FOREWORD

Jennifer M. Urban[†]

I. INTRODUCTION

After more than two decades of the "notice-and-takedown" approach to online copyright infringement and content moderation, the European Union (EU) has moved away from this familiar regime and toward a broader regulatory approach with the Directive on Copyright and Related Rights in the Digital Single Market (CDSMD) and the Digital Services Act (DSA). The Berkeley Center for Law and Technology and the *Berkeley Technology Law Journal*'s 27th Annual Symposium considers this potentially profound shift in copyright enforcement and content moderation policy. On April 6th and 7th, 2023, scholars, policymakers, and industry participants from both Europe and the United States joined in discussion to consider potential benefits and risks of the EU's new approach and whether a new EU/US consensus—or, perhaps, a "Brussels Effect" on US platform liability debates—is likely.

On the first day of the symposium, European experts presented valuable tutorials explaining the architecture of the DSA and the complexities of its core features. They provided US attendees with a map of the DSA's role in the European context, a blueprint of its structure, a breakdown of its interactions with the CDSMD, a comparison to previous approaches, and an analysis of its potential effects on free speech.[1]

On the second day, US experts joined European experts on a series of panels considering how the DSA affects online service providers' responsibilities, what the intended and unintended consequences of the DSA

DOI: https://doi.org/10.15779/Z38697001X

† Clinical Professor of Law at University of California, Berkeley, School of Law; Director of Policy Initiatives, Samuelson Law, Technology & Public Policy Clinic; Co-Director, Berkeley Center for Law and Technology (BCLT). Opinions are my own and should not be attributed to my institution, the California Privacy Protection Agency, or the California Privacy Protection Agency Board. This conference was a transatlantic group effort. Thank you to Professors Martin Senftleben and João Pedro Quintais of the Institute for Information Law (IViR) at the University of Amsterdam and Professors Pam Samuelson and Erik Stallman at UC Berkeley, to the expert BCLT staff, and to the team at the *Berkeley Technology Law Journal.*

1. *27th Annual BTLJ-BCLT Symposium: From the DMCA to the DSA—A Transatlantic Dialogue on Online Platform Liability and Copyright Law Agenda*, BERKELEY LAW (Apr. 6–7, 2023), https://www.law.berkeley.edu/research/bclt/bcltevents/from-the-dmca-to-the-dsa-a-transatlantic-dialogue-on-online-platform-liability-and-copyright-law/agenda/.

may be on fundamental rights, and whether the DSA will influence firm behaviors beyond the EU via a "Brussels Effect."[2]

Attendees also heard from a panel of industry experts on industry perspectives, and benefited from keynote addresses by officials from both sides of the Atlantic. Irene Roche-Laguna, a European Commission official who was key to developing the DSA, discussed the DSA's origins, and goals.[3] She pointed out that the DSA attempts to address a host of critiques of notice-and-takedown, many originating from the US. She asserted: "This is your baby."[4] Shira Perlmutter, the Register of Copyrights for the US, discussed how emerging technologies are currently affecting copyright policy. Among other examples, she walked the audience through the Copyright Office's recent analysis of copyright issues related to generative artificial intelligence technologies.[5]

The five papers in this symposium edition of the *Berkeley Technology Law Journal* both helped constitute this cross-Atlantic discussion and grew from it. They offer viewpoints from both sides of the Atlantic, highlighting potential benefits and risks in the EU's new approach. As Europe moves away from liability rules premised on notice-and-takedown processes and toward horizontal "due diligence" and "accountability" requirements, these papers offer background, optimism, pessimism, and critique. Brief introductions to their rich analyses follow.

II. HUSOVEC: THE DSA AS A BLUEPRINT

In "Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules," Martin Husovec, of The London School of Economics and Political Science, analyzes the DSA as the "first comprehensive attempt to create a second generation of rules for digital services that rely on user-generated content."[6] Though recognizing that some of the regulation's features may be too Europe-specific to travel, Husovec argues that "the principles behind the DSA could be useful in other jurisdictions—perhaps even in the United States" by serving as "the basis for

2. *Id.*

3. *Id.*

4. *See* author's note (on file with author).

5. *27th Annual BTLJ-BCLT Symposium: How Are Emerging Technologies Affecting Copyright Policy?*, BERKELEY LAW, https://bk.webcredenza.com/watch?id=85216 (last accessed Jan. 10, 2024).

