VOLUME 6 July 2025 ISSUE 2

JOURNAL ON EMERGING TECHNOLOGIES

NOTES

HARMONIZING GLOBAL STANDARDS: USING THE EU ARTIFICIAL INTELLIGENCE AND DIGITAL SERVICES ACTS TO ESTABLISH AN AMERICAN FRAMEWORK AT THE FOREFRONT OF DIGITAL GOVERNANCE

AUDRA KIM

Harmonizing Global Standards: Using the EU Artificial Intelligence and Digital Services Acts to Establish an American Framework at the Forefront of Digital Governance

AUDRA KIM

INTRODUCTION

Artificial Intelligence (AI) in the modern Digital Age is as revolutionary as it is feared. It is "a fast evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities."[1] These technologies are expected to fuel sectors "including environment and health, the public sector, finance, mobility, home affairs, and agriculture."[2] Digital (social) media and AI development continue to transform the contours of the 21st century. "Information society services and especially intermediary services have become an important part of the . . . economy and the daily life of . . . citizens."[3] However, the emergence of these technologies is far from a novel concept; both have been around for decades, seeping into mainstream prominence and steadily evolving and changing the way society, businesses, and governments interact. The first concept of AI traces back to the 1950s when British polymath, Alan Mathison Turing, who is now regarded as "the father of AI," posed the question of whether machines could think.[4] John McCarthy, a professor at Dartmouth College, later coined the term "artificial intelligence" and its subsequent acronym where the colloquial use of AI is now both standard and popular vernacular. By the mid-1960s, AI research in the United States (US) gained institutional acknowledgment in the form of funding from the Department of Defense (DOD) and private

---

[1] *EU Artificial Intelligence Act*, OFFICIAL JOURNAL OF THE EUROPEAN UNION (June 13, 2024), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[2] *Artificial Intelligence Act Briefing*, EUROPEAN PARLIAMENT, (Aug. 6, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
[3] *Digital Services Act*, OFFICIAL JOURNAL OF THE EUROPEAN UNION (Oct. 19, 2022), https://www.eu-digital-services-act.com/.
[4] B.J. Copeland, *The History of Artificial Intelligence*, BRITANNICA (June 14, 2024), https://www.britannica.com/science/history-of-artificial-intelligence#ref379822.

laboratories.[5] With the Cold War backdrop, the internet as we know it began to take shape with the development of the DOD's communications systems project, Advanced Research Projects Agency Network (ARPANET).[6] A few decades later, with the dot-com bubble, the internet boomed with widespread public accessibility, ushering in the era of digital platforms that define and influence the global state of the current world. Significant modern milestones started with computers and machine learning algorithms such as IBM's "Deep Blue" chess-playing program and rapidly evolved into Windows' speech recognition software, robot vacuums, digital assistants (e.g., Apple's Siri), driverless cars, and advanced chatbots like ChatGPT. Today, AI dominates the global digital landscape, permeating multifarious aspects of everyday life and fundamentally reshaping how the public, private, and government sectors operate.[7]

Despite the vast and pivotal role of these advancing technologies, the US severely lags in establishing a comprehensive federal regulatory framework to address the unique challenges posed by digital services and AI technologies.[8] Instead, the US "relies on existing federal laws and guidelines" which are often ill-applicable and inconsistent.[9] Outdated statutes like Section 230 of the 1996 Communications Decency Act (CDA) and the 1914 Federal Trade Commission (FTC) Act are relied on to govern accountability and user protections. Forcing AI–with all its nuance and specialization–into traditional, pre-existing legal categories misaligns with its distinct makeup. The under-regulated US landscape is perhaps most clearly exemplified by the idiomatic expression of trying to fit a square peg into a round hole. By contrast, the European Union (EU) has taken bold steps in issuing harmonizing legislation like the EU AI and Digital Services Act (DSA) to protect its citizens. Likewise, "countries worldwide are designing and implementing AI governance legislation commensurate to the velocity and variety of proliferating AI-powered technologies," while in the US, "prospects for broad Congress-passed

---

[5] *The Birth of Artificial Intelligence (AI) Research*, LAWRENCE LIVERMORE NATIONAL LABORATORY, https://st.llnl.gov/news/look-back/birth-artificial-intelligence-ai-research.

[6] Science and Media Museum, *A Short History of the Internet* (Dec. 3, 2020), https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet.

[7] Rockwell Anyoha, *The History of Artificial Intelligence*, HARVARD U., (Aug. 28, 2017), https://huguesrey.wordpress.com/2017/12/28/the-history-of-artificial-intelligence-by-rockwell-anyoha-source-harvard/.

[8] White & Case, *AI Watch: Global Regulatory Tracker - United States* (May 13, 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states#:~:text=Laws%2FRegulations%20directly%20regulating%20AI,AI%20albeit%20with%20limited%20application.

[9] *Id.*

legislation remain doubtful."[10] By issuing this AI Act, the EU is operating intentionally and strategically to advance its goal to "strengthen its digital sovereignty and set standards, rather than follow standards set by others."[11]

As the US leads in technological innovation and economic influence, the nation's laissez-faire approach to digital governance causes global dissonance and a loss in credibility as a historically well-positioned leader and advocate for human rights and affairs. "Amongst the great challenges posed to democracy today is the use of technology, data, and automated systems in ways that threaten the rights of the American public."[12] A passive approach to AI governance by the US causes asymmetry on the international playing field amongst other countries and superpowers. It also subjects the country to outside rule. AI capabilities far outpace traditional US regulatory approaches with the lead only widening. Time is past due for the US to address the regulatory gap and protect not only its citizens but also its businesses in the digital world. This paper proposes that, given the extraterritorial aspect of the EU DSA and AI Act for consumer and business markets worldwide, the US needs to establish its own comprehensive regulating framework to safeguard core American values, US-based businesses, and the economy as a whole. Section II will examine the deficiencies in the current US digital regulatory landscape. Section III will highlight the EU DSA and AI Act's leading approach as a benchmark for comprehensive governance, Section IV will explore AI as a game changer in the global economy, and Section V will discuss the importance of embracing and addressing AI in the US corporate, academic, and legal sectors. Section VI will explore how to uphold human rights by further grounding US digital governance in a global setting, Section VII will consider implementation challenges and discuss recommendations, and Section VIII will serve as a conclusion.

I. THE PROBLEMATIC US DIGITAL LANDSCAPE

The US approach to digital regulation is emblematic of a

[10] European Parliament, *United States Approach to Artificial Intelligence* (Jan. 2024), https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf.
[11] European Parliament, *Shaping the Digital Transformation: EU Strategy Explained*, (Apr. 22, 2021) https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained.
[12] WHITE HOUSE, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022), https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.

fragmented, piecemeal, and reactive system–absent of a comprehensive framework–that ignores the blaring complexities of a digital media, AI-driven world. Legislating digital services in the US, particularly Very Large Online Platforms (VLOPs), is "wrought with either adversarial animosity or sweetheart deals" which is telling of the adverseness surrounding the rush to regulate this powerful sector.[13] Similarly, the federal government has "largely sidestepped the issue of crafting law dictating limitations and expectations regarding the use of AI technology."[14] However, relatively recent AI hearings (at least at the Senate level) have underscored that the US does not want to repeat the social media regulatory failures of Congress by missing the opportunity to regulate AI.[15] Yet, the US remains without a robust framework, or even a pending regulatory framework, akin to the EU AI Act and DSA. Only a proposed bill to enforce (specifically) algorithm accountability has been put forth.

