the notice and action mechanisms. The DSA provides for a "notice and action" mechanism, wherein all providers of online platforms must establish a system wherein any person may notify the platform of what they consider illegal content.[136] Upon receipt of such a notification, this creates the actual knowledge referenced in DSA Article 6, which removes the shield of liability for providers.[137] This mechanism incentivizes platforms to remove content upon receiving an allegation of illegality; if they do not do so "expeditiously," they face legal liability for the illegal content.[138] The liability scheme

---

[132] *See e.g.*, *Lingens v. Austria*, No. 9815/82, ¶ 42 (July 8, 1986), https://hudoc.echr.coe.int/eng?i=001-57523 ("The limits of acceptable criticism are accordingly wider as regards a politician as such than as regards a private individual. Unlike the latter, the former inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must consequently display a greater degree of tolerance.").
[133] *See Otto-Preminger-Institut v. Austria*, No. 13470/87, ¶ 10 (September 20, 1994), https://hudoc.echr.coe.int/eng?i=001-57897.
[134] *See id.,* at ¶ 57
[135] *See e.g., Silencing the Messenger: Communication Apps Under Pressure*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2016/silencing-messenger-communication-apps-under-pressure (finding an increase in government action against speech on social media due to the explosion in usage of these platforms).
[136] *See* Regulation 2022/2065, art. 16(1), 2022 O.J. (L. 277).
[137] *See id.,* art. 6(3).
[138] *See id.*, art. 6(1)(b).

within the DSA essentially creates an incentive for platforms to choose to be safe rather than sorry when removing alleged illegal content, particularly considering the safe harbor provision.

This incentivization to censor illegal content provides perhaps the most significant difficulty in assessing the permissibility of the DSA's limitations on the freedom of expression. Anyone can flag any expression as unlawful, which creates actual knowledge on behalf of the platform to remove that content that opens them up to liability, making it so that DSPs are encouraged to delete first and ask questions second. This impact appears disproportionate to the goal of respecting the rights and reputations of others. However, considering the highly deferential approach of the CJEU to the proportionality of the aim of respecting the reputation and rights of others, it is unlikely the CJEU would rule that this limitation violates the freedom of expression as it is understood.

Overall, the new limitations on the freedom of expression introduced in the DSA are not outside the territory of the existing case law. The drafters of the DSA made substantial efforts to respect fundamental freedoms in drafting this regulation. However, this respect for fundamental freedoms is as the CJEU and the Union overall understand them. From a more global perspective, there exist circumstances where the freedom of expression is both more and less expansive. This variety of opinions between countries is of note due to the extraterritorial nature of the DSA and the platforms it seeks to regulate, making the coordination of the implementation of the DSA an issue of substantial importance.

V. THE UNION MADE ITS DECISION: NOW, HOW CAN THEY ENFORCE IT?

The DSA is a regulation, binding and directly applicable to the Member States, who must implement it. As it marks a significant shift from the hands-off approach of global regulators concerning technology companies by establishing a host of new requirements on intermediaries, looking at how these obligations and requirements operate is crucial for

determining the effectiveness of the DSA. This section explores the framework for the enforcement of the DSA found in Chapter IV of the DSA. In doing so, it looks at the shortfalls of prior attempts at regulating digital services, such as selective enforcement and discord between implementation across national borders. It assesses the likelihood of those issues under the new structure of the DSA. This structure is one of the shared competencies for enforcement between Member States and the European Board for Digital Services, contrasted by the European Commission's exclusive role in regulating VLOP and VLOSE.