6. Martin Husovec, *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, 38 BERKELEY TECH. L.J. 882 (2023).

a dialogue between liberal democracies about how to best regulate user-generated content services."[7]

Husovec first traces a history of the DSA's foundations, highlighting the influence of section 512 of the US Digital Millennium Copyright Act (DMCA) on the European E-Commerce Directive and the EU's ensuing "conditional immunity" approach to service provider liability for user-generated content.[8] Husovec praises this approach as a structurally sound method of encouraging the growth of decentralized communication networks, arguing that, via liability exemptions, "everyone commits to constraining themselves in order to facilitate the emergence of an environment from which everyone can benefit."[9]

But, Husovec argues, today this structure "seems insufficient when the clear legislative goal of the liability exceptions was to lay down incomplete and unrestrictive rules that would allow the medium to flourish." We are now in a world of "many societal challenges that require solutions," a task that, in Husovec's view, cannot be completed via liability exemptions alone.[10]

This brings us to the DSA, which Husovec characterizes as resting on "two pillars": due process requirements for content moderation and risk management obligations for service providers.[11]

As to the first, Husovec stresses that the DSA regulates the process by which service providers make content moderation decisions, not the underlying rules for what content is acceptable. Those rules (for lawful content) remain in service providers' hands.[12] Husovec sees the DSA's process requirements as a way of addressing underinvestment by service providers in content moderation decision-making.[13]

The DSA then imposes another layer of regulation—risk mitigation requirements—on online platforms, very large online platforms (VLOPs) and very large online search engines (VLOSEs).[14] The services that fall into these categories must avoid manipulative product design generally, and must consider the effects of their product design on children specifically. The largest services are treated as "public squares" and must make additional risk mitigation efforts; these include engaging in dialogue with regulators about risks to both individual freedoms and democratic institutions.[15] Husovec sees

7. *Id.* at 887.
8. *Id.* at 883–87.
9. *Id.* at 893.
10. *Id.* at 897.
11. *Id.* at 899.
12. *Id.* at 901.
13. *Id.*
14. *Id.* at 900–1.
15. *Id.*

this approach as a recognition of the importance of product design in outcomes and of longstanding asymmetries of information and resources between firms and regulators.[16] At the same time, he recognizes that regulatory attempts to address systemic risk in this way invite suppressing individual expression, especially for "lawful but harmful" content.[17] Husovec considers the key question to be who—regulators or firms "sets the boundaries for the content of communications."[18] In his view, the DSA leaves room for firms to make decisions about legal content, while incentivizing investment in good decisionmaking.

Husovec advocates for other jurisdictions to be guided by five "principles" that he has extracted from the DSA: accountability not liability; horizontality; shared burden; empowerment; and ecosystem solutions.[19]

As to *accountability not liability*, Husovec argues that platforms "as facilitators of user-generated content cannot be expected to bear the liability burden of ordinary publishers."[20] But, he argues, they should be "more accountable" for protecting "individual grievances " by exercising due diligence.[21] He finds the DSA's model superior to liability limitations alone because "[i]n the liability framework, the lack of diligence puts providers at risk of being an accessory to the entire wrongs of others. On the other hand, the accountability framework blames them only for not giving some specific assistance."[22] "Accountability not liability" ties to the principle of *shared burden*, which Husovec summarizes as "everyone is expected to play their part" to limit speech risks. He argues that this principle can be fulfilled by using both liability exemptions and accountability mechanisms to allocate responsibilities.[23] In turn, the principle of shared burden ties to the principle of *user empowerment*, which Husovec uses to argue for users to share risks—but only so far as they are able to counter those risks.[24] The DSA's due diligence obligations, in his view, encourage firms to provide users with the necessary tools.[25]

Husovec is even more complimentary toward the *horizontality* of the DSA, calling it a "digital civil charter that shines through the entire legal system and radiates minimum rights of individuals," regardless of the specific EU

16. *Id.* at 904–5.
17. *Id.* at 906–8.
18. *Id.* at 906.
19. *Id.* at 909.
20. *Id.*
21. *Id.* at 910.
22. *Id.* at 911.
23. *Id.* 913–14.
24. *Id.* at 914–15.
25. *Id.*

jurisdiction.[26] The DSA also sweeps broadly across legal sectors; Husovec argues that this tamps down regulatory arbitrage and forces regulators to consider tradeoffs across the entire landscape of online speech.[27] And relatedly, Husovec compliments the DSA for, in his view, employing the final principle of *ecosystem solutions*. The DSA both sweeps across jurisdictions and sweeps in multiple actors. Husovec argues that previous regimes exhibited a "preoccupation with [online service] providers," giving "little consideration" to others, such as "trusted NGOs . . . fact-checkers, journalists, or researchers."[28] The DSA's allowances for "trusted flaggers," information-sharing, and research will, in Husovec's view, be highly beneficial if they are implemented fully.[29]