The under-regulated US landscape is perhaps most clearly exemplified by its continued reliance on the CDA, which is legislation enacted back in 1996. The problem is that Section 230 of the CDA does not adequately address modern challenges pertaining to user protection that arise from online platforms, as it was initially designed to shield the online platforms themselves (from liability regarding user-generated content).[16] In other words, this piece of legislation was designed to foster, not regulate, the rapid growth of the digital economy and, further, was created before most VLOPs were even founded with zero existing in their current form.[17] VLOPs have since evolved into mass, influential forces with the ability to engage billions of users across the globe, serving as "so-

---

[13] Davis Morar, *The Digital Service Act's Lesson for US Policymakers: Co-Regulation Mechanisms*, BROOKINGS (Aug. 23, 2022), https://www.brookings.edu/articles/the-digital-services-acts-lesson-for-u-s-policymakers-co-regulatory-mechanisms.

[14] Srinivas Parinandi et al., *Investigating the Politics and Content of US State Artificial Intelligence Legislation*, CAMBRIDGE UNIVERSITY PRESS (Mar. 18, 2024), https://www.cambridge.org/core/journals/business-and-politics/article/investigating-the-politics-and-content-of-us-state-artificial-intelligence legislation/B603D28F79C55446368OB22F3CA8F805.

[15] Daniel Howley, *Senators Say They Failed to Act on Social Media, Won't Make Same Mistake with AI*, YAHOO FIN. (May 17, 2023), https://finance.yahoo.com/news/senators-say-they-failed-to-act-on-social-media-wont-make-same-mistake-with-ai-195217014.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADfqF6wfm-nsf7ITCdVbH7QWVAJF8ddd4Vdvemk6yOnbl94Eob2c-yTdmz3ZqH9n8_OO6emFve4497OYJ_ol6QN2vQLsJ9JlTd6kvAlppecEYxan6v6U53bQPZUtAoxXDXQl4l9M-s_-uAP6tNKtzjfesU4R6I9fpuzXGl9UBTwH.

[16] 47 USC 230 (2021).

[17] *See Id.*

called gatekeepers between businesses and internet users."[18] Over the past two decades, companies including Google, Meta, Apple, and Amazon have risen to become powerhouse institutions, transcending their role as passive intermediaries; they now hold the means to control the flow of information, the dynamic of the economy, and even democratic processes.[19] The broad immunity provision of Section 230 has drawn criticism for enabling these platforms to evade accountability for allowing harmful content, misinformation, privacy violations, and other societal harms linked to their operations.[20] However, efforts to reform Section 230 have stalled due to ideological and polarizing divisions from issues contemplating the government's role in regulating private enterprise to the balancing of free speech with platform responsibility.[21] These divisions are particularly pronounced in debates over content moderation as some stakeholders advocate for stronger measures to combat harmful content and misinformation, emphasizing the need for enhanced platform accountability, while others focus on concerns over potential overreach, such as censorship and the suppression of free expression, particularly in relation to politically sensitive or controversial content. This lack of consensus on the scope and focus of regulation has led to legislative gridlock in the US, stalling comprehensive and needed reform.

Alongside the CDA, an even older piece of legislation serves to inadequately address the modern Digital Age. The FTC Act of 1914 is relied on to regulate deceptive and unfair practices that affect commerce and is stretched to apply to social media.[22] And AI.[23] However, its limited scope and narrow application fails to truly resolve prevalent consumer protection issues, including the lack of platform transparency and accountability, unkempt algorithm biases, and systemic discrimination. Therefore, consumer data is massively collected and misused. Hate speech, disinformation, and extreme propaganda are enabled and proliferated. AI and harmful algorithm biases go unchecked, and a lack of access to remedies continues to exist. Thus, leaving victims few avenues to practical redress. As revolutionary as technologies like digital

---

[18] *See Id.*
[19] *EU Digital Markets Act and Digital Services Act Explained*, European Parliament (Dec. 14, 2021), https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained.
[20] Michael D. Smith & Marshall W. Van Alystne, *It's Time to Update Section 230*, HAR. BUS. REV. (Aug. 12, 2021), https://hbr.org/2021/08/its-time-to-update-section-230.
[21] *Id.*
[22] 15 USC. §§ 41-58 (2021).
[23] *Id.*

media and AI are, they generate a plethora of unprecedented challenges. "Social media has been weaponized to spread disinformation, interfere in elections, and promote and incite violence" and there are "example after example of real harms due to AI, automated technologies, and other forms of algorithm-driven technologies" like facial recognition technologies being "demonstrably biased against minorities, which has led the city of San Francisco to ban their use."[24] These biases not only violate the principles of equality and anti-discrimination but also surface and entrench existing disparities that further marginalize vulnerable populations. Additionally, social media platforms, shielded by the broad immunity of the CDA, have also contributed by serving as breeding grounds for inciteful messaging that disproportionately targets marginalized communities, fueling hate, harassment, discrimination, and, again, violence. Further, driving platform algorithms possess the ability to amplify this already harmful content to the masses, as they are typically programmed to prioritize public engagement over anything and everything. Therefore, divisive, inflammatory content gets pushed and disseminated with less regard for human rights and societal consequences.

In terms of VLOPs, these private entities only exacerbate human rights issues stemming from digital media and AI. These platforms wield unparalleled influence over public discourse, commerce, and privacy, yet they operate under minimal regulatory oversight. As a result, harmful content, exploitative labor practices, and the misuse of user data continue to emerge as persistent challenges. In the absence of comprehensive federal legislation, progressive states such as California have stepped forth to take a stab, enacting measures like the California Consumer Privacy Act (CCPA). [25] And while these state initiatives represent progress, they nonetheless contribute to the issue, creating a patchwork system of inconsistent rules, further complicating compliance for businesses operating across multiple jurisdictions. This not only increases compliance costs across the board but also undermines the broader goal of creating a secure, united, and equitable digital environment. The current digital landscape of the US does not adequately hold VLOPs accountable and exposes the lack of laws to protect consumers and their data. This is best exemplified through the

[24] Molly Gavin, *Human Rights in Age of Social Media, Big Data, and AI*, NATIONAL ACADEMIES (Sep. 23, 2019), https://www.nationalacademies.org/news/2019/09/human-rights-in-age-of-social-media-big-data-and-ai.
[25] *See California Consumer Privacy Act*, State of California – Department of Justice (Mar. 13, 2024) https://oag.ca.gov/privacy/ccpa.

Cambridge Analytica case study. During the 2016 presidential campaign, Cambridge Analytica, a political consulting firm, illicitly harvested and misused the personal data of over 87 million US Facebook users without their consent. [26] This data was weaponized to influence electoral outcomes, using "personal information … for the purposes of voter profiling and targeting."[27] The scandal revealed the extent to which user data could be exploited by private companies for political and economic gain, prompting government investigations into Facebook's privacy practices and sparking a global conversation about the responsibilities of digital platforms. "In 2019, Facebook agreed to pay $5bn to resolve a Federal Trade Commission probe into its privacy practices" and also paid "$100 million to settle US Securities and Exchange Commission claims that it misled investors about the misuse of users' data."[28] According to the lead lawyers for the plaintiff-users in the class action, Facebook (now Meta) deciding to settle the Cambridge Analytica scandal for 725 million dollars was a "historic settlement [that] will provide meaningful relief to the class in this complex and novel privacy case." However, even if each victim made a claim, the payout would only amount to mere dollars per person. The case illuminated the limitations of reactive regulatory approaches, as existing frameworks warrant minimal recovery and fail to prevent such serious violations that attempt to destabilize the democratic process in the first place.

In the overall realm of digital governance, the US federal landscape is outdated and complicated by inconsistencies amongst agencies, states, and extraterritorial applications of international legislation like the EU DSA and AI Act. [29] The consequences of this regulatory inertia and the absence of a comprehensive framework comparable to the EU DSA and AI Act leave US citizens vulnerable and unprotected. US executive efforts in AI governance consist only as a mere blueprint, aptly titled "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People."[30] Issued by the White House Office of Science and Technology Policy (OSTP), these guiding principles are insufficiently short of regulation, but are a step in the right direction in supporting "the development of policies and

---

[26] *See* Shiona McCallum, *Meta Settles Cambridge Analytica Scandal Case for $725m*, BBC (Dec. 23, 2022),https://www.bbc.co.uk/news/technology-64075067.
[27] *Id.*
[28] *Id.*
[29] DSA, *supra* note 3.
[30] *Blueprint for an AI Bill of Rights*, WHITE HOUSE (Oct. 2022), https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.

practices that protect civil rights and promote democratic values."[31] With a non-binding nature, the lack of accountability at scale in digital media and AI remains a problem in the US.

