The Impact of the European Union's Digital Services Act on the United States: Perspectives from American Stakeholders

Nicholas Alexander Sidor

University of Michigan

School of Information

4/25/2023

Research Statement

America houses some of the largest tech platforms in the world. However, the European Union sets global standards for Internet governance and platform regulation. The Digital Service Act (DSA) is an effort to recognize that the current online system is an unregulated space needing provisions that build safety and trust. It outlines a framework of values for operating in Europe's digital space and places new obligations on private and public stakeholders. This landmark bill challenges America's position as a global influence, and its swift legislation forces policymakers in the U.S. to realign their own digital governance and regulation strategies. This research investigates the potential impact of the DSA on the United States. To do so, I conducted an extensive literature review of scholarly material available on the topic and three expert interviews with digital policy scholars. Interviews were aimed at identifying experts' perceptions about the DSA, with a focus on whether and to what extent the bill may influence digital policy and legislative processes in America.

Table of Contents

Introduction

The increasing dominance of tech platforms and the advent of artificial intelligence has created a need for regulating the digital space to ensure safety and trust for all stakeholders of the Internet. The fundamental rights of Internet users must be protected, along with accountability for e-commerce services and intermediaries. The European Union has been at the forefront of digital governance. Its recent legislation, the Digital Service Act (DSA), sets a framework for values organizations must follow while operating in the digital space. This landmark bill has implications beyond The EU's single market. Its efficient process and extensive regulation cause policymakers in the United States to reevaluate their digital governance strategies.

This study examines the impact of the DSA on the United States, with a focus on how American stakeholders perceive the bill and to what extent it may influence the digital policy and legislative process in the United States. The first section provides context on the DSA in its development status as of March 2023. The following section looks at the efforts of the current Biden-Harris Administration, focusing on relevant digital governance initiatives and legislation in the United States. The digital policy perspectives of both governments are later analyzed via literature reviews and interviews with digital policy experts.

The findings of this study are presented and discussed, highlighting the perception of the DSA by American stakeholders and its potential impact on digital governance in the United States. Ultimately, this research aims to shed light on the implications of the DSA on digital governance, providing insight for policymakers and stakeholders as they navigate the digital landscape.

The Digital Services Act

The Emergence & Overview of the DSA

The digital age has dramatically transformed how people interact, communicate, and access information. Although digital platforms have provided numerous benefits, they have also introduced challenges related to illegal and harmful content, user protections, and fair competition (European Commission, 2022). To address these issues, the European Union (EU) introduced the Digital Services Act (DSA), a legislative proposal aimed at establishing a standard set of rules for intermediaries across the EU's single market or internal commerce (European Commission, 2022).

The impetus for the Digital Services Act came from the European Democracy Action Plan, which President Ursula Von Der Leyen introduced in 2019 to empower Europeans and strengthen democracies. The action plan was considered a "digital revolution" in which

European democracy would be protected by leveraging digital spaces to bridge the gap between the public and policymakers (European Democracy Action Plan, 2020).

The EU recognized an opportunity to strengthen democracy and bring governance to the Internet by using emerging forms of digital communication. Strengthening democracy refers to the protection of election integrity, media transparency, and proactive measures against misinformation. The Digital Services Act was an unprecedented move to accomplish this mission in one swift maneuver.

President von der Leyen promised that the DSA would "ensure that the online environment remains a safe space, safeguarding freedom of expression and opportunities for digital businesses. It gives practical effect to the principle that what is offline should be illegal online. The greater size, the greater the responsibilities of online platforms" (European Commission, 2022).

The official vote approving the DSA in April 2022 marked the culmination of a three-act legislative process referred to as the proposal, opinion, and reading stages. President von der Leyen hailed the passage of the DSA as "historic, both in speed and substance" (European Commission, 2022). The proposal stage began in June 2020, with a series of meetings discussing issues related to digital services and platforms, including the spread of illegal and harmful content, election fraud, and misinformation (European Commission, 2020).

The potential impact of the proposed policies was surveyed across a diverse panel of nearly 3,000 stakeholders within the EU and its strategic partners; the US, UK, and Canada (European Commission, 2020). A two-section strategy incorporated stakeholders from both the private and public sectors, involving business providers of all sizes, advocacy groups, national authorities, academia, the tech community (ICANN, Internet Architecture Board), International governance (UN, Council of Europe), and the general public (European Commission, 2020).

These consultations helped the EU and its stakeholders define the issues that made the Internet an unregulated space and suggest forward-thinking policies to make it safer. The data and feedback collected from June to December 2020 formed the proposal introduced to the European Commission. The first half of 2021 saw the production of official reports by three European Commission departments during the opinion stage, which is part of the ordinary legislative procedure.

The final reading stage took place in April 2022 when the bill was read and approved by vote. Only a month later, the European Parliament solidified its approval of the DSA with written amendments to the bill. Throughout the year, the European Commission held discussions over the DSA, and on October 27, 2022, a copy of the Digital Services Act was published. The

official journal granted 15 months for all stakeholders to address new obligations before the EU enforces the new law. Big tech companies like Meta have been granted four months (European Union, Proposal, 2020).

The Digital Services Act establishes an unprecedented standard for online platform accountability concerning illegal and harmful content, ensuring better protection for Internet users and their fundamental rights (European Commission, 2022). The DSA aims to create a single set of rules within the Internet market, facilitating the growth of smaller platforms by eliminating cross-border barriers (European Commission, 2022).

It imposes greater responsibilities on larger platforms, reflecting the potential risks associated with their size and influence. To enforce these rules, the European Commission will supervise large platforms and have the authority to impose sanctions on up to 6% of their global turnover. In the case of repeated serious breaches, they may ban the platform from operating in the EU. (European Commission, 2022).

The DSA represents a significant milestone in the regulation of digital platforms within the European Union. The swift legislative process carried by the momentum of the European Democracy Action Plan demonstrates the EU's commitment to addressing the challenges of the digital age and protecting its citizens and businesses existing in digital spaces.

Key Goals

The framework of the DSA is not built solely to punish bad behavior online but to cultivate a less toxic environment for all entities within the EU's digital landscape. For users, the act ensures the protection of fundamental rights, more choices (fair competition), and less exposure to illegal content. For digital providers, it means a harmonization and standard set of rules that lead to easier start-up and scale of digital services. For businesses, it will create a fair market and work to eliminate competition created by illegal goods. For society at large, it grants greater democratic control and oversight over systemic platforms, which mitigates their risk of manipulation or disinformation.

The framework's intentions are admirable, but how are they possible? That answer came from three stages of stakeholder feedback and public consultation that helped draft the DSA. Specifically, they helped draft the new obligations that support key goals set by the framework. The DSA states that efforts of traceability and transparency must exist between online marketplaces and their users, with reasonable efforts to check whether products or services are illegal.

The DSA includes effective safeguards for users, including the possibility to challenge platforms on content moderation decisions and place bans on certain types of adverts targeting

children or use special categories of personal data such as race, political views, or sexual orientation. Concretely, the DSA contains actionable measures to counter illegal goods, services, or content online, such as mechanisms for users to cooperate with platforms and authorities as "trusted flaggers" to identify illegal activity or potential violations (DSA: Ensuring, 2020).

Transparency for online platforms also includes measures for algorithms used for recommendations. This places an obligation on large platforms to conduct risk-based actions and allow independent audits of their risk management systems. In regards to the capability of platforms to meet these obligations, earlier feedback promoted innovation toward blockchain technology to support transparency and traceability (European Union, Proposal, 2020).

Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age, stated, "Platforms should be transparent about their content moderation decisions, prevent dangerous disinformation from going viral, and avoid unsafe products being offered on marketplaces" (DSA: Commission welcomes, 2022).

New Rules

Although rules governing digital spaces previously existed in the EU, they were dated in comparison to the digital landscape created by technological advancements. The e-Commerce Directive, established two decades prior, has been the primary legal framework for digital services in the EU, regulating digital services in the European single market. However, over the past 22 years, the online landscape has transformed with platforms facilitating innovation, cross borders trading, and creating new opportunities for businesses (European Commission, Questions and Answers, 2022). These platforms have also been exploited for disseminating illegal content and selling illegal goods or services. Some larger platforms have become public spaces with unique risks for users' rights and information flows.