Accordingly, in Husovec's analysis, the DSA, if properly implemented, promises to support user-generated content, while "inject[ing] trust" into the system.[30]

III. TUSHNET: RIGHTSIZING REGULATION THROUGH TEST SUITES

In "Three Sizes Fit Some: Why Content Regulation Needs Test Suites," Rebecca Tushnet of Harvard Law School takes a more skeptical view, identifying potential weaknesses in the DSA's novel structure. In Tushnet's assessment, the DSA fails in one of its key features: establishing size-based tiers of online service providers and then differentially imposing obligations by tier. This feature of both the DSA and CDSMD is intended to tailor obligations to relative risk and resources. Yet Tushnet considers them "totalizing," and likely to "damage a thriving online ecosystem," because they fail to capture the true variation within that ecosystem.

Tushnet's skepticism begins at the first gate: establishing the "size" of service providers in order to sort them into regulatory tiers.[31] The DSA requires providers to count monthly active users who have "engaged" with the service for this purpose.[32] Yet, Tushnet points out, there is inherent ambiguity in the required metric. Further, the metric raises potential privacy issues: not all platforms "extensively track users," as not all seek to monetize or prolong

26. *Id.* at 912.
27. *Id.* at 912–13.
28. *Id.* at 917.
29. *Id.* at 918–20.
30. *Id.* at 920.
31. Rebecca Tushnet, *Three Sizes Fit Some: Why Content Regulation Needs Test Suites*, 38 BERKELEY TECH. L.J. 921 (2023).
32. DSA Art. 3(p).

visits.[33] Tushnet points to Wikipedia, the Organization for Transformative Works' Archive of Our Own, and DuckDuckGo as examples of service providers for which the risk of bad behavior seems low, but the potential costs of tracking seem high.[34]

Tushnet also considers the DSA's extensive due process requirements too generalized, and at risk of creating unintended consequences. She points out, for example, that the requirements—which include individualized explanations of platform decisions and a redress process—apply equally to brief comments and longform content, and to acts ranging from demonetization, to removing an "a politician's entire account," and on "to downranking a single post by a private figure."[35] Coupled with protections against bad-faith actors that are, in Tushnet's view, inadequate, particularly in light of demographic differences in who is likely to be willing to use redress systems, this design may lead service providers to reduce their efforts to moderate "lawful but awful" content. Further, the cost of the DSA's requirements could create anticompetitive barriers to smaller and newer market actors.[36]

In Tushnet's analysis, these challenges arise from a regulatory myopia that prompts regulators to focus on "the giant names they know" when crafting regulations. To ameliorate this issue, she argues for regulators to use "test suites" to explore varying types of online service providers, the risks (or relative lack of risk) they present, and the different challenges they face. In her view, "true proportionality" is achievable only with closer attention to the actual diversity of online service providers.[37]

IV. SENFTLEBEN, QUINTAIS, AND & MEIRING: HUMAN RIGHTS IMPLICATIONS OF PLATFORM REGULATION

Martin Senftleben, João Pedro Quintais, and Arlette Meiring, from the University of Amsterdam, complement Tushnet's critique with a detailed analysis of the human rights implications of the CDSMD and DSA, focusing on monetization. In "How the European Union Outsources the Task of Human Rights Protection to Platforms and Users: The Case of User-Generated Content Monetization," the authors take as case studies the content monetization remedies several major providers allow large rightholders to exercise against user-generated content (UGC). These examples illustrate what

33. Tushnet, *supra* note 31, at 924.
34. *Id.* at 923–25.
35. *Id.* at 926–27.
36. *Id.* at 929.
37. *Id.* 930–32.

the authors view as human rights issues created by design deficits in the CDSMD and the DSA.