II. THE EU DSA AND AI ACT AS A BENCHMARK

Many of the regulatory structures currently governing the digital space date back to the early days of the internet.[32] In this period, the primary legal concern was fostering innovation and ensuring the nascent digital economy could flourish. Laws such as the EU's E-Commerce Directive of 2000 sought to create a uniform framework for cross-border digital trade while minimizing burdens on service providers.[33] However, the deficiency of existing laws to address the issues arising from the transformation of AI and big actors like VLOPs become increasingly prominent as they grow. The E-Commerce Directive, while foundational in its respective transitory time, offers limited guidance on the responsibilities of giant platforms in moderating harmful content or managing the risks associated with algorithmic decision-making.[34] Thus, the EU issued the DSA and AI Act.[35]

A. The DSA

Focusing on digital media regulation, the DSA is a cornerstone regulation, bold, and the first of its kind. Enacted in 2022, the DSA embodies the EU's commitment to fostering a safer, more transparent, and accountable digital environment. Its objectives extend to include the aim to harmonize the internal market, eliminate regulatory fragmentation, and provide "legal certainty" for businesses and consumers alike.[36] "The internal market should be harmonized, so as to provide businesses with access to new markets and opportunities to exploit the benefits of the internal market while allowing consumers and other recipients of the services to have increased choice." [37] By

---

[31] Tom Krantz & Alexandra Jonker, *What is the AI Bill of Rights?*, IBM (Sep. 27, 2024), https://www.ibm.com/think/topics/ai-bill-of-rights.
[32] Everett Ehrlich, *A Brief History of Internet Regulation*, PROGRESSIVE POLICY INSTITUTE (Mar. 13, 2014), https://www.progressivepolicy.org/a-brief-history-of-internet-regulation-2/.
[33] *Directive No. 2000/31/EC*, WORLD INTELLECTUAL PROPERTY ORGANIZATION (June 8, 2000), https://www.wipo.int/wipolex/en/legislation/details/6393.
[34] *The eCommerce Directive and the UK*, GOV.UK (Jan. 18, 2021), https://www.gov.uk/guidance/the-ecommerce-directive-and-the-uk.
[35] DSA, *supra* note 3.
[36] DSA, *supra* note 3.
[37] *Id.*

establishing obligations for a wide array of digital service providers, from intermediary and hosting services to VLOPs and Very Large Online Search Engines (VLOSEs), the DSA operates to ensure "responsible and diligent behavior by providers of intermediary services" as it is "essential for a safe, predictable and trustworthy online environment."[38]

At its core, the DSA is a "targeted set of uniform, effective and proportionate mandatory rules" established at the Union level to provide "conditions for innovative digital services to emerge and to scale up in the internal market." [39] The DSA introduces a proportionate, tiered structure that assigns obligations based on the size and societal impact of the service provider. This ensures that the largest actors (i.e., VLOPs) with over 45 million monthly active EU users, are held to the strictest standards due to their extensive influence. Intermediary services, such as VPN providers, are required to comply with orders from national authorities to remove illegal content and provide user information while maintaining clear and accessible terms of service. Hosting services, such as website platforms like Squarespace, must implement notice-and-action mechanisms to allow users to flag and report illegal content. This obligation operates to inspire actual accountability as it is inherently on the service to act "expeditiously" to have that content removed upon notice. [40] With regard to online platforms (e.g., Reddit), clear explanations for the removal of content or the suspension of accounts must be provided to users, and an internal complaint system must exist. Additionally, to increase transparency and protect minors, platforms must actively label paid content as advertisements, disclose the identity of the ad originator, and explain targeting criteria. Platforms are also prohibited from engaging in targeted advertising based on profiling minors as well as required to implement safeguards to protect them from harmful and inappropriate content.

For VLOPs and VLOSEs, the DSA imposes the strictest obligations and penalties for non-compliance. These include identifying and mitigating risks related to illegal content, disinformation, algorithm bias, and infringement on fundamental rights, forcing them to look at all the ways their platforms could harm society to prevent them from turning a blind eye. Annual audits conducted by external evaluators are also required. Additionally, VLOPs must disclose the mechanisms behind their algorithms, addressing the spread of misinformation, discrimination, and filter bubbles, to give users greater control over

---

[38] *Id.*
[39] *Id.*
[40] *Id.*

recommendation systems and shed light on dark patterns. Cooperation with outside researchers must also be provided for the purpose of studying systemic risks and improving platform practices.

At a high level, the overall spirit of the DSA is to tackle modern challenges by encouraging collaboration amongst and with platforms to achieve the shared goal of creating a reputable and reliable digital space. The DSA's mandatory risk assessments and transparency requirements promote fairness and diversity while addressing the amplification of existing inequalities. To enforce compliance, the DSA establishes Digital Services Coordinators at the Member State level, empowering the European Commission to directly oversee VLOPs. In terms of violations, hefty penalties exist to underline the EU's will for the DSA to carry weight. Remedy-wise, violators face substantial penalties to the tune of fines of up to six percent of their global annual turnover, doubling down on the EU's commitment to making the DSA effective at all levels.[41] Lastly, the EU recognizes the ever-changing nature of the digital landscape. Thus, the DSA is designed as a living document (flexible and adaptable) that leaves space for interpretation and is capable of evolving alongside technological advancements and emerging challenges.

B. The AI Act

The AI Act, introduced in 2021, is the EU's first dedicated legislative effort to regulate AI technologies.[42] It adopts a risk-based approach, classifying AI systems into categories: unacceptable risk, high-risk, and low-risk, with tailored obligations for each level.[43] AI systems deemed to pose unacceptable risks, such as social scoring or subliminal manipulation, are outright banned. High-risk systems, including those used in critical sectors like healthcare, law enforcement, and employment, are subject to stringent requirements, including mandatory risk assessments, data governance standards, and transparency obligations. Low-risk applications face minimal regulatory oversight but are encouraged to adhere to voluntary codes of conduct.

The Act exemplifies how regulation can proactively address AI's potential harms while fostering innovation. For example, its focus on algorithmic transparency and bias mitigation directly confronts issues like discriminatory practices in hiring algorithms and surveillance

---

[41] *Id.*
[42] *EU AI Act: First Regulation on Artificial Intelligence*, EUROPEAN PARLIAMENT (Feb. 19, 2023, 5:46 PM), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence, (hereinafter "*EU AI Act*").
[43] *Id.*

technologies. The US, where AI governance remains underdeveloped and largely reactive, could draw valuable lessons from the AI Act's structured and planned approach. Implementing similar measures would help mitigate algorithmic bias, enhance accountability, and align AI deployment with human rights principles.

In synchrony with the DSA, the AI Act emerges in the broader context of the EU's commitment to digital governance and ethical AI deployment. As AI technologies continue to evolve rapidly, concerns surrounding their misuse, unintended consequences, and societal impact have grown. The EU has long positioned itself as a global leader in tech regulation, most notably with the General Data Protection Regulation (GDPR), which sets a high standard for data privacy.[44] The AI Act follows a similar trajectory, aiming to balance innovation with fundamental rights, ensuring that AI technologies remain ethical, trustworthy, and human-centric. A key objective of the Act is to establish clear legal certainty for businesses and developers while protecting citizens from potential AI-related harms.[45] The regulation also seeks to enhance Europe's competitive edge in AI by creating a unified framework that fosters responsible innovation rather than stifling technological progress. By implementing strict guidelines for high-risk AI applications while allowing low-risk AI systems more flexibility, the Act reflects a nuanced understanding of AI's varied applications.