A. "Who is Regulating What?": Competencies Under the DSA.

For companies with their main establishment in the EU, the Member State of their establishment has jurisdiction.[139] For non-EU companies covered by the DSA, the location of their legal representative is their place of establishment for enforcement purposes.[140] When a provider does not have a legal representative, any Member State may exercise dominion. Member States must designate one or more "competent authorities" to enforce the DSA's provisions.[141] Of these authorities, Member States must designate one as a "Digital Services Coordinator" ("DSC").[142] Unless the Member State sets up its enforcement divided between several competent authorities, the DSC is responsible for all national enforcement of the DSA.[143]

National law is the predominant force behind the enforcement of the DSA due to the few harmonized areas of criminal law across the Union. The national DSC has substantial regulatory authority under the DSA. This authority includes an ability to conduct investigations of allegedly illegal content, including seizing information and requiring cooperation with the power to impose fines and penalties for non-compliance with these

---

[139] *See id.*, art. 56 (1).
[140] *See id.*, art. 56 (6)
[141] *See id.*, art. 49 (1).
[142] *See id.*, art. 49 (2).
[143] *See id.*

investigations.[144] As a reserve measure, DSCs may request that national judicial authorities restrict access to the service when there is a threat of severe harm or a potential criminal offense involving a danger to life and safety.[145]

Focusing on national law and competent national authorities generates intriguing questions for enforcement and how the DSA will bridge conflicting statutes. The first of these questions is how the DSA will approach legal content in one Member State and illegal in another. The second is how the DSA will reconcile laws requiring conflicting actions, such as information that national law requires disclosure of in one Member State where sharing this same information is illegal in another Member state. To avoid some of these conflicts, or at least work through them, the DSA provides co-competency to two other bodies to help coordinate regulation amongst Member States, the European Board for Digital Services ("the Board") and the European Commission.[146]

The Board does not have jurisdiction over a specific enforcement authority but instead acts in an advisory capacity to support the enforcement of the DSA.[147] The members of the Board are the national DSCs, and the European Commission chairs it.[148] The Board's responsibilities are to support joint investigations and the audits of VLOP and VLOSE, issue advisory opinions, and advise the Commission on its regulation of VLOP and VLOSE.[149] The recommendations and advice of the Board are not binding on the other authorities under the DSA.[150] Instead, if they do not follow the Board, they must provide the reason for their decision and outline what actions they plan to take.[151]

---

[144] *See id.*, art. 51 (1)(a)-(c); (2)(a)-(e).
[145] *See id.*, art. 51 (3)(a)-(b).
[146] *See id.*, art. 57.
[147] *See id.*, art. 61(1).
[148] *See id.*, art. 62(1)-(2).
[149] *See id.*, art. 63 (1)(a)-(e).
[150] *See id.*, art. 63 (2).
[151] *See id.*

Finally, perhaps most importantly, is the European Commission's role in enforcing the DSA. The Commission holds jurisdiction over the obligations imposed on VLOP and VLOSE due to their size and the complexity of managing the impact on the internal market from these large companies[152]. In conjunction with the Board, the Commission is responsible for developing the code of conduct that guides the due diligence obligations of Chapter III § 6.[153] The Commission's duties include the due diligence, risk assessments, audits, and transparency requirements imposed on VLOP and VLOSE.[154] However, this sequestration of responsibility for VLOP and VLOSE is not as complete as it may appear. For VLOP and VLOSE established within the Union, the Member State of their location may enforce the regulation where the Commission did not act. Thus, the Commission and the Member State of the provider's establishment share jurisdiction to ensure compliance with obligations.[155]

The drafters of the DSA have attempted to provide a harmonized approach to regulation by circumventing the Member States regarding the most impactful and large companies.[156] These three institutions form the regulatory framework for the implementation of the DSA. Unlike the GDPR and ECD, which rely on the country of origin of the transmission or content to determine jurisdiction, the DSA gives the Commission direct authority with a global impact. [157] However, the DSA acknowledges Member State's sovereignty by allowing them to regulate those companies within their borders.[158] This construction has not solved all the issues of implementing previous regulations, and the new arrangement brings many further questions.

---

[152] *See id.*, at recital 48.
[153] *See id.*, art. 56(2)
[154] *See id.*
[155] *See id,* art. 56(4).
[156] *See id.*, at recital 48.
[157] *See id.*, art. 56(2).
[158] *See id.*, art. 56(1); art. 56(4).