The Digital Services Act (DSA) builds on the rules of the e-Commerce Directive to address the emerging issues surrounding online intermediaries. Different regulations across Member States have created barriers for smaller companies looking to expand, resulting in varying levels of protection for European citizens. The DSA aims to lift unnecessary legal burdens due to different laws, fostering a better environment for innovation, growth, and competitiveness. Simultaneously, it seeks to uphold fundamental rights and protect all users in the EU from illegal goods, content, and services (European Commission, Questions and Answers, 2022).

The Digital Services Act is a massive legal document with over 300 pages of detailed rules and regulations. The DSA establishes a comprehensive framework to address a wide range of issues, such as content moderation, user rights, platform transparency, and systemic risks. The legislation encompasses new responsibilities and enforcement powers for the European

Commission and national authorities. The European Commission broadly categorizes these rules into thirteen obligations.

1. Clear Rules for how to handle illegal content and mechanisms for users to flag illegal content online. The DSA updates the process by which digital services providers must remove illegal content based on national or EU law. The new process reinforces an EU-wide ban on general content monitoring, such that platforms won't be forced to systematically police themselves to the detriment of free speech (Albert, 2023).

2. New rights for users to challenge content moderation decisions, with platforms required to provide detailed explanations for blocking accounts or removing or demoting content, and offering users the right to challenge these decisions and seek outside settlements if necessary (Albert, 2023).

3. Enhanced transparency on recommender systems and online advertising, including clear and intelligible terms and conditions, transparency on the algorithms used for recommending content or products, and clear information about ad targeting and how to change its parameters. Users must be offered at least one alternative “feed” not based on profiling. It also calls for clear transparency from all influencers advertising commercial communications. (European Commission, 2022; Albert, 2023).

4. New obligations for the protection of minors on any platform in the EU and a ban on targeting advertisements to children profiling individuals based on “sensitive” traits like religious affiliation or sexual orientation (European Commission, 2022; Albert, 2023).

5. General transparency and reporting requirements, including the production of annual reports on content moderation efforts detailing the number of orders to take down illegal content, the volume of user complaints and their handling, and descriptions of any automated systems used to moderate content and their potential accuracy and error rates (European Commission, 2022; Albert, 2023).

6. Obligations for the largest platforms (VLOPs) to rein in systemic risks by formally assessing how their products, including the algorithmic systems, may exacerbate risks to society. Measurable steps must be taken to prevent such risks, including oversight through independent audits of their risk management systems (European Commission, 2022; Albert, 2023).

7. Legally-mandated data access for external scrutiny, with platforms required to share their internal data with independent auditors, the European Commission, Member State authorities, and researchers from academia and civil society for the identification of systemic risks while holding platforms accountable for their obligation to address them (European Commission, 2022; Albert, 2023).

8. A unique oversight structure, with the European Commission as the primary regulator for VLOPs and VLOSEs, enforcement powers similar to those it has under antitrust proceedings, and an EU-wide cooperation mechanism established between national regulators and the European Commission. This includes new competencies and enforcement powers over the largest platforms and search engines, imposing fines of up to 6% of global turnover, and applying supervisory fees to help finance enforcement tasks (European Commission, 2022; Albert, 2023).

9. A ban on using 'dark patterns' on the interface of online platforms refers to misleading tricks that manipulate users into choices they do not intend to make (European Commission, 2022).

10. New provisions that allow access to data for researchers of key platforms to scrutinize how platforms work and how online risks evolve. Platforms will be held accountable for how they handle concerns raised by the research. (European Commission, 2022).

11. Users will have new rights, including a right to complain to the platform, seek out-of-court settlements, complain to their national authorities in their language, or seek compensation for breaches of the rules. Representative organizations will also be able to defend user rights against large-scale breaches of the law (European Commission, 2022).

12. A new crisis response mechanism in cases of serious threat to public health and security, such as a pandemic or a war (European Commission, 2022).

13. The liability rules for intermediaries have been reconfirmed and updated by the co-legislator, including a Europe-wide prohibition of generalized monitoring obligations (European Commission, 2022).

Impact of Obligations

The Digital Services Act confronts the challenge of regulating the Internet by building a concrete framework that defines the intentions of the DSA along with a set of obligations that enforce accountability. The EU describes the framework as a foundation built on European values that rebalances the rights and responsibilities of Internet users, providers, platforms, and authorities. The term "providers" refers to intermediaries or hosting services, online platforms, and large platforms (anything that reaches over 10% of the 450 million consumers in Europe).

Online platforms and companies will be forced to accommodate the new obligations in proportion to their size, with the understanding that their size may increase (DSA: Ensuring, 2020). For example, whistleblower Frances Haugen exposed Meta's dark algorithms that intentionally harmed teen girls (WSJ, 2021). In this type of event, the platform (Facebook) would have to show the European Commission how it has allocated time, money, and resources to rectify the problem before it can continue to operate in the EU's single market. Meanwhile, a

new start-up with a small number of employees would be expected to report on potential dangers its product imposes and how it intends to mitigate harm to its users. The start-up's obligations would increase with its growth. The rapid growth of online platforms will be granted a 12-month transitional period to address new obligations (European Union, Proposal, 2020).

Perhaps the most progressive and impactful part of the DSA's transparency efforts is the obligation for all large platforms to grant researchers access to key data to understand how online risks evolve. This oversight will require many resources to address complex systems operating on the Internet. EU countries will take on primary roles of monitoring digital entities within their borders with the support of a new European Board for Digital Services. Large platforms will be under the supervision and enforcement of the European Commission.

Commissioner for the Internal Market, Thierry Breton, stated that large platforms have acted "too big to care" regarding regulation and safety (DSA: Commission welcomes, 2022). The DSA obligates platforms to grant access to safety surveillance by agencies approved by the European Commission. Penalties for apathy, obfuscation, or policy violations may incur sanctions of up to 6% of the corporation's global turnover and possible expulsion from the EU's single market. All providers, whether they are based in Europe or not, must comply with the new rules (European Commission, Questions and Answers, 2022).

Entities established outside of the EU will have to appoint a legal representative, as many companies have already done as part of their obligations in other legal instruments. The European Commission states that online intermediaries will benefit from legal clarity, liability exemptions, and a single set of rules when providing their services in the European Union (European Commission, Questions and Answers, 2022).

Next Steps

Following the adoption of the Digital Services Package in the first reading by the European Parliament in July 2022, both the Digital Services Act and its sister legislation, the Digital Markets Act (DMA), have been adopted by the European Union and published in the Official Journal of the European Union on October 27th, 2022. The DSA entered directly into force on November 16th, 2022, and will become applicable across the EU and apply 15 months after or from January 1st, 2024, whichever comes later after entry into force (European Commission, 2023).

By February 17th, 2023, online platforms were required to publish their numbers of active users. Suppose a platform or search engine has more than 45 million users (10% of Europe's population). In that case, the Commission will designate the service as a very large online platform, "VLOPs," or very large search engines, "VLOSEs" (Albert, 2023). This concerns Article 24(2) and Recital 77 of the DSA. Against this background, this document provides answers to several questions that the Commission received from providers of

intermediary services in light of the February 17th, 2023, deadline laid down in Article 24(2) DSA for the first publication of information on the number of average monthly active recipients of the service (European Commission, DSA: Guidance, 2023).

VLOPs and VLOSEs were granted four months to comply with the DSA. These obligations include carrying out and providing the commission with its first annual risk assessment (European Commission, 2023). The February deadline also set one year for DSA rule compliance. By February 17th, 2024, EU member states were tasked with appointing Digital Services Coordinators (DSCs). The DSCs are responsible for enforcing rules on smaller platforms established in their country as well as liaising with the Commission and other DSCs in broader enforcement efforts. In addition, all platforms with less than 45 million users will be expected to comply with DSA rules.

The implementation of the DSA involves four notable steps.

Step One: Assessment

Assessment of user numbers to determine VLOP and VLOSE status. By February 17th, 2023, platforms and search engines were expected to report their active end users in Europe to the EU Commission. The Commission must then assess the validity of these reports to determine which services meet the 45 million active EU user threshold. Based on initial disclosures, platforms such as Facebook, Instagram, Google, YouTube, TikTok, and Twitter are expected to qualify (Albert, 2023).