Breaking down the levels of risk categories, AI systems falling under the unacceptable risk category are outright banned due to their potential to harm fundamental rights, safety, or democracy. Examples include AI-driven social scoring (akin to China's social credit system), real-time biometric surveillance in public spaces (except in strictly defined security scenarios), and AI that manipulates human behavior subliminally.[46] High-risk AI systems operate in critical sectors where failures or biases could have severe consequences. Examples include AI used in medical diagnostics, autonomous vehicles, employment decisions, and credit scoring. High-risk AI must comply with stringent regulations, including robust data governance, detailed risk assessments, human oversight mechanisms, and transparency measures to mitigate biases and discriminatory outcomes. AI applications that pose lower risks are subject to lighter regulations but must adhere to transparency

---

[44] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[45] *EU AI Act*, *supra* note 42.
[46] *Id.*

obligations. This category includes AI-driven chatbots, automated customer service systems, and recommendation algorithms, which must inform users when interacting with an AI system rather than a human. Meanwhile, AI applications deemed to have negligible risks, such as AI-powered spam filters or video game algorithms, face no regulatory restrictions. While voluntary adherence to ethical guidelines is encouraged, compliance with the AI Act is not mandatory for these systems.

One of the AI Act's most significant contributions to AI governance is its emphasis on transparency and accountability. High-risk AI systems must provide clear explanations of how decisions are made, particularly in areas like hiring, credit scoring, and judicial decision-making, where algorithmic bias has historically led to unfair or discriminatory outcomes. Organizations deploying high-risk AI must conduct bias audits and ensure that their AI models are trained on diverse and representative datasets to prevent systemic discrimination. Another crucial aspect of the AI Act is its provisions on human oversight. High-risk AI cannot operate autonomously in critical decision-making processes without meaningful human intervention. This safeguard is designed to prevent overreliance on AI in sensitive domains, such as law enforcement and healthcare, where human judgment remains essential.[47] As the AI Act presents both challenges and opportunities for businesses operating in the space, compliance with high-risk AI regulations requires substantial investments in risk assessment, data management, and algorithmic transparency. Companies developing AI systems for regulated sectors may face higher operational costs but will benefit from increased consumer trust and market legitimacy. For startups and SMEs, the Act introduces regulatory "sandboxes," which are controlled environments where companies can test innovative AI solutions under regulatory supervision.[48] These sandboxes aim to foster innovation while ensuring compliance with ethical and legal standards. By providing a structured pathway for AI development, the Act strikes a balance between regulatory rigor and technological advancement.

The AI Act also has an extraterritorial component and is poised to influence AI regulation far beyond EU borders. Much like the GDPR, which prompted other countries to adopt similar data protection laws, the AI Act can set a precedent for AI governance worldwide. Countries such as Canada and Japan are already considering AI regulations that

---

[47] *Id.*
[48] *Id.*

align with the EU's risk-based approach.[49] In contrast, the US has yet to introduce a comprehensive AI regulatory framework. Again, while there have been executive orders and sector-specific AI guidelines, such as ones in healthcare and defense, US AI governance is missing in action. The EU AI Act presents as a model for US development, paving a structured path forward that emphasizes accountability, bias mitigation, and transparency. China, on a third hand, has adopted a more centralized and government-controlled approach to AI regulation, focusing on state oversight and national security concerns. [50] The EU's emphasis on fundamental rights and ethical AI stands in contrast to China's strategy, reinforcing the EU's role as a leader in human-centric AI governance.[51] The US and other global players should glean from the EU AI Act's base framework to ensure that AI technology serves humanity without compromising fundamental rights and freedoms.

C. A Benchmark for the US

The US stands to benefit significantly from adopting similar principles to the EU's DSA and AI Act. While still taking into account the nation's own unique legal, cultural, and political context, there are several key aspects of EU legislation that the US should take away. First is the EU's emphasis on the importance of proportionality. Both acts tailor obligations based on the size and influence of entities, ensuring that regulatory burdens are commensurate with potential societal impact. This nuanced approach avoids stifling smaller enterprises like startups, and mitigating innovation-hindering concerns while holding larger actors accountable. For the US, implementing a similarly tiered regulatory framework would address scrutiny regarding overregulation (the negative impact on innovation) and foster compliance across the digital landscape. Additionally, the EU's emphasis on transparency mandates that require disclosures about algorithms, content moderation practices, and advertising systems, offers a roadmap for addressing algorithmic opacity, a persisting challenge in the US. These measures empower regulators and the public to scrutinize platform behavior,

---

[49] Maoko Kamiya & James Keate, *AI Watch: Global Regulatory Tracker - Japan*, WHITE & CASE (July 1, 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-japan; *AI Watch: Global Regulatory Tracker – Canada*, WHITE & CASE (Dec. 16, 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-canada.
[50] Matt Sheehan, *China's Views on AI Safety Are Changing – Quickly*, CARNEGIE ENDOWMENT (Aug. 27, 2024), https://carnegieendowment.org/research/2024/08/china-artificial-intelligence-ai-safety-regulation?lang=en&center=india.
[51] *Id.*

fostering trust and accountability. Furthermore, the DSA's focus on user-centric protections, such as accessible grievance mechanisms and robust tools for reporting illegal content, highlights the importance of prioritizing consumer rights and providing effective remedies for online harms.

III. AI AS AN UNYIELDING FORCE IN THE GLOBAL ECONOMY

In the modern corporate landscape, AI is integral to the strategic and operational frameworks of businesses across the globe as its core nature is to streamline, automate, and relieve human capital of lower-impact tasks. AI is efficient and cost-effective. It is a steadfast force in the corporate world because it increases bottom lines, making the employment of AI systems perennial. Milton Friedman's Theory of Social Responsibility posits that "there is one and only one social responsibility of business–to use its resources and engage in activities designed to increase its profits," meaning a company's social responsibility does not extend to the public or society, only its shareholders.[52] His argument supports the view of AI longevity in business as AI is projected to significantly continue to reduce operational costs and grow revenue.[53] However, Friedman's theory is increasingly contested by the implications of AI on users and society as a whole. Because AI is an inherent disruptor, the ethical complexities introduced expand the scope of corporate responsibilities. Corporations cannot easily turn a blind eye to the concerns that arise from AI because AI influence extends across the main facets of society. Individual rights, social norms, and equitable treatment are impacted. Adhering strictly to Friedman's profit-centric approach encourages companies to overlook these issues while not considering how their practices may significantly harm society. Is it time to expand the corporate mandate to include the interests of stakeholders, not just shareholders?

In business, "artificial intelligence is used as a tool to support a human workforce in optimizing workflows and making business operations more efficient" by "using AI to automate repetitive tasks, generate information based on machine learning algorithms, quickly

---

[52] Milton Friedman, *A Friedman Doctrine – The Social Responsibility of Business Is to Increase Its Profits*, N.Y. TIMES (Sep. 13, 1970), https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html (quoting Milton Friedman, *Capitalism and Freedom*).