The authors first offer a detailed analysis of the intricate interaction between the CDSMD and the DSA, highlighting human rights implications. They identify two main human rights effects, which they term *outsourcing* and *concealing*.[38]

Outsourcing stems from the laws' failure to include "concrete solutions for human rights tensions in the law itself."[39] Instead, the law "outsources" safeguards for fundamental rights to private parties—online platforms, in cooperation with the creative industry, and activist users.[40] For example, the DSA requires UCG platforms to "act in a diligent, objective and proportionate manner . . . with due regard to . . . the fundamental rights of [users]"—thus outsourcing the protection of fundamental rights to platforms.[41] The DSA also requires platforms to inform users about how they approach content moderation, including via algorithmic decision-making.[42] And platforms must provide internal systems for handling complaints about content moderation decisions, and information about those systems.[43] The authors take these and similar requirements as evidence of outsourcing not just to platforms, but also to users, who are expected to understand the platforms' policies and use the platforms' systems "to play an active role in the preservation of their freedom of expression and information."[44]

The authors are skeptical about whether legislators can "legitimately 'outsource' the obligation to safeguard fundamental rights" in this way.[45] In part, this is because leaving so much responsibility to private parties may conceal human rights issues from view. For example, both the CDSMD and the DSA rely on user complaints to identify problematic content blocking or removal. But, the authors point out, a "low number of user complaints . . . may be misinterpreted as an indication that content filtering hardly ever encroaches upon freedom of expression and information."[46] Instead, cumbersome complaint procedures and other barriers make it "unrealistic to assume that"

38. Martin Senftleben, João Pedro Quintais, & Arlette Meiring, *How the European Union Outsources the Task of Human Rights Protection to Platforms and Users: The Case of User-Generated Content Monetization*, 38 BERKELEY TECH. L.J. 933, 943–73 (2023).
39. *Id.* at 943.
40. *Id.* at 943–55.
41. *Id.* at 941.
42. *Id.* at 939–40.
43. *Id.* at 941.
44. *Id.*
45. *Id.* at 942.
46. *Id.* at 957.

user complaints "reveal[] the full spectrum and impact of free expression restrictions" at issue.[47] Problems may exist, but may be hidden by practical limitations on users' ability to affirmatively assert their rights.

Overall, the authors see in the CDSMD and the DSA "a worrying tendency of reliance on industry cooperation and user activism to safeguard human rights."[48] Though the Court of Justice for the European Union has guarded free expression by "stating unequivocally" that filtering systems must "be capable of distinguishing lawful from unlawful content,"[49] the Court "did not seize the opportunity to unmask human rights risks . . . inherent in the [CDSMD's] heavy reliance on industry cooperation," nor did it address the "human rights risks that could arise from the ineffectiveness of complaint and redress mechanisms for users."[50] The authors do find promise in the DSA's audit provisions, which could return some responsibility for protecting human rights to the European Commission. Accordingly, the audit provisions "must not be underestimated" as "a promising counterbalance to outsourcing/concealment risks."[51] Still, it remains unclear whether the audit requirements will fulfil this promise. Ultimately, both the intended protections for lawful uses in Article 17(7) of the CDSMD and the audit requirements contained in the DSA are too "underdeveloped" to fully counter the authors' concerns.[52]

The authors then apply their analysis to one method of content moderation: monetization programs. As the authors point out, content removal and blocking/filtering garner much more attention from commentators, but 'monetization'—the opportunity to capture "advertising revenue that accrues from the continued online availability of UGC"—is a very popular choice for rightholders who have access to it.[53] Indeed, the authors report, rightholders eligible for YouTube's ContentID chose monetization as the remedy for over 90% of claims made over a six-month period.[54] Yet the CDSMD "largely ignores the topic" of monetization.[55] The DSA does include "demonetization" in its framework, including it specifically in the set of negative actions users (or others) can appeal through platforms' complaint

47. *Id.* at 959.
48. *Id.* at 973.
49. *Id.* at 964 (citing CJEU, 26 April 2022, case C-401/19, Poland v Parliament and Council).
50. *Id.* (citing CJEU, 26 April 2022, case C-401/19, Poland v Parliament and Council).
51. *Id.* at 972.
52. *Id.* at 973.
53. *Id.*
54. *Id.* at 986 (internal citations omitted).
55. *Id.* at 974 (internal citations omitted).

systems.[56] Still, the authors view the DSA as addressing monetization "at a superficial level, mostly by outsourcing its regulation to private parties."[57] Due to this outsourcing, the authors point out, the "workings of [monetization systems] are mostly concealed behind complex terms and conditions and opaque algorithmic systems" employed by platforms in cooperation with rightholders.[58]