Step Two: Compliance

Once designated as a VLOP or VLOSE, these entities will have four months to comply with the DSA's rules (European Commission, 2023). This includes conducting and publishing their first annual risk assessment and implementing content moderation rules. Users should begin to notice changes on platforms, such as easily operated features for flagging illegal content and updated Terms and Conditions that are clear and intelligible to all users, including minors (Albert, 2023).

Step Three: Empowerment

On February 17th, 2024, the DSA will become fully applicable across the EU for all entities within its scope. By that time, each EU member state must appoint its own Digital Services Coordinator (DSC), an independent regulator responsible for enforcing the rules on smaller platforms established in their country and liaising with the commission and other DSCs in broader enforcement efforts (Albert, 2023).

Step Four: Supervisory Fees

Under the DSA, the Commission is empowered to impose a fee on providers under its supervision, which is expected to be levied for the first time in autumn 2023. The delegated regulation provides legal certainty to service providers designated as VLOPs or VLOSEs under the DSA. It specifies the methodology and procedures for calculating and levying the supervisory fee. The delegated regulation will be transmitted to the European Parliament and the Council, which have three months to scrutinize it (European Commission, 2023).

Challenges and Enforcement

Following the implementation of the DSA implementation timeline, EU countries and the Commission must build the necessary capacities and human resources to adequately enforce the law. The Commission recently launched a European Centre for Algorithmic Transparency to aid its enforcement efforts. It has promised to thoroughly examine VLOP and VLOSE compliance starting in the summer of 2023 (Albert, 2023).

Enforcement battles are anticipated, as seen with recent turmoil from Twitter under its new owner Elon Musk. This may prove to be an early test for EU watchdogs looking to enforce the DSA (Albert, 2023). Twitter's rollout of a paid verification system immediately turned into a chaotic mess, creating a flood of misinformation that included high-profile accounts being spoofed and announcing to people with diabetes that insulin is now free (Belanger, 2022).

Haphazard rollouts that lead to platform misinformation and potentially cause real-world damage will trigger investigations and significant fines under the DSA, given the law forbids VLOPs from implementing any major design change without conducting a prior risk assessment. Because the DSA establishes one set of platform regulations for the entire EU, some national digital regulations, like Germany's NetzDG, may have to be revised (Albert, 2023). This could be considered positive enforcement, given heavy criticisms over NetzDG by the UN Human Rights Committee (Baghdasaryan, Gullo, 2021).

Future Developments

Beyond open questions on enforcement, several delegated acts, implementing acts, potential codes of conduct, and voluntary standards referenced in the DSA have yet to be developed. These will eventually clarify certain aspects of the law, such as the technical conditions for data sharing between platforms and external researchers (Albert, 2023). The delegated regulation for supervisory fees proposed by the European Commission follows a public consultation on the draft that took place between December 22, 2022, and January 19th, 2023. Following the scrutiny period, the European Parliament and the Council may provide

further input on the delegated act, shaping implementation and enforcement (European Commission, 2023).

The Digital Services Act represents a significant step towards regulating Big Tech and creating a safer and more accountable online environment in the EU. As the implementation process unfolds, all stakeholders need to collaborate and address the challenges that arise during enforcement. By monitoring the DSA's progress and adapting its rules and procedures accordingly, the European Union can work towards achieving its goal of shaping a more transparent and responsible digital future.

Digital Governance in the United States

Digital governance has evolved significantly over the past few decades, with a history of prioritizing innovation over-regulation in the United States. As the digital landscape has expanded, so have the nuances that come with governing it. Current efforts by the Biden administration and the Office of Science and Tech Policy have attempted to define the values, rights, and standard practices of data and algorithms to necessary regulation in a "culture of innovation." Looking at America's recent shift of focus from innovation to ethics, we can predict that digital governance in the US will increasingly include conversations surrounding privacy protection, fostering competition, addressing algorithmic bias, and platform content moderation. With a comprehensive look at digital governance in the US, we will be able to compare it to European policies, such as the Digital Services Act.

Innovation Over Regulation in Early US Digital Governance

Over the past 25 years, US innovation policy has consistently emphasized fostering an environment that promotes entrepreneurship, technological advancement, and economic growth. The core principle of Internet policy during the late 1990s was "permissionless innovation" which creates a legal and regulatory environment that enables entrepreneurs to experiment with new business models without seeking approval from regulators (Thierer, Haaland, 2019). The Clinton administration argued that "the Internet should develop as a market-driven arena, not a regulated industry" (Thierer, Haaland, 2019).

Starting with the Clinton administration's Framework for Global Electronic Commerce in 1997, US innovation policy took a market-driven approach to the internet, prioritizing a minimalist and simple legal environment for commerce. This set the stage for the thriving technological landscape we know today (Thierer, Haaland, 2019).

Successive administrations, including Bush, Obama, and Trump, have continued to support pro-innovation policies, with initiatives like the American Competitiveness Initiative, released by Bush in 2007 to put the United States at the forefront of science and technology.

Bush stated, “The great engine of our growing economy is our Nation’s capacity to innovate” (Thierer, Haaland, 2019).

During the following Obama administration, the Senate unanimously approved the development of the “Internet of Things” (IoT), a strategy to “incentivize the development of the Internet of things in a way that maximizes the promise connected technologies hold to empower consumers, foster future economic growth, and improve our collective social well-being” (Thierer, Haaland, 2019).

President Obama updated the Strategy for American Innovation, which continued America’s focus on innovation in what Obama called “the technological frontier” (Thierer, Haaland, 2019). The succeeding Trump administration carried innovation policy forward for another presidential term by creating the White House Office of American Innovation. The office brings together stakeholders from the public and private sectors to develop innovative technologies to support government agencies. Both Obama and Trump utilized digital policies and initiatives to reduce unnecessary government spending (Simonite, 2018).

The Biden-Harris Approach to Digital Policy

As represented by the Biden-Harris Administration, the United States’ approach to digital governance is upheld by two foundational pillars (Knight Foundation, 2022). The first pillar emphasizes the importance of privacy protections, particularly for children, fostering competition in the tech industry, ensuring algorithmic fairness by guarding against bias and discrimination, and promoting algorithms and content moderation transparency.

The second pillar revolves around the Declaration for the Future Internet, which has garnered support from over 60 nations, advocating for an Internet free from censorship, universally accessible, and governed by multiple stakeholders to preserve its democratic nature. These high-level pillars outline America’s perspective on digital governance.

Although President Biden has not endorsed any specific regulation, he acknowledges the need for legislative action, particularly concerning special protections for big tech, potential amendments to Section 230, and privacy laws. However, the details of such legislation are left to ongoing, bipartisan negotiations in the legislative branch.

Foundational Pillars

Pillar One: Tech Issues Flagged for Concern

The Biden Administration has recognized the importance of addressing digital privacy, competition in the tech space, and algorithmic bias and discrimination. These concerns can be

identified by four official statements and policies that have been proposed or implemented during Biden's time as President and his prior office as Vice President of the United States.

The first point of concern from the Biden Administration is digital privacy, with a focus on children. In 2021, The Federal Trade Commission (FTC), under Biden, reinforced its commitment to enforce the Children's Online Privacy Protection Act (COPPA) (Vedova, 2022). The Rule imposes certain requirements on operators of websites or online services directed to children under 13 years of age and on operators of other websites or online services collecting personal information online from a child under 13 years of age (Vedova, 2023).

Secondly, in July 2021, President Biden signed an Executive Order on Promoting Competition in the American Economy. This order called for the creation of The White House Competition Council to address issues in agriculture, prescription medicine, telecommunication, and technology. The Order stressed, "Too many small businesses across the economy depend on those platforms and a few online marketplaces for their survival. And too many local newspapers have shuttered or downsized, partly due to the Internet platforms' dominance in advertising markets" (The White House, 2021).

Promoting Competition in the American Economy prevents the accumulation of excessive market power and reduces the influence of large technology companies. It states enforcement of "Antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially when they stem from serial mergers, the acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects" (The White House, 2021).