[53] Thomas Lah, *Cutting Costs and Increasing Revenue: The Role of AI in Today's Tech Industry*, TECH. & SERVS. INDUS. ASS'N (Nov. 13, 2024), https://www.tsia.com/blog/cutting-costs-and-increasing-revenue-the-role-of-ai-in-todays-tech-industry.

process vast amounts of data sets and extract meaningful insights, and predict future outcomes based on data analysis."[54] Corporations – from small and medium enterprises (SMEs) to large and very large businesses – harness the powers of AI to enhance their strategic capabilities, optimize operations, and personalize customer interactions on an unprecedented scale.[55] Firstly, AI enables corporations to process and analyze nearly unmanageable amounts of data swiftly, allowing for timely, strategic decision-making that fluently aligns with global trends and consumer behaviors. This capability is advantageous for maintaining a competitive edge in rapidly evolving markets. For example, in sales, AI is able to comprehend consumer behavior patterns to better target campaigns. In sectors like finance, AI algorithms can be used for real-time stock trading, fraud detection, and risk assessment. Moreover, AI systems are integral to optimizing complex supply chains which ensures efficient and resilient output that is freer of human error and limitations. AI also relieves human workforces of manual, administrative, and repetitive tasks (e.g., data entry, production lines, etc.) so that higher-level work can be focused on.[56] Finally, AI allows these corporations to achieve personalization at scale by offering tailored marketing, dynamic pricing, ease, and product recommendations to consumers worldwide (via chatbots, virtual assistants, facial identification, personalization algorithms, etc.).[57] For example, Amazon uses AI to track customer spending behaviors in anticipation of what they will want and buy.[58] This, in turn, increases customer satisfaction, loyalty, and recognition by facilitating ease. "Businesses are also moving beyond these use cases and using AI to assist in higher-level, strategic initiatives that help drive broader business value."[59]

Through the lens of Friedman's Theory of Social Responsibility, AI will continue to be maximized in application by businesses as it provides informed, current data analysis and decision-making, achieves operational efficiency through automation, and effortlessly enhances customer experience. Most importantly, it is profitable. With that being said, Friedman's theory is also challenged by AI and the push for its

---

[54] Camilo Quiroz-Vazquez & Michael Goodwin, *What is Artificial Intelligence (AI) in Business*, IBM (Feb. 20, 2024), https://www.ibm.com/think/topics/artificial-intelligence-business#:~:text=Artificial%20intelligence%20in%20business%20is,productivity%2C%20and%20drive%20business%20value.
[55] *Id.*
[56] *Id.*
[57] Ramesh Rajagopalan, *10 Examples of Artificial Intelligence in Business*, UNIV. OF SAN DIEGO, https://onlinedegrees.sandiego.edu/artificial-intelligence-business/.
[58] *Id.*
[59] Quiroz-Vazquez, *supra* note 54.

regulation. AI-driven decisions in areas such as hiring, customer service, and recommendations can have profound implications on privacy, bias, and fairness. The deployment of AI in sensitive sectors such as healthcare and law enforcement raises additional concerns surrounding accuracy, accountability, and transparency. AI's ethical implications, codified by the EU's AI Act, hold businesses socially responsible for what they induce onto society at large when they, themselves profit from AI deployment.

IV. EMBRACING AI IN US SECTORS

In the 21st century's era of digitalization, an overall change in general mentality is sorely needed in the US to facilitate the adoption of AI regulation. For contrasting purposes, the UK communicates that "unleashing the power of AI is a top priority in the plan to be the most pro-tech Government ever."[60] In the academic, corporate, and legal sectors, it is undeniably acknowledged that AI presents both significant opportunities and perceived challenges. While the integration – and acceptance – of AI can drastically enhance efficiency, innovation, and competitive advantage (as discussed in Section III), there are barriers to entry that hold nations back from evolving with the times. However, the shortcomings must be addressed as expeditiously as they rise. In the words of Charles Darwin, "It is not the most intellectual of the species that survives; it is not the strongest that survives; but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself."[61] Boiled down, most barriers to AI are self-imposed, stemming from fear of use, lack of technical expertise, and an unwillingness to possess the proactive mentality needed to overcome the "if it ain't broke…" idiom that is ill-applied.

In academia, there is a palpable tension surrounding the use of AI technologies like ChatGPT and even grammar-enhancing tools like Grammarly. Restrictive classroom leaders and academic codes of conduct often prohibit, project, and instill fear of using these technologies, categorizing them as forms of (or near forms of) cheating. This perspective, however, fails to recognize AI as a critical tool in research and learning, similar to the way calculators, dictionaries, and

---

[60] *Artificial Intelligence and Intellectual Property: copyright and patents*, GOV.UK (June 28, 2022), https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/artificial-intelligence-and-intellectual-property-copyright-and-patents.

[61] Nikol Chen, *The One Most Adaptable to Change is the One that Survives*, LAIDLAW SCHOLARS NETWORK (Apr. 19, 2021), https://laidlawscholars.network/posts/the-one-most-adaptable-to-change-is-the-one-that-survives.

the internet are used today. Historically, each new tool — from print books to digital resources — was initially met with skepticism but eventually became an essential step in a diligent work process and overall output. Enforcing a non-use policy when it comes to AI does a disservice to students and educators alike, hindering their ability to engage with contemporary methods of information collection, processing, and creation. It is acknowledged that there is a negative connotation fastened to taking credit for an AI's autonomous work. Plagiarism is the dirty word thrown around. However, there are two points to be made here. First is food for thought in that UK copyright law currently offers protection to autonomous computer-generated works that are completely without a human author.[62] The AI designer is credited for the output produced by their AI, rendering human touch unneeded. Second, the large portion of concerns over unoriginality and AI error are premature and misguided as they undermine the premise that human counterparts should remain relevant and necessary. Teaching the proper use and incorporation of AI avoids concerns over plagiarism and may be a more productive path forward… as adoption is inevitable. With cream always rising to the top, the more skilled AI users will produce better-generated responses and therefore, more desirable work product. These inhibitive concerns should not result in encouraged avoidance, rather, the solution lies in teaching toward strategies for better use and results. The reluctance to adopt AI does not just hold back innovation, it disadvantageously fails to prepare generations for a "full-integration" world where the use of AI is expected and accepted.

In fact, it is not the younger generation that AI warnings should be imposed upon as they are typically more adept at using technology responsibly and properly, utilizing AI tools to enhance and verify their original work rather than replace it.[63] In contrast to Generation Z (Gen Z) and Alpha, a lack of understanding of how to effectively use AI is often more pronounced amongst older generations, as evidenced in sectors beyond academia. This gap in understanding can be illustrated by the 2023 incident involving a lawyer, Steven Schwartz, and his misuse of ChatGPT.[64] Schwartz's legal brief cited fictitious cases generated by ChatGPT, highlighting the crucial role of due diligence that AI users still

---

[62] *Artificial Intelligence and Intellectual Property: copyright and patents*, *supra* note 60.

[63] Dimani Jayatissa, *Generation Z – A New Lifeline: A Systematic Literature Review*, 3 SRI LANKA J. SOC. SCI. & HUMANS. 179 (2023).

[64] Matt Novak, *Lawyer Uses ChatGPT in Federal Court and It Goes Horribly Wrong*, FORBES (May 27, 2023), https://www.forbes.com/sites/mattnovak/2023/05/27/lawyer-uses-chatgpt-in-federal-court-and-it-goes-horribly-wrong/.

need to carry out. Schwartz admitted he had "never used ChatGPT before and had no idea it would just invent cases."[65] Such examples underscore the need for the legal sector not only to accept but actively engage with AI to avoid these mishaps. Rather than resisting, legal professionals should be at the forefront, tackling new technological concerns head on-especially as societal leaders. As the influential corporate sector, driven by the economic principles outlined in Friedman's theory of social responsibility, is more inclined to incorporate AI to maximize shareholder value, the law must stay a few proactive steps ahead. By adopting AI tools and learning their proper application, the legal sector is better able to develop regulations that govern these technologies as it will be from an informed and educated position.

The US must therefore move to lead the shaping of AI regulation. If not, the US risks falling behind other nations that, like the EU, are setting ambitious and extraterritorial precedents in digital governance. The country's passive actions of "accommodation" may be perceived as less than competent.[66] For the US to reinforce its leadership position and influence amongst other world superpowers, embracing AI across all sectors with informed enthusiasm and strategic foresight is in the nation's best interest.