B. Has the EU Learned from the Mistakes of Past Regulations?

Like the answer to almost all-important questions, it depends on whom one asks. The DSA introduces Union-wide coordination in the form of the powers of the Commission.[159] However, the Board functions as the only structural means of coordination among the Member States.[160] Nevertheless, none of its recommendations or advice for how states can coordinate their actions are binding. Because of this, the DSA's purported multilateral format for enforcement will likely devolve into a bilateral give-and-take between the national DSCs and the Commission, with the Board acting as a near-ornamental third party.

During the crafting of the DSA, two camps existed concerning jurisdiction over providers. These camps differed in whether they believed jurisdiction should arise from the origin or the point of destination. [161] There are issues with enforcing the DSA due to similar competencies as those in the GDPR regarding the state of establishment. States where providers establish carry enforcement burdens that delay the entire system. For example, Ireland is the place of establishment for many top US tech companies.[162] This concentration results in outsized responsibility for enforcing the regulation, which some claim has created a bottleneck in the entire enforcement system.[163]

In a 2021 report, the Irish Council for Civil Liberties found that one-fifth of all complaints referred under the GDPR go to Ireland, and seven nations in the EU receive 72% of all complaints.[164] This heavy concentration creates dual problems. First, the enforcement systems within Ireland are overworked as they receive the lion's share of complaints leading

---

[159] *See id.* art. 65; art. 66.
[160] *See id*. art, 63(1)(a)
[161] *See* Luca Bertuzzi, *Ireland draws a red line on country of origin principle in DSA*, WWW.EURACTIV.COM (2021), https://www.euractiv.com/section/digital-single-market/news/ireland-draws-a-red-line-on-country-of-origin-principle-in-dsa/.
[162] *See* Catherine Barrett, *Emerging Trends from the First Year of EU GDPR Enforcement*, 16 Scitech Lawyer 22 (2020).
[163] *See* Johnny Ryan, *Europe's enforcement paralysis: ICCL's 2021 GDPR report*, Irish Council for Civil Liberties (2021), https://www.iccl.ie/digital-data/2021-gdpr-report/ (last visited Dec 6, 2022).
[164] *Id.*, at 4 (showing the disparity in complaints with the highest recipients being Ireland, Germany, France, Netherlands, Luxembourg, Sweden, and Spain).

to lessened enforcement overall. Second, this creates an incentive for under-enforcement as the concentration of tech companies within one nation is an economic boon for a country. Thus, national regulators are less incentivized to enforce regulations as this may lead to companies incorporating elsewhere.

In July 2022, Commissioner for the Internal Market Theirry Breton, the man in charge of EU digital policy in Brussels, released an outline of the implementation priorities of the DSA. This outline included a plan to massively expand the Commission's internal organization to support its monitoring obligations and establish a Centre for Algorithmic Transparency to oversee platform transparency and data obligations.[165] As of December 2022, the Commission has released no implementing or delegating acts for public consideration. With all of these future decisions in the air, once a political agreement is reached on the number of necessary implementing and delegating acts, the Digital Services Act may look like an entirely new piece of regulation.

The DSA leaves to future implementing acts many important specifics regarding how it will operate in essential areas, such as: establishing procedures to meet transparency obligations,[166] determining the methodology for counting a platform's active users,[167] setting processes for the audits of VLOP and VLOSE,[168] determining when VLOP and CLOSE must share data,[169] creating a methodology for the assessment of supervisory fees on VLOP and VLOSE.[170] These are all critical areas that will likely provide opportunities for further dissolution of the regulation's strength due to the other debate, political compromise, and