In its broad sense of technology policy, the executive order acknowledged the importance of addressing protection against bias and discrimination (The White House, 2021). However, it has not released any specific policy targeting algorithmic bias and discrimination. The issue can be recognized as a third concern due to the National Artificial Intelligence Act, signed into law in 2021. It called for the National Science Foundation (NSF), in coordination with the White House's Office of Science and Technology Policy (OTSP), to form a National AI Research Resource (NAIRR) Taskforce. It consulted a range of experts and stakeholders from government agencies, private industry, academia, and civil and disabilities rights organizations. It was informed by ongoing interagency efforts around leveraging cloud computing resources to support federally funded AI research and development (National Science Foundation, 2023).

Developing research and departmental formations regarding digital governance and technology has been continually promoted throughout the Biden Administration. The Executive Order on Promoting Competition in the American Economy carves out space for a fourth point

of concern, transparency into algorithms and content moderation. The policy acknowledges the importance of a fair and open Internet, which may suggest future policy development in this area (The White House, 2021). Specifically, issues of transparency in broadband Internet prices create a digital divide. It also encourages the Consumer Financial Protection Bureau (CFPB) to issue rules allowing customers to download their banking data and take it with them (The White House, 2022).

In terms of content moderation, President Biden has concerns about Section 230 of the Communications Act, which provides liability to online platforms for third-party content. He called for its revocation, arguing that tech companies avoid responsibility for the content shared on their platforms. He stated, "Section 230 should be revoked, immediately should be revoked, number one. For Zuckerberg and other platforms" (Kingsbury, 2020). Section 230 has been a highly criticized piece of legislation, and various bills have been introduced in ill attempts to surgically remove it (Jeong, 2019). The president believes that repealing or amending Section 230 would hold these companies accountable for the information they disseminate, promoting a safer and more transparent environment

The Biden Administration has taken steps to address digital privacy, competition in the tech space, and algorithmic bias and discrimination. While some policies have been implemented, others require further development to ensure comprehensive protection for all citizens in the digital age. In consideration of these four main concerns, a clear perspective on digital policy can be seen through the tenets of the second pillar, The Declaration for the Future Internet.

Pillar Two: The Declaration for the Future Internet

The Declaration for the Future of the Internet, launched by the United States along with 60 global partners, is a timely response to the rising trend of digital authoritarianism, where some states have to take steps to repress freedom of expression, censor independent news, interfere with elections and promote disinformation across the globe (U.S. Department of State, 2022).

This collaborative effort, aligned with existing processes in the United Nations, G7, G20, OECD, WTO, ICANN, and Freedom Online Coalition, among other organizations, aims to fortify these institutions and promote the principles of a free, interoperable, and secure global Internet (U.S. Department of State, 2022). It was developed through intensive work with international partners, industry, academia, and other stakeholders. The United States and its endorsing partners are committed to implementing these principles and promoting a global vision while respecting each other’s regulatory autonomy and adhering to domestic laws and international legal obligations (U.S. Department of State, 2022).

The Declaration’s core commitments:

- Protect human rights and fundamental freedoms of all people.
- Promote a global Internet that advances the free flow of information.
- Advance inclusive and affordable connectivity so that all people can benefit.
- Promote trust in a global digital ecosystem with the protection of privacy.
- Protect and strengthen a multistakeholder approach to governance.

(U.S. Department of State, *Declaration for the Future of the Internet, 2022)*

Although not targeted at specific countries, the declaration's principles serve as norms that all nation-states should follow, particularly concerning issues like censorship, unlawful surveillance, and other forms of digital authoritarianism. It is described as not an end but rather a beginning to a continuous conversation on digital policymaking. It remains open to additional partners who wish to join and uphold its principles. The collaborative effort will reinforce the work of multilateral and multi-stakeholder institutions' work in shaping the Internet's future (U.S. Department of State, 2022).

Efforts from the OSTP

President Biden's digital policy approach is strongly supported by the Office of Science and Technology Policy (OSTP). Former OSTP Director, Dr. Alondra Nelson, focused the office's efforts on two key aspects: data and algorithms. This dual-pronged approach is evident in the administration's initiatives, such as the CHIPS Act and Blueprint for the AI Bill of Rights. Both endeavors were carried out and are now being supported by the Office of Science and Technology and the National Science Foundation.

Data

The CHIPS Act (Creating Helpful Incentives to Produce Semiconductors Act) addresses the data aspect of President Biden's digital policy approach, specifically focusing on the semiconductor industry. Semiconductors are vital components in modern electronics and digital devices, and the act aims to bolster the domestic production and supply of these essential chips.

The CHIPS Act, which combines two bipartisan bills, was passed in August 2022. It seeks to enhance the United States' competitiveness in the global market by investing in semiconductors research, design, and manufacturing. It provides financial incentives, such as grants and tax breaks, to encourage domestic production and reduce reliance on foreign suppliers. By doing so, the act seeks to address the vulnerabilities of the supply chain and promote long-term economic growth and national security (The White House, 2023).

Dr. Alondra Nelson, speaking at the Knight Foundation's INFORMED CONFERENCE 2022, discussed the data aspects of digital policy, highlighting the CHIPS and Science Act. She noted that one of its key components is the authorization to move forward with a National Secure Data Service. To be polluted by the National Science Foundation, this service aims to provide privacy-protected access to federal data. Nelson emphasized that the government is acting as a prime mover in ensuring data safety and helping the American public understand that taxpayer data belongs to them. The government is working on creating systems to grant access to this data while collaborating with the research community to achieve those goals (Knight Foundation, 2022).

Algorithms

The White House Office of Science and Technology Policy (OSTP) has identified five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence. This initiative aims to eliminate inequity, embed fairness in decision-making processes, and affirmatively advance civil rights, equal opportunity, and racial justice in America. It directly responds to the signed order on President Biden's first day in office, The Executive Order On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (OSTP, 2023).

The principles outlined in the Blueprint for the AI Bill of Rights, a white paper published by The White House, support practices and governance of automated systems (OSTP, 2023). They include public accountability, non-discrimination, fairness, transparency, and human-centered values. The White House believes that these principles will help protect the public from the potential harms of AI and ensure that AI is advanced for the public good. In October of 2022, the OSTP released a Blueprint for the AI Bill of Rights based on the outline of five key principles.

I. Safe and Effective Systems: You should be protected from unsafe or ineffective systems.

II. Algorithmic Discrimination Protections: You should not face discrimination by algorithms, and systems should be used and designed in an equitable way.

III. Data Privacy: You should be protected from abusive data practices via built-in protections and have agency over how your data is used.

IV. Notice and Explanation: You should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.

V. Human Alternatives: Consideration and Fallback: You should be able to opt-out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

(OSTP, 2023)

By building on existing work and learning from the experiences of experts in the field, the Blueprint for the AI Bill of Rights acts as a roadmap and positions the government as "a first mover, not only in the market but also in shaping values surrounding technology" (Knight Foundation, 2022). The OSTP's Blueprint provides practical guidance for government agencies to take action and regulate algorithms while using existing regulatory powers to ensure better outcomes. This proactive approach supports President Biden's vision for "A world with more robust legislative protection in the realm of digital policy" (Knight Foundation, 2022).

Implementing the CHIPS Act with the AI Bill of Rights demonstrates the Biden administration's commitment to addressing data and algorithmic aspects of digital policy. The OSTP's support for these initiatives highlights the importance of fostering technological innovation, ensuring ethical and responsible use of algorithms, and securing a reliable supply of critical components to maintain the United States' position as a global leader in the digital era.

European Vs. American Digital Policymaking

The Digital Services Act (DSA) and the Biden-Harris Administration's approach to digital governance both aim to create a safer, more accountable, and more competitive digital landscape. However, their scope and implementation differ. The DSA is a more comprehensive, blanketing legislative proposal. At the same time, the current digital governance under the Biden Administration covers a broad range of specific issues and relies on existing US regulatory bodies for enforcement (see Table 1).