V. THE UNGPS AS ANOTHER FRAMEWORK

The United Nations Guiding Principles on Business and Human Rights (UNGPs) may offer a promising model to help bridge gaps and modernize US digital governance. Grounded in principles of protecting human rights, respecting societal values, and providing remedies for harm, the UNGPs can guide the US toward establishing a coherent and ethically grounded approach to regulation.[67] Adopting a UNGP-forward framework would not only harmonize US digital regulation with global standards but also ensure alignment with fundamental human rights principles – principles that should ideally be present in legislation across the board.

"It has long been recognized that business can have a profound

---

[65] *Id.*

[66] Wang Liao et al., *Expertise Judgment and Communication Accommodation in Computer-Mediated and Face-to-Face Groups*, 45 COMM. RES. 1122 (2018), https://journals.sagepub.com/doi/10.1177/0093650215626974.

[67] U.N. Off. of the High Comm'r for Hum. Rts., *Guiding Principles on Business and Human Rights*, U.N. Doc. HR/PUB/11/04 (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

impact on human rights."[68] The UNGPs may be leveraged to modernize US digital regulation by examining the current deficiencies in US digital policy, the transformative potential of the DSA and AI Act, and the realistic applicability of the UNGPs. In doing so, a roadmap for establishing a balanced, stable, and versatile digital governance framework will be outlined in this section. By leveraging global best practices, the US can harmonize its digital governance with international standards, ensuring a safer and more equitable digital ecosystem.

The UNGPs "provide a blueprint for action" and should serve as essential scaffolding for addressing the regulatory deficits within the US digital governance framework.[69] Especially with international business and human rights experts like Dr. Michael Addo–former member of the United Nations (UN) Working Group on Business and Human Rights–zealously championing these principles.[70] UNGPs can also guide the US in adopting a comprehensive regulatory system akin to the EU DSA and AI Act. Focusing on the DSA, by drawing from these UN guiding principles and traces of their fingerprints in EU legislation, the US can also establish a coherent approach to safeguarding human rights in the digital age while still fostering innovation and accountability.

A. The State Duty to Protect Human Rights

The first pillar of the UNGPs addresses the State's duty to protect individuals from human rights abuses committed by companies. This duty requires that the State must take appropriate steps to "prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."[71] It is also stipulated that states should set clear expectations that companies domiciled in their territory or jurisdiction should respect human rights throughout their operations in every country and context in which they operate.[72] Additionally, under this pillar, some companies (particularly larger multinational ones) will be required to report on their social and environmental performance worldwide. Requiring such communicative, public reporting will drive transparency and enable official and public

---

[68] U.N. Off. of the High Comm'r for Hum. Rts., *Frequently Asked Questions About the Guiding Principles on Business and Human Rights*, U.N. Doc. HR/PUB/14/3 (2014), https://www.ohchr.org/sites/default/files/Documents/Publications/FAQ_PrinciplesBussinessHR.pdf (hereinafter referred to as FAQs).
[69] *Id.*
[70] Michael K. Addo, *The Reality of the United Nations Guiding Principles on Business and Human Rights*, 14 HUM. RTS. L. REV. 133 (2014).
[71] *Id.*
[72] *Id.*

scrutiny which ensures accountability that companies are respecting human rights.

The DSA serves as a direct reflection of how a regulatory framework can embody the core principles of the UNGPs first pillar; the DSA's emphasis on risk assessment, transparency, and accountability aligns closely with the expectations set out under the UNGPs. Specifically, the DSA mandates that VLOPs proactively identify and mitigate systemic risks, addressing potential human rights abuses that they are most privy to resolve. These requirements run parallel to the UNGPs' call for States to establish clear legislative and regulatory expectations for companies. Unlike the EU, the US lacks a comparable framework capable of institutionalizing the same protective measures for its citizens. Adopting a UNGP-inspired framework (like the DSA) would operationalize the State duty to protect and meet global standards, creating a tried-and-true structure for holding and encouraging companies to be accountable for their impacts on society. Incorporating such obligations into US digital regulation would also address inequitable risks surrounding disinformation, hate speech, and algorithmic discrimination that disproportionately impact vulnerable populations. "The recognition of the equal and inherent worth of human persons is, today, the only widely shared suprapositive [sic] value with which positive law and legal systems worldwide are reasonably judged and critiqued"–a principle that warrants real action by the US.[73] By mandating transparency by requiring platforms to disclose their algorithms and content moderation practices, the US can benefit from thought-out and established methods for safeguarding privacy and freedom of expression rights. As a bonus, these provisions already mirror the UNGPs' logic that transparency drives accountability to further meet the duty to honor human rights.

B. The Corporate Responsibility to Respect Human Rights and Access to Remedy

The second pillar of the UNGPs establishes that business enterprises should respect human rights, meaning that they should "avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[74] This responsibility requires companies to embed human rights considerations

---

[73] Paolo G. Carozza, *Human Rights, Human Dignity, and Human Experience, in Understanding Human Dignity* 615 (Christopher McCrudden ed., Oxford Univ. Press 2013).
[74] *Id.*

into their policies, due diligence processes, and operational practices to not only mitigate but prevent their cause or contribution to adverse impact, including if they are directly linked through their business relationships.[75] Moreover, the corporate responsibility to respect human rights calls for businesses to provide real mechanisms for individuals to raise concerns and seek redress. This also plays into the third pillar: ensuring that States will provide victims with "access to an effective remedy when their rights have been violated."[76]

The DSA provides a compelling model by requiring platforms to implement notice-and-action mechanisms that allow users to flag and report illegal or harmful content, a clear pathway that embodies the corporate responsibility to address adverse impacts. These mechanisms ensure swift action by platforms to not only take down flagged content but also provide clear explanations for their decisions. This proactive approach also aligns with the UNGPs by fostering accountability and mitigating harm. Additionally, the transparency obligations under the DSA, such as requiring companies to outline their content moderation practices and algorithmic processes help to keep platforms from promoting harmful content, discrimination, and disinformation by addressing the risks tied to their operations.

The third pillar of the UNGPs, access to remedy, is another area where the DSA can serve a future US regulatory framework by already aligning with the UNGPs. Under the DSA, elaborate user grievance mechanisms–internal complaint systems–are established. Regarding content removal processes, platforms are required to provide clear explanations and accessible mechanisms for users to contest the decisions in the event a user's content is removed or their account is suspended. This aids in empowering individual users in the face of VLOP decisions which creates a process that is transparent, fair, and supportive of consumer rights and accessible remedies. To conclude this section, the DSA "mirrors core elements of the UNGPs when it comes to assessing risks, providing transparency about platform governance, and engaging with stakeholders around corporate practices."[77] That is why future US digital governance should look towards both in developing a viable framework.

---

[75] UNGPs, *supra* note 67.
[76] FAQs, *supra* note 68, at 34.
[77] Isabel Ebert et al., *The Business & Human Rights Dimension of the Digital Services Act*, UNIV. OF ST. GALLEN, SWITZ. (Aug. 31, 2023), https://freiheitsrechte.org/uploads/publications/Digital/Grundrechte-im-Digitalen/The-Business-Human-Rights-Dimension-of-the-Digital-Services-Act.pdf.

VI. CHALLENGES, REALITIES, AND A PATH FORWARD

A UN Special Rapporteur, on the promotion and protection of the right to freedom of opinion and expression, remarked that "human rights–its vocabulary, its framework, its vision–provides a basis for restraining the worst intrusions and violations of the digital world, and promoting its best." [78] This statement embodies the necessity of embedding human rights principles into the governance of the digital world. For the US, implementing a comprehensive regulatory framework that mirrors the EU DSA and AI Act while aligning with the UNGPs presents a dual challenge of navigating deeply seeded legal, cultural, and political barriers while not missing the opportunity to harmonize with (and set global standards for) the shapeable forefront of digital governance as a world leader.