After undertaking a thorough review of (the admittedly limited) publicly available information about several large companies' [59] approaches to monetization, the authors conclude that outsourcing monetization remedies to private actors leads to, and conceals, at least three important human rights issues. First, major rightholders can appropriate and exploit transformative UGC, invading and "usurp[ing] this freedom of expression space."[60] Second, relatedly, misappropriating user creativity in this manner encroaches on the user's fundamental right to property by treading on the user's intellectual property rights.[61] And third, favoring large-scale rightholders over user-creators "gives rise to the question of whether it violates the principle of equal treatment" in the Charter of Fundamental Rights of the European Union.[62]

Accordingly, though the DSA contains some promising features, Senftleben, Quintais, and Meiring consider it insufficient to the task of protecting human rights. They call for collective licensing with "non-waivable remuneration" for UGC creators, and for a general redesign of monetization systems to benefit user-creators as well as large rightholders.[63]

V. GRIMMELMANN & ZHANG: AN ECONOMIC MODEL OF INTERMEDIARY LIABILITY

In "An Economic Model of Online Intermediary Liability," James Grimmelmann and Pengfei Zhang take a different tack. Rather than focusing on the DSA from the outset, these authors take a step back in order to "clarify the terms of the debate" over how best to structure intermediary liability by developing a generalized economic model.[64] They argue that standardizing

56. *Id.* at 982–83 (internal citations omitted).
57. *Id.* at 974.
58. *Id.*
59. The authors review YouTube, Meta, TikTok, and third-party offerings from Audible Magic and Pex. *Id.* at 984–98.
60. *Id.* at 1000.
61. *Id.* at 1004.
62. *Id.* at 1006.
63. *Id.* at 1010.
64. James Grimmelmann & Pengfei Zhang, *An Economic Model of Online Intermediary Liability*, 38 BERKELEY TECH. L.J. 1011, 1013 (2023).

arguments into a formal economic model promotes communication, intuition, visualization, rigor, proof, and empiricism.[65] By standardizing the terms of the debate and making its assumptions explicit, the authors believe, they can order and improve the intermediary liability debate. They then use their model to compare the relative benefits and drawbacks of different approaches to platform regulation, including section 230 of the US Communications Decency Act, and section 512 of the DMCA, and the DSA.[66]

Reviewing the available literature on platform liability, the authors find that there is very little formal economic analysis; varied views on the best approach (ranging from no liability, to conditional liability, to strict liability (or even criminal liability) for certain harms); and some descriptive empirics on platform behavior.[67] But there is an "immense" literature exploring economic theories of liability.[68]

Drawing on this literature, Grimmelmann and Zhang seek to determine which is economically optimal: "online intermediary liability" or "online intermediary immunity."[69] They take as initial assumptions two observations: platforms have *imperfect information* about the harmfulness of content they host; and content can have *positive externalities* that go beyond the benefits the platform can internalize. Taken together, these features of the online content ecosystem, they argue, could plausibly cause platforms to overmoderate.[70]

Relying on these assumptions, the authors illustrate the uncertainty platforms face with a simple probability model. Any given piece of content carries a probability of being harmless or harmful. Platforms do not know whether a given piece of content actually is harmful, but they can know something about the probability that it is.[71] The authors then include the probabilities of various consequences flowing from hosted content: that the platform receives some benefit; that society receives some benefit; and that harmful content causes someone harm. To sharpen the model, they assume that there exists some set of "good" content that benefits the platform, benefits society, and is always harmless. Likewise, they assume that there exists some set of "bad" content that is bad for society and always harmful. This allows them to visualize a "moderation threshold" at which a rational moderator will shift from removing content to leaving it up, along with

65. *Id.* at 1013–14.
66. *Id.* at 1060–64.
67. *Id.* at 1014–18.
68. *Id.* at 1014.
69. *Id.*
70. *Id.* at 1019.
71. Later, the authors add options for costless and costly investigations of content by platforms. *Id.* at 1032–39.

changes in platform profit, social benefit, and social harm as the threshold shifts.[72]