Digital Policy	EU Digital Services Act	U.S. Biden Administration
Scope	Regulates all digital intermediaries across the EU, including social media platforms, search engines, online marketplaces, and web hosting / content-sharing services. Scales responsibilities in the proportion of entity size.	Focuses on improving equity and access by regulating specific, digital economy issues, including antitrust enforcement, privacy, taxpayer data access, broadband infrastructure, and global competition in technology.
Content Moderation	Focus on transparency and accountability, ensuring platforms remove illegal content promptly with "trusted flaggers" and standard operating procedures.	Calls for removal of Section 230 as a form of 'platform indemnity.' Encourages platforms to take responsibility for moderation while maintaining American values of free speech.

Market Competition	Creates a level playing field for businesses, targeting the dominance of VLOPs and VLOSEs while fostering start-ups and addressing issues of self-preferencing, data access, and interoperability.	Appointed strong antitrust advocates in key positions and encouraged closer scrutiny of mergers and acquisitions involving large tech companies. Addresses vulnerability in supply chain shortages.
Consumer Protection	Requires transparent information about terms of service. Protects users from fraud and establishes complaint mechanisms.	Expressed the need for a national privacy framework and made steps to develop it with a Blueprint for the AI Bill of Rights.
Enforcement	Established ECAT to aid in enforcement. Member states assign DSCs while the EU Commission handles large platforms. Violators face sanctions of up to 6% of global turnover and possible expulsion from the EU's single market (internal commerce).	Reliance on existing agencies such as the Federal Trade Commission (FTC) and the Department of Justice (DOJ) to identify violations and enforce digital policies, focusing on strengthening their capacity and resources.

Table 1: *Digital Policy Comparison Between EU and US*. Source: European Commission, 2022, the EU Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348; *Fact Sheet: Executive Order on Promoting Competition in the American Economy*, by The White House, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/

By comparing the DSA to the current US approach, we can identify potential areas of alignment and divergence in digital policy. The comparison sheds light on the current state of digital governance in both regions, contributing to a better understanding of their potential influence over stakeholders and the trajectory of future regulations. Reflecting on the evolution of digital governance in the United States, we see a clear transition from prioritizing innovation to addressing ethical and societal concerns. The Biden-Harris administration's approach to digital policy, with its two foundational pillars, demonstrates a moral commitment to regulating the Internet, data, and algorithms so that Americans can experience more equitable outcomes, reinforcing the importance of ethical development while maintaining a culture of innovation.

Research

Research Questions

This study will employ a combination of literature review and expert interviews within the academic community to investigate the impact of the Digital Services Act (DSA) on the United States. The research seeks to identify the perceptions of key stakeholders within the U.S. digital policy landscape regarding the DSA and to what extent this may influence the development of similar laws in the United States.

The research poses two questions:

RQ1: How do stakeholders in the United States perceive the EU's Digital Services Act?

RQ2: How likely will the Digital Services Act influence digital governance in the United States?

Literature Review

This literature review ruminates on research questions by looking at digital governance from a global perspective and then adjusting the focus to examine the current digital policy frameworks in the European Union and the United States. Lastly, it considers the expert opinions forecasting the impact of the DSA on the United States.

The review begins by exploring the global perspective of digital governance by defining the current era of technology and global movements, such as the right to be forgotten and the General Data Protection Regulation (GDPR). Additionally, the review examines emerging trends from the first year of EU GDPR enforcement and UN criticism of digital governance, highlighting the complex process of regulating the online public sphere.

The Digital Services Act is then analyzed, with an examination of the bill's intentions and consideration toward the UK and EU as regulatory first movers. Furthermore, the review considers access to data and algorithms for the effective implementation of the DSA.

A detailed look at the DSA is balanced by examining digital policy in the United States. This includes breaking down The Declaration of the Internet, the Blueprint for the AI Bill of Rights, and concerns over Section 230. These documents, in combination with an intelligence report, were combined with expert panel talks to glean a perspective on how digital governance is being approached in the United States.

The review concludes with expert opinions on the impact of the DSA on digital governance in the United States. These opinions are sourced from Brooking's articles and panel discussions forecasting the impact of the DSA on American stakeholders. Through a comprehensive exploration of digital policy from macro to micro, the review provides valuable insight into how the United States perceives the DSA, and how likely it is to influence its digital policymaking.

Digital Services Act Precursors

To understand how digital governance, specifically the Digital Services Act, is perceived, it is necessary to start at a good vantage point. Looking at previous eras of technology, we can recognize the direction of the Internet's growth and the needs of its users. Jonathan Zittrian's article, *'Three Eras of Digital Governance,'* maps out this timeline. He writes that "digital governance today is dramatically different than it was when the study of "Internet governance" coalesced in the late 1990s" (Zittrain, 2019).

Zittrain's observations draw three eras, the first being a more positive timbre focused on the Internet's capabilities and the *end user's rights*. A clear shift occurred toward the negative regarding the digital governance framework in the following *public health era*, where the harms and risks of technology began to be weighed more heavily (Zittrain, 2019).

The article beckons the dawn of the third *process or legitimacy era*. It is a time for digital governance efforts to reconcile the *rights* and *public health* frameworks with new institutions that can address issues and bring them to closure. Zittrain acknowledges the challenges of balancing individual liberty and collective security, particularly with the rise of intermediaries (2019).

Furthermore, the lack of trust in many civic and private institutions and the complex and deeply debated issues surrounding digital governance have led to uncertainty and contradiction regarding policies for intervention versus abstention among powerful private intermediaries like Facebook, Google, and Cloudflare. No matter how American stakeholders view the DSA, they undoubtedly look at digital governance as the need to reconcile the struggle between rights and public health.

Zittrain suggests that the next era of digital governance should focus on creating inclusive and deliberative processes that are legitimate and ideally federated without limiting the digital expression of ideas (2019). A framework that balances regulation and freedom is by no means a simple task, especially with minimal case studies or examples of institutions implementing this style of governance. One example that we do have is the European Union's General Data Protection Regulation (GDPR).

The GDPR is a comprehensive data protection law that came into effect in the European Union (EU) in May 2018. The purpose of the GDPR is to provide individuals with greater control over their data and to harmonize data protection laws across the EU.

Under the GDPR, organizations are required to obtain explicit consent from individuals before collecting and processing their personal data. Individuals also have the right to access, correct, and delete their data. The GDPR also imposes strict requirements on organizations to protect personal data from unauthorized access, disclosure, or theft. Failure to comply with the GDPR would put organizations at risk of significant fines and penalties, including fines of up to 20 million euros or 4% of their annual global revenue, whichever is greater (GDPR, 2023).

The GDPR represented a significant step forward in data protection and privacy rights, providing individuals with greater control over personal data and holding organizations accountable for how they handle personal data. It acted as a precursor for digital governance in Zittrain's era of *process*, where user rights and public health are reconciled by fair regulation (Zittrain, 2019). However, was the GDPR void of conflict? How was it enforced? The answer to those questions would bounce around the minds of those drafting the DSA a few years later.

One contention with the GDPR was its introduction of the 'right to be forgotten,' a legal concept allowing individuals to request the removal of personal information from search engines and other online platforms (Shefet, 2019).

Dan Shefet is a lawyer involved in several cases related to the right to be forgotten. He has argued that the right to be forgotten can conflict with the right to freedom of expression and that it is important to balance these two rights (Shefet, 2019). He has also argued that the right to be forgotten should not be used to suppress information in the public interest, such as information about public figures or events of public importance (Shefet, 2019).

While individuals have a legitimate interest in protecting their privacy and reputation, there is also a need to ensure the public has access to information important for democratic decision-making and accountability. The battle between human rights and public health is again an accurate prediction of Zittrain's three eras of digital governance (2019).

Aligned with Zittrian's opinion that federal institutions should regulate and enforce these issues, The GDPR is enforced by the European Data Protection Board and surveilled by the Data Protection Authority (DPA) of each Member State (Harvey, 2018). By looking at GDPR enforcement, we can draw similarities to the DSA's structure and penalties. The DSA also sets up a new department to guide enforcement with the ability to find organizations a percentage of their global turnover (European Commission, Questions and Answers, 2022). Perhaps, by

looking at enforcement trends, we can predict how stakeholders in the United States will receive the DSA's enforcement.