A. Challenges

The biggest challenge in implementing a US digital regulatory framework lies in the historically fragmented nature of the system. As mentioned in Section II, the US operates through a patchwork of federal and state laws and struggles to balance government power, which results in inconsistencies. Constitutional constraints rooted in the First Amendment present significant barriers to updated legislation. The US's strong commitment to free speech also complicates efforts to regulate content moderation without raising concerns of government overreach or censorship. [79] Historically, courts have upheld expansive interpretations of free expression, making it difficult to impose restrictions on how platforms manage or amplify UGC. [80] This foundational principle, while vital to American democracy, has greatly contributed to the core barriers in the actual implementation of a modernized US digital governance framework.

Furthermore, the litigious nature of the US legal system adds another layer of hurdles. New regulations are often subjected to lengthy court challenges, delaying their implementation and potentially undermining their effectiveness. The political influence of technology giants such as Meta, Google, and X (formerly Twitter) exacerbates the

---

[78] Gavin, *supra* note 24.
[79] William Echikson, *Europe Struggles to Enforce New Free Speech Rules*, CTR. FOR EUROPEAN POL'Y ANALYSIS (Aug. 28, 2024), https://cepa.org/article/europe-struggles-to-enforce-new-free-speech-rules/.
[80] *Id.*

problem as the US is hesitant to constrict these economic players.[81] Many of these VLOPs wield substantial lobbying power anyway. They often resist regulatory reforms that could impose stricter oversight and more work on their operations, so they are keen on preserving the status quo.[82] The absence of a unified federal framework allows these companies to exploit the gaps and loopholes created by patchy legislation, prioritizing corporate interests over the public and human rights in general.

Despite these challenges, the EU DSA and AI Act can be interpreted as a call to action for the US to shake from its state of inertia and assume its place as a leading global superpower. As the home to many transformative VLOPs, the US should not be ceding regulatory standard-setting to other nations, especially when obligations are extraterritorial. It is in the US's best interest as a nation to step into first-mover advantage and *not* take a back seat when it comes to leading in governance because, one, it is an opportunity to promote core American values, and two, the DSA disproportionately targets American companies.[83] The US's updated federal framework for digital regulation should take the best of existing EU legislation–as it already incorporates the UNGPs–and embed distinct American ideology and values, such as free speech protections and innovation incentives, while addressing emerging challenges like algorithmic bias and data misuse. Such a framework would not only protect global users, but also American businesses and, thus, the US economy.

By assuming leadership, the US can offer a global model that demonstrates acknowledgment of the challenges that arise with VLOPs, constructing and initiating checks upon itself instead of having other nations reach into the country to apply their own checks. Put differently, the US has the power to prevent external international legislation from establishing influence by setting its own standards. With that, the US should also leverage its position as a technological and economic superpower to broker cooperation, consistency, and interoperability. Internally, the US should establish its own centralized digital governance authority to oversee platform accountability, transparency, and algorithm audits; a group that is separate and preferable from the EU

---

[81] William Alan Reinsche & Kati Suominen, *Are US Digital Platforms Facing a Growing Wave of Ex Ante Competition Regulation?*, CTR. FOR STRATEGIC AND INTERNATIONAL STUD. (June 21, 2023), https://www.csis.org/analysis/are-us-digital-platforms-facing-growing-wave-ex-ante-competition-regulation.
[82] *The Lobby Network: Big Tech's Web of Influence in the EU*, CORP. EUROPE OBSERVATORY (Aug. 31, 2021), https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu.
[83] Reinsche, *supra* note 81.

DSCs. Overall, the framework should be grounded in the country's constitutional principles of freedom, equality, and democratic accountability. For the US, the EU DSA and AI Act serve as pieces of guidance and a wake-up call, signaling that it is past time to change its approach from under-regulation to proper regulation.

B. Comparing EU and US Realities

Similar to the way cultural differences in communication styles are not apples to apples, the respective realities of an EU vs US landscape should be considered when implementing a new framework.[84] A framework similar to the EU DSA and AI Act in the US would be distinctly challenging due to significant legal, political, economic, and cultural differences between the two jurisdictions. The EU has developed these regulations to ensure greater oversight of artificial intelligence and digital platforms, prioritizing consumer protection, transparency, and accountability. However, the US faces unique constitutional and structural constraints that would complicate the adoption of similar policies.

One of the most significant obstacles concerns the US's legal structure and constitutional framework, particularly regarding the First Amendment. There exist vast differences in data privacy and consumer protection laws between the US and the EU. The broad protections for free speech make it difficult to implement stringent content moderation rules, which are central to the EU's DSA. The EU has already established a robust data protection framework through the GDPR, which aligns with the DSA. In contrast, the US lacks a comprehensive federal data privacy law, instead relying on a patchwork of state-level regulations, such as the California Consumer Privacy Act.[85] Unlike the EU approach, which includes principles such as the right to be forgotten (i.e., deletion of online history and personal data to protect privacy), the US legal system tends to favor minimal restrictions on expression instead. Without a uniform national privacy framework, implementing broad digital regulations similar to the EU's would require resolving these foundational gaps first, a process that could take years. Moreover, American businesses and consumers have different expectations regarding data usage, with many US firms relying heavily on data-driven

---

[84] *See generally* Y. Connie Yuan et al., *Judging Expertise Through Communication Styles in Intercultural Collaboration*, 33(2) *Mgmt. Comm. Q.* 238 (2019).
[85] *California Consumer Privacy Act (CCPA)*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/privacy/ccpa (last visited April 4, 2025).

business models that would be disrupted by EU-style restrictions.

Additionally, regulatory authority in the US is fragmented among multiple agencies, including the FTC, FCC, and Department of Justice.[86] Unlike the EU, which has more centralized digital governance through the European Commission, coordinating oversight across different US agencies would create significant bureaucratic challenges and regulatory inconsistencies.[87] Political resistance and corporate lobbying further complicate the likelihood of implementing an EU-style framework in the US. Historically, Congress has been resistant to comprehensive federal regulation of technology companies, with political polarization often preventing bipartisan consensus on digital governance issues. Additionally, major technology firms (e.g., Google, Meta, Amazon, Tesla) have substantial influence in Washington and are likely to oppose regulations they perceive as overly burdensome.[88] While the EU has a more unified approach to passing legislation through the European Commission and Parliament, the US legislative process is often slowed by partisan gridlock, making it unlikely that a comprehensive AI and digital services framework would pass without significant dilution.

Economic and market considerations could also pose a challenge. The American technology sector is a key driver of the national economy. Imposing strict regulations on AI and digital platforms could potentially hinder innovation and global competitiveness. Unlike the EU, where many large digital platforms are foreign-owned, stricter US regulations would primarily impact domestic firms, leading to significant industry resistance. The AI industry in its relative infancy is still developing, and regulation at this stage could deter investment at some scale. Historically, the US has favored a passive approach to technology regulation in order to prioritize market-driven solutions over prescriptive legal frameworks. Cultural and societal differences also distinguish the US from the EU. The EU tends to adopt a precautionary approach to emerging technologies, regulating potential harms before they materialize. In contrast, the US emphasizes innovation and economic growth, favoring reactive rather than preemptive regulation. Additionally, American attitudes toward government intervention in

---

[86] Hongkang Xu, *Regulatory Fragmentation and Internal Control Weaknesses*, 44 J. OF ACCT. & PUB. POL'Y 1, 4 (2024), https://www.sciencedirect.com/science/article/abs/pii/S0278425424000140.

[87] *Id.*

[88] Cecilia Kang & Kenneth P. Vogel, *Tech Giants Amass a Lobbying Army for an Epic Washington Battle*, N.Y. TIMES (June 5, 2019), https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html.

business affairs are generally less favored, with many citizens and lawmakers viewing excessive regulation as a threat to entrepreneurship and economic liberty.[89] This skepticism makes broad AI and digital regulations politically unpopular and difficult to pass without substantial industry and public support. Even if the US were to adopt an AI and digital services framework similar to the EU's, enforcement and compliance could pose substantial difficulties. The EU has established centralized regulatory bodies to oversee compliance across member states, but the US, with its federal system, would need to coordinate enforcement among multiple state and federal agencies. Compliance costs could also disproportionately impact smaller companies and startups, discouraging competition and reinforcing the dominance of existing tech giants. Many small businesses rely on AI-driven tools and digital platforms to remain competitive, and increased regulatory burdens could reduce their ability to innovate and grow.