---

[165] *See* European Commission, Sneak peek: how the Commission will enforce the DSA & DMA - Blog of Commissioner Thierry Breton, EUROPEAN COMMISSION https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_4327.
[166] *See* Regulation 2022/2065, art. 24(6), 2022 O.J. (L. 277).
[167] *See id.*, art. 33 (3)
[168] *See id.*, art. 37 (7)
[169] *See id.*, art. 40 (13) (note this action involves the Commission consulting the Board as well)
[170] *See id.*, art. 43 (3)-(4)

chance for lobbying crafting these implementing acts will bring. For example, with the definition of active users in an online marketplace, there is disagreement concerning whether this should only include viewers or actual buyers.[171] While less of a threat of dissolution and more of another impediment to implementation, the DSA also leaves the system for sharing information between DSCs and the Commission for future implementing acts.[172]

Overall, the DSA focuses more on creating a check against gridlock, which has hampered the efficacy of the GDPR, by having the Commission directly oversee VLOP and VLOSE. However, the lack of specificity in the DSA regarding how Member States and the Commission will coordinate their efforts when joint jurisdiction arises raises concerns about their ability to forge consensus and what the options are when they do not reach an agreement. Finally, the differences between the laws of member states create uncertainty for smaller providers, particularly when it comes to removing content.

VI. CONCLUSIONS AND RECOMMENDATIONS

The Digital Services Act will undoubtedly cause a massive change in how individuals interact with the providers of online services, whether they are social media websites, online marketplaces, or even providers of internet services. To see how the Digital Services Act will impact online spaces, one can look at the massive increase in hate speech on Twitter after its new owner's shift toward unmoderated areas[173] and consider that this laissez-faire approach would bring substantial repercussions for the platform under the DSA both financially and potentially for its ability to continue operation in Europe. Commissioner Breton has already

---

[171] Mathilde Adjutor, *Online Marketplaces: What EU Lawmakers Will Look at Next*, Disruptive Competition Project (2022), DISRUPTIVE COMPETITION PROJECT, https://www.project-disco.org/european-union/090822-online-marketplaces-what-eu-lawmakers-will-look-at-next/ (last visited Dec 6, 2022).
[172] *See* Regulation 2022/2065, art. 85(3), 2022 O.J. (L. 277).)
[173] *See* Sheera Frenkel & Kate Conger, *Hate Speech's Rise on Twitter Is Unprecedented, Researchers Find*, THE NEW YORK TIMES, December 2, 2022, https://www.nytimes.com/2022/12/02/technology/twitter-hate-speech.html.

warned Twitter about ensuring compliance with the DSA.[174] The Commission must resist the temptation to cave to the power of the tech lobby, particularly as they craft implementing legislation, lest they risk undermining the hard work put into preparing the world's most robust framework for regulating online services.

While this paper concludes that the DSA does not violate freedom of expression, as aforementioned, this is due to a restrictive definition of this fundamental freedom under the Charter. Member States may derogate the freedom of expression for a broad range of reasons, a stance which the CJEU does not appear ready to reverse in hindsight of its Facebook Ireland decision. The DSA does commit to respecting fundamental freedoms, particularly in its requirements for VLOP and VLOSE to consider fundamental rights in their execution of risk mitigation.[175] Nevertheless, this commitment does not entail a binding legal obligation with specific standards to which these platforms can be held accountable. The DSA leaves this to the implementing acts.

The EU considered the challenges it faced implementing the GDPR when crafting the DSA and attempted to circumvent some of these issues. Concerning the divergence between the Member States in implementing the GDPR, the concentration of power in the Commission hopes to solve this problem. However, this may replace the current discord between Member States with friction between Member States and the Commission. Whether the DSA will succeed in its goals of harmonizing the rules for the internet is left to the implementation. For now, companies and consumers must familiarize themselves with this new landscape, lest they find themselves lost within the new complex web this regulation creates.

---

[174] See Brian Fung, *Twitter must comply with Europe's platform rules, EU digital chief warns Musk in virtual eeting | CNN Business*, CNN (2022), https://www.cnn.com/2022/11/30/tech/twitter-eu-compliance-warning/index.html. ("Twitter will have to implement transparent user policies, significantly reinforce content moderation and protect freedom of speech, tackle disinformation with resolve, and limit targeted advertising")
[175] *See* Regulation 2022/2065, art. 35(1), 2022 O.J. (L. 277).