Catherine Barret's article "*Emerging Trends from the First Year of EU GDPR Enforcement*" discusses the implementation and enforcement of the GDPR during its first year of operation. Barret noted a significant increase in the number of data breach notifications since the GDPR came into effect, which reflects both the heightened awareness of organizations regarding their obligations under the regulations as well as the increased scrutiny and enforcement actions taken by regulatory authorities (Barrett, 2019).

The GDPR's enforcement ability to raise awareness, in turn, prompted new, positive behaviors around digital services. Barret highlighted a growing trend of 'privacy by design,' where organizations started incorporating privacy and data protection principles into their products and services from the outset rather than retrofitting them after the fact. This approach is recognized as a proactive way to minimize the risk of data breaches and privacy violations (Barrett, 2019).

Besides the inevitable nuances of digital governance, the GDPR's rollout and enforcement significantly impacted data protection practices and raised the bar for privacy protection worldwide. Barrett's article noted that the GDPR continues to be enforced, and as privacy concerns become more prominent, organizations will need to continue to prioritize data protection measures to ensure compliance (Barrett).

It is encouraging to view the GDPR as an overall success, especially when considering the DSA's similar framework and encapsulation of the GDPR as a built-in regulation (European Commission, Questions and Answers, 2022). However, not all digital legislation in Europe has gone over so smoothly. Germany's NetzDG law threatens violators with fines one and a half times that of the GDPR (Modzelewska, 2020). Yet, its enforcement has been criticized by the likes of the UN Human Rights Committee (Baghdasaryan & Gullo, 2021).

The NetzDG law puts social media platforms to police online speech, requiring them to remove "obviously illegal" content, including hate speech, within 24 hours of being notified or face large fines (Baghdasaryan & Gullo, 2021).

The UN Human Rights Committee expressed concerns that the law may be too broad and could restrict freedom of expression. It also criticized the lack of transparency and due process in the enforcement of the law, as well as the potential for over-censorship and the chilling effect on free speech (Baghdasaryan & Gullo, 2021).

The committee urged Germany to take steps to ensure that the NetzDG law is consistent with international human rights standards, including the right to freedom of expression. The committee recommended increased efforts to promote digital and media literacy to enable individuals to better identify and respond to forms of harmful content and hate speech (Baghdasaryan & Gullo, 2021).

Zittrain's keen warning of an ongoing debate over the appropriate balance between freedom of expression and the regulation of online content has proved to be a major challenge in the *era of the process* of digital governance (Zittrain, 2019). A conference at Columbia University in the fall of 2022 discussed how online speech could be regulated while balancing freedom of expression and protection of individual rights.

"*Session IV, Part 1: Regulating Online Speech: Between the First Amendment and the Digital Services Act"* covered a panel's discussion on the challenge of freedom of expression vs. regulation by citing Germany's NetzDG, digital governance processes in Latin America and the GDPR's foreshadowing of the Digital Services Act.

The panel discussed the DSA by considering the difference between US and European approaches to regulating online speech. The US prioritized free speech, and the EU emphasized protecting individual privacy while combating hate speech and disinformation (Columbia University, 2023).

The panelists acknowledged that solutions to regulating online content are complex and often problematic. They highlighted the difficulty in defining illegal content and the potential of abuses in fragile democracies, such as those in the "global south" (Columbia University, 2023). The idea of "trusted flaggers" for decentralized content moderation was mentioned, but questions remain about whether such a system would give users more agency than they currently have online (Columbia University, 2023).

Christina Campbell, a leading expert in international law and human rights in Latin America, discussed the concepts of "harmful but legal" and "oversight implementation" in the context of social media regulation. The panelists also explored the lack of consensus across regions on the problems that must be addressed and the means to solve them (Columbia University, 2023).

"Harmful but legal" refers to content that may be considered offensive, inappropriate, or harmful to certain individuals or groups but is not explicitly illegal under existing laws. This content may not violate specific regulations but could still negatively impact users and contribute to a toxic online environment. Social media platforms often face challenges balancing the need

to protect users from such content while upholding the principles of free speech expression (Laidlaw, 2017, pgs 278-302).

‘Oversight implementation” refers to establishing and enforcing rules, guidelines, and procedures to ensure compliance with social media regulations. This may involve monitoring and evaluating how platforms moderate content, handle user complaints, and implement policies addressing hate speech, disinformation, and cyberbullying. Oversight implementation often requires coordination between regulatory authorities (Gowa, Binns, Katzenbach, 2020).

Transparency and process were identified as key aspects of regulation, but questions remain about the scope and limits of transparency and oversight implementation (Columbia University, 2023). The panelists expressed concerns that regulation cannot remain content neutral, may not focus on underlying harms, and may lack clear oversight processes (Columbia University, 2023).

Regarding the Latin American context, the panelists pointed out the region's unique legal frameworks, such as explicit prohibitions on prior censorship and indirect restrictions on freedom of expression (Columbia University, 2023). They noted that Latin America lacks a section 230-like intermediary liability regulation, excluding Brazil. Instead, the region has addressed online content regulation primarily through courts and jurisprudence, resulting in case-by-case solutions (Columbia University, 2023).

Leaving moderation to a focused, case-by-case basis was debated against Europe’s approach to the Digital Services Act. Panelists stressed the importance of transparency to ensure fairness and rule of law. Although some panelists felt transparency was too vague of a term to enforce, others cited the DSA’s efforts of transparency as a necessary way to understand what platforms are actually doing about content moderation (Columbia University, 2023).

Proponents of the DSA noted that European legislation is value-oriented and aimed at protecting public health, consumer protection, and user autonomy (Columbia University, 2023). The panel came to a consensus that self-regulation and platform autonomy would continue to play a role in the DSA’s implementation. They expressed hope that, despite nuanced challenges, common ground could be found to ensure stable and democratic online spaces for future generations (Columbia University, 2023).

We find ourselves in an era of digital governance where rights and public health must be balanced in a way that regulates the processes of digital intermediaries. The DSA represents an ambitious attempt to achieve this balance, building on the foundations laid by the GDPR and learning from the challenges faced by legislative actions like Germany's NetzDG law.

The DSA aims to create a more inclusive and deliberative process, as Zittrain proposed, that addresses individual liberties and collective security. As digital governance continues to evolve, it is crucial to strike the right balance between freedom of expression and the need to protect individuals from harmful content.

While the DSA's implementation and enforcement will undoubtedly face challenges and debate, it presents an opportunity for international collaboration and learning. By observing and analyzing the success and shortcomings of the GDPR and other legislative efforts, stakeholders can better understand how to shape the future of digital governance in a way that promotes transparency and upholds democratic values.

The Implementation of the Digital Services Act

The Digital Services Act (DSA) is a new regulation by the European Union aimed at modernizing and harmonizing the regulatory framework for digital services with a single set of rules for the entire EU. Coming into force on November 16th, 2022, the objective of the DSA is to ensure a safe and accountable online environment while promoting innovation and competitiveness in the digital sector (European Commission, 2020).

The new legislation is designed to update rules in the e-Commerce Directive, which has been in place since 2000. The e-Commerce Directive provides limited liability for online intermediaries for user-generated content. Still, it does not provide clear rules for online platforms on how to moderate the content or ensure transparency in their content moderation policies.

The DSA sets horizontal rules covering all services and all types of illegal content, including goods and services. The act does not replace or amend but rather compliments sector-specific legislation such as the Audiovisual Media Services Directive (AVMSD), the Directive on Copyright in the Digital Single Market, the Consumer Protection Acquis, or the Proposal for a Regulation on preventing the dissemination of terrorist content online.

The DSA introduces several new obligations for digital intermediaries to follow, including:

- Measures to counter illegal goods, services, or content online, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers."
- Traceability of business users in online marketplaces to help identify sellers of illegal goods and reasonable efforts by online marketplaces to perform random checks on products and services to identify whether they are considered illegal in any official database.

- Effective safeguards for users, including the possibility to challenge a platform's content moderation decisions.
- A ban on certain types of targeted advertisements on online platforms, such as those targeting children or using special categories of personal data like ethnicity, political views, or sexual orientation.
- Transparency measures for online platforms on a variety of issues, including the algorithms used for recommendations.
- Obligations for a very large platform (VLOPs) and very large online search engines (VLOSEs) to prevent the misuse of their systems by taking risk-based action and undergoing independent audits of their risk management systems.
- Access for researchers to key data of the VLOPs and VLOSEs to understand how online risks evolve.
- Oversight structure to address the complexity of the online space, with EU countries taking the primary role, supported by a new European Board for Digital Services and the Commission supervising and enforcing rules for VLOPs (European Commission, 2020).