However, the purpose of outlining these challenges is to highlight what needs to be considered and overcome, not reasons to ride the status quo and make no legal change. Rather than replicating the EU's approach, the US will need to develop a more tailored regulatory framework that balances innovation with responsible governance to account for the country's unique legal and economic landscape.

C. Recommendations

The US stands at a crossroads. While the EU has taken decisive steps in shaping the global regulatory landscape, the US has dithered. If this complacent inertia continues, the US cedes normative influence to imported foreign regulatory regimes and loses the window to align international digital media and AI standards with American values. What is required now is a deliberate and strategic game plan.

Looking through the lens of a "resilience agenda," the focus should be "primarily on government, corporate, and other institutions to preserve, reinvent, and protect societal goals, interests, and values from disruption."[90] The first step is the mentality shift discussed in Section V: embracing AI as a reality across sectors. Forward-thinking is crucial at

---

[89] Anu Bradford, *The False Choice Between Digital Regulation and Innovation*, NW. U. L. REV. (Oct. 2024), https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?params=/context/faculty_scholarship/article/5567/&path_info=Bradford_The_False_Choice_Between_Digital_Regulation_and_Innovation.pdf.

[90] Danielle Keats Citron & Kristen Eichensehr, *Resilience for a Digital Age*, 2024 U. CHI. LEGAL F. 45, 55 (2025).

every level–from the political branches to classrooms, boardrooms, and courtrooms. AI must be acknowledged and respected as, fundamentally, a new category. It is not simply another technological advancement, but its own beast. It cannot be effectively governed by retrofitting laws that were never intended to anticipate machines capable of autonomous decision-making and continuous self-learning. Going back to the square peg and round hole, AI demands its own regulatory architecture, one with the capacity to evolve alongside the technology it oversees. The most streamlined approach to accomplishing this is by establishing a "Department of Technology" with a dedicated AI branch (and digital media branch) that serves as a task force focused exclusively on governance. This is long overdue and would provide clarity amongst agencies such as the FTC and FCC which handle overlapping digital policy issues. [91] As acknowledged by Justice Elena Kagan, "[t]he questions of whether, when, and how to regulate online entities… are understandably on the front-burner of many legislatures and agencies."[92] These questions need only be at the front-burner of one united, consolidated body. Such a body would not only hold regulatory expertise and authority but also signal institutional recognition of digital media and AI's systemic importance. It could serve as the national locus for developing technical standards, monitoring risk, coordinating enforcement, and facilitating public engagement.

The next step is enacting legislation and international standardization. Rather than reinventing the wheel, the US should look outward. The DSA, the AI Act, and the UNGPs offer robust foundations upon which an American framework can be built. These instruments reflect a broad international consensus on core governance principles that are already accepted amongst other countries. The US can tailor these models to consider its own constitutional commitments, economic biases, and structure. This includes adapting risk assessment procedures to preserve First Amendment protections and embedding due process safeguards for content moderation and automated decisions, all while promoting growth and business.

Once an initial governance framework is set, the next play should be alignment with the private sector. If the US fails to set standards, American companies (many of which dominate the digital realm at a global scale) will continue to fall under the jurisdiction of foreign regimes. Early coordination with the US business community can foster a sense of ownership, reduce compliance burdens, and build support on

---

[91] Xu, *supra* note 86.
[92] *Moody v. NetChoice, LLC*, 603 US 707, 716 (2024).

all fronts. This coordination should not be viewed as deference to industry but as a collaborative effort to ensure that the US—not other countries—sets the global standards to which American companies are held. A common cause the entire nation can (and should) rally behind. Such efforts can be facilitated through multi-stakeholder task forces composed of government officials, industry leaders, technical experts, and civil society advocates. These bodies could co-develop sector-specific governance protocols—ranging from healthcare and finance to education and national security—and generate buy-in from a wide range of institutions. Additionally, as outlined in Section III, the EU's AI Act categorizes by risk levels: unacceptable, high-risk, and minimal-risk, which allow for differentiated regulatory treatment.[93] The US should follow a similar approach. A tiered regulatory model that scales obligations based on the risk profile, size, and function of systems would further ease adoption, particularly for small and medium-sized enterprises. Implementing a risk-based model would encourage responsible deployment without stifling innovation in industries where AI plays a transformative role.

To address First Amendment concerns while ensuring accountability, content moderation policies should emphasize transparency and procedural fairness. Unlike the EU, where strict platform liability rules govern content removal, the US must balance speech protections with digital safety. A potential solution is mandating transparency reports from major platforms detailing content moderation decisions, AI-driven enforcement measures, and user appeals processes. With this "New School Speech Regulation" approach, private platforms can be held accountable without content being directly regulated.[94] The establishment of an independent digital media branch within the "Department of Technology" could provide nongovernmental adjudication of content-related disputes while ensuring due process for users affected by content moderation decisions. Operations could work in tandem with similar efforts (e.g., Meta's Oversight Board). The US government may also establish voluntary best practices and regulatory sandboxes—controlled environments where AI developers can test innovations under regulatory supervision. This approach would allow policymakers to refine AI governance frameworks based on real-world applications while enabling companies to adapt to evolving regulatory requirements without excessive compliance burdens. The National

---

[93] EU AI Act, *supra* note 42.

[94] Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018).

Institute of Standards and Technology (NIST) has already taken steps toward AI risk management frameworks, and expanding these initiatives into a broader regulatory partnership would ensure that industry expertise informs legislative developments. [95] Lastly, public trust is needed in the longevity to carry the success of this framework. The governance of AI must be transparent, inclusive, and democratically accountable.

CONCLUSION

The rapid evolution of digital media and artificial intelligence is reshaping the global landscape, presenting profound opportunities and challenges that demand modern governance. This paper outlines the transformative impacts of AI, the proactive strides taken by the EU through the DSA and AI Act, and spotlights the stark contrast of the fragmented regulatory approach currently seen in the US. The US, while a leader in technological innovation, lags in its digital regulation, relying on outdated pieces of legislation. Given the extraterritorial aspect of the EU DSA and AI Act for business operations worldwide, the US needs to establish a regulatory path that: one, reaffirms its sovereignty over digital technology use; two, safeguards the US economy; and three, promotes American values of liberty, privacy, and innovation while procuring international alignment. The current laissez-faire approach not only poses risks to individual rights and societal values but also exposes the nation's economy, credibility, and security on the global stage. It is imperative that American leadership expands to the forefront of life-altering technologies, starting with the realm of digital media and AI governance to maintain and increase its soft powers. "In America, law and policy are made through often messy processes of discourse, deliberation, and democratic forms of decision-making," which means the implementation of a legislative path forward needs to progress in a meaningful way.[96] Respectfully put forth in this paper is a digital media and AI governance game plan.

As the world steps to the brink of another new digital wave with the widespread use of AI technologies, the US must choose to shape the digital landscape rather than be shaped by it. The US should embrace the challenges and opportunities that arise from AI with generational vision to craft a regulatory framework that will best serve the nation,

---

[95] *AI Risk Management Framework*, NIST (Jul. 26, 2024), https://www.nist.gov/itl/ai-risk-management-framework.

[96] O. CARTER SNEAD, WHAT IT MEANS TO BE HUMAN: THE CASE FOR THE BODY IN PUBLIC BIOETHICS1 (Harv. Univ. Press 2020).

frontrunning amongst the world. What is the opportunity cost of doing nothing at the precipice of AI-driven global transformation? With the digital natives of Gen Z rising into the workforce and continuing to influence greater society, the "do less" rationale has reached its expiration. It is time to do more.