Armed with this model, the authors test various models of liability. Giving platforms *blanket immunity*, perhaps surprisingly, can result in both undermoderation (where platforms leave up too much harmful content) and overmoderation (where platforms remove too much socially beneficial content). This is because platforms don't fully internalize the benefits of hosted content (and so might remove content that benefits society), and also don't internalize harms suffered by third parties (and so might leave up harmful content).[73] On the other hand, imposing *strict liability* on platforms always causes overmoderation, a conclusion the authors can nicely demonstrate with their model.[74] The authors complicate the picture by testing the effects of platforms engaging in *costless investigations* (which are always to the good) or *costly investigations* (which will cause some overremoval).[75]

Clarifying assumptions and formalizing policy components in this way allows the authors to compare different policy approaches to content moderation. Regulators wishing to address undermoderation have a few traditional tools to choose from. They could impose liability based on *actual knowledge* by the platform of harmful content; the authors consider this option to be an improvement over strict liability if "actual knowledge" is not distorted into a lower threshold (at which point platforms begin to overmoderate).[76] Regulators could impose *liability on notice* from victims, which leaves some uncompensated harm (due to victims' investigation costs), but at first appears to enhance social welfare.[77] However, if victims can shirk proper investigation and send notices for content that is not harmful, then liability on notice "might collapse into strict liability" because the bad notices "are of no use to the platform in distinguishing harmful from harmless content," but still trigger strict liability for the platform.[78] This is an observed problem with section 512 notice-and-takedown that likely causes overmoderation.

Regulators could also impose standards-based models of liability. They could turn to *negligence* and impose a standard of care that requires some amount of investment by platforms in preventing harm.[79] This can run into

72. *Id.* at 1019–25.
73. *Id.* at 1025–29.
74. *Id.* at 1029–32.
75. Note: here I have radically simplified seven pages of close and careful reasoning. *Id.* at 1032–39.
76. *Id.* at 1045–46.
77. *Id.* at 1046–47.
78. *Id.* at 1047.
79. *Id.* at 1049–53.

difficulty because it's difficult to choose the optimal standard.[80] Or regulators could create *conditional immunity* by setting a threshold of harm and providing immunity to platforms that don't cross it.[81] These methods sound very similar, but are distinct because negligent platforms are liable for specific pieces of content for which they didn't exercise sufficient care, while platforms that lose conditional immunity lose it for all content by blowing their harm "budget."[82]

After briefly considering approaches to overmoderation (subsidies and must-carry requirements),[83] the authors use their findings to evaluate existing and proposed approaches.[84] In their model, Section 230 functions as blanket immunity for the content it covers, and reform proposals vary.[85] The Citron-Wittes proposal, which turns on overall moderation efforts, is a conditional immunity approach. Efforts to impose common-law distributor liability function as liability on notice. And the Platform Accountability and Consumer Transparency Act would impose liability on notice, but where relevant "notice" requires a court order. The model allows some important trade-offs inherent in these approaches—for e.g., the cost of investigations, or the loss or accrual of social benefits—to be made explicit and compared.

The authors' model is especially helpful in bringing analytical order to the hodge-podge that is section 512 of the DMCA. According to their analysis, section 512 combines multiple approaches, starting with blanket immunity, but then adding five exceptions, each a different "flavor" of liability.[86] First, the platform loses immunity with actual knowledge.[87] Second, it loses immunity if it fails to remove infringing material when it has a sufficient level of awareness (negligence).[88] Third, it loses immunity if it has the ability to control and is strongly under-investing in investigations[89] Fourth, the platform loses immunity if it receives a notice of claimed infringement and fails to remove it (liability on notice).[90] Finally, it loses immunity if it fails to ban "repeat infringers" according to some threshold. This exception, the authors point out, has functioned as a conditional immunity standard, with some platforms staying on the "safe" side of the harm threshold while others (most famously,

80. *Id.* at 1052.
81. *Id.* at 1053–55.
82. *Id.* at 1054.
83. *Id.* at 1055–61.
84. *Id.* at 1061–65.
85. *Id.* at 1061–62.
86. *Id.* at 1062–64.
87. *Id.* at 1062.
88. *Id.* at 1062–63.
89. *Id.* at 1062.
90. *Id.*

Cox Communications) ending up on the wrong side of the line and thus, without immunity for their users' infringement.[91]