All platforms, except the smallest ones (employing fewer than 50 persons and whose annual turnover or annual balance sheet does not exceed 10 million euros), will be required to set up mechanisms that collect and respond to complaints, perform out-of-court settlements, cooperate with trusted flaggers, vet the credentials of third party suppliers, and provide user-facing transparency of online advertising (European Commission, 2020).

In addition, VLOPs and VLOSEs reaching at least 45 million users are subject to specific rules due to the risk they pose in the dissemination of illegal content (European Commission, 2020). VLOPs will have to meet risk management obligations, undergo external risk auditing and maintain public accountability, provide transparency of their recommender systems and user choice for access to information, as well as data sharing with both authorities and researchers.

The Supervision of the DSA rules will be shared between the European Commission and the Member States. The Commission will primarily be responsible for VLOPs and VLOSEs, while the Member States will be responsible for smaller platforms within their regions (European Commission, 2020). The commission will have the same supervisory powers it has possessed under current anti-trust rules, including investigatory powers and the ability to impose fines of up to 6% of global revenue (European Commission, 2020).

Member States were required to designate competent authorities, known as Digital Services Coordinators (DSCs), by February 17th, 2024, to supervise compliance of the services

established on their territory with the new rules. They will also participate in the EU cooperation mechanisms proposed by the DSA (European Commission, 2020).

The DSC will be an independent authority with strong requirements to perform its tasks impartially and with transparency. This new coordinator within each Member State will be an important regulatory hub, ensuring coherence and digital competence. They will cooperate with an independent advisory group called the European Board of Digital Services, which can support analysis, reports, and recommendations and coordinate the new tool of joint investigations by Digital Service Coordinators (European Commission, 2020).

The Digital Services Act represents an essential step forward in the regulation of digital services in the EU, complementing existing sector-specific legislation. It includes specific requirements for platforms of different sizes and introduces risk management obligations for large entities. While legitimate concerns about its potential impact on free speech and innovation exist, the need to address the growing challenges of online harmful and illegal content is undeniable. The DSA, with its supervision between the Commission and the Member States, will likely continue to be the subject of debate and discussion as it moves into its implementation phase.

As the Digital Services Act strives to establish a comprehensive regulatory framework for digital services in the EU, it is essential to consider the interplay with other significant legislation in the same field. One such legislation is the Digital Markets Act (DMA). In conjunction with the DSA, it seeks to address a wide array of challenges related to digital markets.

In the article *"Access to Data and Algorithms: For an Effective DMA and DSA Implementation"* (Edelson, Graef, Lancieri, 2023), the authors discuss the ambitious obligations introduced by both the DMA and DSA that require digital platforms to share data and information with various stakeholders and enhance transparency in content moderation and algorithmic control. As these regulations are implemented, their impact on the digital landscape and the way they interact with each other will be critical in shaping digital governance in the European Union.

The DMA and DSA obligations mandate digital platforms to share certain types of data information with regulators, vetted researchers, competitors, and society more broadly. These regulations also impose transparency obligations regarding digital platforms' internal content moderation activities and the algorithms controlling digital markets (Edelson et al., 2023).

The big question surrounding the DSA and other digital legislation is how can its new obligations actually be carried out. The article provides a detailed mapping and categorization of the 54 data access and transparency obligations present in the DMA and DSA, aiming to develop

insights on how to implement these provisions effectively while minimizing the tensions with conflicting interests (Edelson et al., 2023).

The research article also presents a case study of three selected obligations to identify implementation challenges that regulators, companies, and civil society must overcome (Edelson et al., 2023). The obligations discussed include the creation of a database for online advertisement (Article 39 of the DSA), granting vetted researchers access to internal data from large digital platforms (Article 40 of the DSA), and mandating very large platforms (VLOPs) to share click-and-query data with smaller competitors (Article 6(11) of the DMA)(Edelson et al., 2023).

Beyond the DSA setting obligations, it further acts as a framework by supporting future legislation in digital governance. The conclusion of the article outlines how the categorization exercise can be extended to other EU legislation under discussion such as the proposal for an AI Act and Data Act (Edelson et al., 2023). The authors emphasize that the challenges faced during the implementation of the DMA and DSA package do not end there, and future EU legislation also contains obligations relating to transparency and access to data. Their goal was to demonstrate how the categorization and variables could help rationalize obligations under discussion in complex regulations and facilitate discourse around the harmonization of rules that apply to digital markets in an overlapping way (Edelson et al., 2023).

The report was an in-depth look at how the obligations of the DMA and DSA can be carried out. By looking at potential implementations, it became clear that regulation like the Digital Services Act is only the beginning, and a piece of legislation that stands as a solid framework for additional legislation, such as the AI Act and Data Act.

This evolving regulatory environment has inspired other nations to adapt at varying speeds, as highlighted by Tom Wheeler in his article "*The UK and EU Establish Positions as Regulatory First Movers While the US Watches*" (2023). The EU has been proactive in introducing the GDPR and DSA; the UK has similarly pursued its own path with the Online Safety Bill (Wheeler, 2023). Meanwhile, the US maintains a more cautious stance.

As the European Commission implements the DSA, it is developing the "DNA of a regulator" (Wheeler, 2023). The UK's parliament has established the Digital Markets Unit (DMU) within their Competition and Markets Authority (CMA) and Ofcom, the UK's equivalent of America's FCC (Wheeler, 2023). The UK's DMU will be responsible for the Online Safety Bill and is working to build up staff while already conducting market studies and consultations to define their ultimate actions (Wheeler, 2023).

The UK and EU digital regulation initiatives are based on the common law "Duty of Care," which holds that providers of goods and services are responsible for anticipating and

mitigating the adverse effect of their offerings. Governments are stepping in because they believe digital platforms companies have not sufficiently exercised this "Duty of Care." The initiatives focus on identifying risks by platforms and mitigating them(Wheeler, 2023).

To prevent incompatible regulations that would disrupt consumers and companies, there is a heightened awareness of the need for compatibility between EU and UK policies. UK agencies, Ofcom and the DMU plan to pursue "participatory regulation," working closely with target companies to develop enforceable behavioral expectations (Wheeler, 2023).

The US is a passive observer of activities in the UK and EU. Congress has failed to pass either privacy or competition protection legislation. The Federal Trade Commission (FTC) is looked to for regulatory intervention but is under-resourced, underemployed, and over stretched with responsibilities extending across the entire economy. The FTC made headlines when it recently added a dozen people to its new Office of Technology. Still, that workforce pales in comparison to the hundreds of specialists being mobilized in the EU and UK (Wheeler, 2023).

Wheeler (2023) points out that the major digital platforms are American companies that have successfully used their economic and political power to keep Congress from acting. Having achieved what they wanted, they now face the reality that nations, where they are not national assets, will be making rules for the interconnected world.

London and Brussels are creating a *de facto* global digital risk management standard. The US will have a difficult time participating in the development of a global standard if it has no policy of its own. As a result, American platforms are looking at a future in which others define the rules, and then the US government, late to the party, decides, "Well, you do it over there; let's set the standard for American markets as well" (Wheeler, 2023).

Wheeler (2023) suggests that the different approaches to digital regulation could have significant implications for the future of the digital economy. The EU and UK's more proactive approach could lead to greater trust in online platforms, while the US's hands-off approach could result in a loss of trust and legitimacy in the digital sector. As countries around the world respond to these developments, understanding diverse approaches to digital regulation will be crucial in fostering a more interconnected and harmonized digital landscape (Wheeler, 2023).

The Digital Services Act represents a significant step forward in modernizing and harmonizing the regulatory framework for digital services within the European Union. The new rules and obligations introduced by the DSA aim to create a safer and more accountable online environment while promoting innovation and competitiveness in digital sectors. As the EU and Member States work towards the effective implementation of these obligations, nations outside of the EU are adapting at varying speeds, with the UK pursuing a similar regulatory path and the US and parts of Latin America adopting a more cautious, observatory stance.