Informed by their model, the authors find several things to like in the DSA's approach.[92] First, it more sharply distinguishes between "mere conduits" and "hosting providers" than the DMCA does. Under the DSA, and like the DMCA, conduits have no content moderation requirements. However, the DSA does not, in the authors' view, condition platforms' immunity on terminating repeat infringers. Nor does it have vicarious-liability-like provisions. This approach more cleanly focuses content moderation responsibilities on hosting providers, which are subject to notice-and-takedown requirements.[93] The authors also compliment the DSA's "trusted flagger" system, which sets an investigation standard for trusted flaggers to meet. They characterize this a "clever response to the signaling problem" evident in the DMCA (which lacks sufficient disincentives to sending under-investigated notices).[94] Finally, the DSA, like section 230 of the CDA, neither requires platforms to actively monitor hosted content nor punishes them for investigating and moderating. Together, this "prevent[s] the *Stratton Oakmont* trap," in which platforms could face strict liability for all harmful content if they remove any at all.[95]

VI. CHANDER: GLOBAL EFFECTS OF THE DSA

In his essay, "When the Digital Services Act Goes Global," Georgetown University's Anupam Chander argues that the DSA is likely to influence jurisdictions beyond Europe via a "Brussels Effect" and considers the ensuing risk to civil society and freedom of expression.[96]

Chander considers it likely that the DSA will "likely carry a Brussels Effect, both de facto through changes in the practices of multinational corporations, and de jure through changes in foreign law."[97] He does not delve deeply into the details, but follows Dawn Nunziato in pointing out the DSA's extraordinary financial enforcement mechanisms—fines of up to six percent of a targeted platform's worldwide turnover—as a source of pressure on firms

91. *Id.* at 1055 (internal citations omitted).
92. *Id.* at 1064–65.
93. *Id.*
94. *Id.* at 1064.
95. *Id.*
96. Anupam Chander, *When the Digital Services Act Goes Global*, 38 BERKELEY TECH. L.J. 1067, 1067–68 (2023).
97. *Id.* at 1071.

to err on the side of European norms when developing content policies.[98] He also points out firms might find it convenient to standardize content policies in response to the DSA's transparency requirements,[99] and that European regulators have stated that they hope to effect "global standards" through the DSA and DMA.[100]

More important to Chander, however, is his view that governments "might find much to envy in the Digital Services Act" leading to a so-called "de jure" Brussels Effect as governments adapt their laws to reflect the DSA.[101] Whereas European leaders hope to encourage "democracy, fundamental values, and the rule of law,"[102] Chander worries that some of the DSA's mechanisms may have very different effects in the hands of "governments with authoritarian tendencies."[103]

To analyze these possible effects, Chander sets a "Putin Test" for various aspects of the DSA.[104] In essence, he asks, "What would Putin do?" with each mechanism. First up are the DSA's Digital Services Coordinators—national regulators who are to be established in each European Member State. Chander points out that the Digital Services Coordinator is entrusted with substantial powers that touch on speech, including choosing "trusted flaggers," investigating user complaints, requesting information from VLOPs and VLOSEs, choosing "vetted researchers," ordering content removal, and issuing those extraordinary six-percent fines.[105] Though the DSA imposes constraints on each of these activities to ensure the protection of fundamental rights, Chander points out that an interested Digital Services Coordinator could act in accordance with narrow political, personal, or ideological preferences to harass platforms or otherwise use its power to achieve anti-democratic goals.[106] Next, Chander worries about the DSA's establishment of emergency powers and its requirement that all EU-serving intermediaries designate local EU representatives. Emergency powers create the potential for abusive government coercion, as do requirements to place a representative within physical reach.[107]

98. *Id.* (internal citations omitted).
99. *Id.* at 1071–72.
100. *Id.* at 1074.
101. *Id.* at 1073.
102. *Id.* at 1075.
103. *Id.* at 1077.
104. *Id.* at 1075–80.
105. *Id.* at 1077–79.
106. *Id.* at 1079.
107. *Id.* at 1079–80.

Ultimately, Chander calls for a recognition that both corporate actors and governments can threaten speech, and for vigilant attention to the ways in which the DSA could be misused in non-EU jurisdictions.[108]

VII. CONCLUSION

The DSA is an exceptionally complicated law, with far-reaching effects and much for scholars to unpack. But the five papers in this symposium issue—complimentary and critical, underpinned by various methods, and from both EU and US perspectives—make an excellent start. With gratitude for the careful analysis and trenchant observations of the symposium presenters and these five authors, and for the able stewardship of the *BTLJ* symposium editors, I commend this collection to you.

108. *Id.* at 1081–83.

This Page Intentionally Left Blank.

This Page Intentionally Left Blank.