The interplay between the DSA and other relevant legislation, such as the DMA, is critical in shaping digital governance in the EU. The implementation of these new obligations will be challenging. Still, by taking a comprehensive and coordinated approach, all stakeholders can work together to overcome obstacles in a way that creates more transparency and accountability in the global digital landscape.

As the DSA provides a robust framework for future legislation, it will be crucial to monitor and assess the impact of these new rules. The evolving regulatory landscape in the EU and UK is shaping global digital risk management standards, making it imperative for other nations, including the US, to develop harmonized rules for digital governance.

Ultimately, the successful implementation and enforcement of the DSA and related legislation will determine the extent to which digital spaces can become safer, more transparent, and more accountable. The ongoing debate and discussion surrounding the implementation of the DSA will highlight the importance of collaboration and cooperation on a global scale.

Digital governance in the U.S.

Digital Governance in the United States is often issue-oriented. In her article "*Section 230 Load Bearing Wall*," Nabiha Syed and two legal scholars discuss the implications of Section 230 of the Communications Decency Act of 1996, which provides immunity to online platforms from liability for user-generated content (Syed, 2023).

Syed argues that Section 230 has played a critical role in the growth of the Internet and online platforms, allowing for innovation and the development of new forms of communication and expression (Syed, 2023). However, she notes that there are concerns about the impact of Section 230 on the spread of harmful content online, including hate speech, disinformation, and illegal activities (Syed, 2023).

Section 230 is referred to as a "load-bearing wall" for the Internet, supporting the growth and development of online platforms while also providing important protection for free speech and innovation. However, Syed argues that the current application of Section 230 may need to be revisited (Syed, 2023).

The author suggests that a more nuanced approach to Section 230 is necessary, one that considers both the law's benefits and the challenges posed by harmful content (Syed, 2023). She notes that this approach should include greater transparency and accountability in content moderation practices and targeted reforms to address specific types of harmful content, such as hate speech and disinformation (Syed, 2023).

The discussion implies that the confusion and varying interpretations of Section 230, especially in terms of publishing scope and algorithms neutrality, highlight the need for a clearer understanding of the legislation and its intended goals (Syed, 2023).

The two legal scholars, James Grimmelman and Kate Klonick, discuss the implications of the Gonzales v. Google cases on Section 230 to suggest the following ideas for revamping Section 230:

- Revisiting the legislative intent of Section 230 to encourage Internet platforms to moderate content without being held liable for content that falls under the radar.
- Ensuring that platforms can remove harmful content without fear of legal repercussions, thus preventing "collateral censorship" of valuable content.
- Clarifying the scope of publishing, including activities such as recommending, endorsing, prioritizing, or presenting the information.
- Discarding the concept of "neutral algorithms" and recognizing that algorithms inherently contain human bias.
- Redirecting liability to individual speakers rather than third-party amplifiers of speech in absence of Section 230.
- Consider the implications of the case on generative AI, as a ruling against algorithmic recommendation could make generative AI ineligible for Section 230 protection.

Online speech regulation is very complex and evolving in nature. It requires careful consideration of the potential impacts of laws like Section 230 on free speech and innovation (Syed, 2023). Specific regulations must be carefully weighted to ensure they reflect the Internet of today, and the potential future, as opposed to the Internet of the mid-1990s.

Section 230 will continue to be a topic of concern in digital governance, as its call for removal has been made by both President Biden, and US Senators like Gary C. Peters, from Michigan. Senator Peters was ranked as the most effective Senator in the 116th Congress (2019-2020), despite being a minority (Volden, 2022). Among various legislation, Senator Peters helped author and pass the CHIPS and Science Act. In an email correspondence, the Senator stated that Section 230 was intended to protect America's constitutional right to free speech, however it does not excuse online platforms from their responsibility to monitor the spread of harmful activity on their systems. Senator Peters wrote, "I believe that Section 230 must be modernized. We can maintain a free and open internet while also making sure people are safe and engaging only in legal activity online (US Senator Gary C. Peters, 2023).

As digital governance in the US addresses specific issues, it also appears to be cognizant of the broader implications of regulations, which play a significant role in fostering government trust and can ultimately lead to either the globalization or fragmentation of nations on a technological scale.

The National Academies of Sciences, Engineering, and Medicine report on "*Cryptography and the Intelligence Community: The Future of Encryption*" underscores the challenges in predicting the extent of government regulation of cryptocurrencies and the possible consequences of national and international dynamics (Columbia University, 2023). It addresses the complex interplay between society and digital governance with several findings.

The report emphasizes the challenge of predicting government regulation of cryptocurrencies, with criticisms surrounding low and high regulation levels (Columbia University, 2023). The future role of intelligence agencies in accessing financial information remains uncertain. While increasing technological interdependence promotes globalization and similar approaches to encryption, government regulation of communications technology may lead to fragmentation along national lines due to competing national security concerns (Columbia University, 2023). Early detection of trends is crucial for risk management.

National regulations to enhance cybersecurity, curtail hate speech, and protect user data privacy may vary significantly around the globe. A rise in mistrust of governments may lead to a corresponding growth in encrypted communications (Columbia University, 2023). Individual countries or blocs of like-minded countries might impose content requirements at national levels, such as banning or discouraging end-to-end encryption or mandating various governmental access to otherwise encrypted communications (Columbia University, 2023).

The report on how the intelligence community perceives encrypted technology suggests the US is cognizant of the significant impact that digital regulations can have on technological cooperation and interdependence on a global scale. While no definitive strategies have emerged, the US has recognized the need for a collaborative approach to address these challenges. "*A Declaration for the Future of the Internet*" serves as a preliminary step in convening nations to discuss and develop shared digital governance principles. This collective effort aims to mitigate the risks of fragmentation along national lines and foster an environment that encourages innovation, respect for human rights, and sustainable growth in the digital age.

"A Declaration for the Future of the Internet" is a call for a new digital declaration that invites all nations to actively support a future for the Internet that is free, global, and secure (U.S. Department of State, 2022). The document acknowledges the potential of digital technologies to promote democracy, sustainable development, and the enjoyment of human rights and

fundamental freedoms. However, it recognizes the risks inherent in reliance on the Internet and the challenges we face.

The document highlights the importance of protecting human rights online and across the digital ecosystem (U.S. Department of State, 2022). The partners in this declaration intend to work towards an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy.

The declaration affirms the importance of maintaining an open and free Internet: "The immense promise that accompanied the development of the Internet stemmed from its design: it is an open 'network of networks', a single interconnected communications system for all of humanity" and "the once decentralized Internet economy has become highly concentrated, and many people have legitimate concerns about their privacy and the quantity and security of personal data collected and stored online" (U.S. Department of State, 2022). The document calls for use of digital technologies to reinforce democracy and respect for human rights and offers opportunities for innovation and maintaining connections between our societies.

The document outlines a set of principles to promote the vision, which includes the promotion of affordable, inclusive, and reliable access to the Internet for individuals and businesses where they need it and support efforts to close the digital divide around the world to ensure all people of the world are able to benefit from the digital transformation (U.S. Department of State, 2022). The partners in this declaration intend to promote and use trustworthy network infrastructure and service suppliers, relying on risk-based assessments that include technical and nontechnical factors for network security.

The document also emphasizes the importance of protecting individuals' privacy and personal data: "Protect individuals' privacy, their data, the confidentiality of electronic communications and information on end-users electronic devices, consistent with the protection of public safety and applicable domestic and international law" (U.S. Department of State, 2022).

A Declaration for the Future of the Internet is a comprehensive document that outlines a set of principles to promote an open and secure Internet. It highlights the importance of protecting human rights and promoting democracy and innovation in the digital ecosystem (U.S. Department of State, 2022).

In addition to a digital declaration, the United States has also drafted a white paper referred to as a "*Blueprint for an AI Bill of Rights*," which aims to develop a set of principles specifically designed to protect digital rights in the rapidly evolving landscape of artificial

intelligence and automation. The White House Office of Science and Technology Policy (OSTP) has identified the use of technology, data, and automated systems as one of the greatest challenges facing democracy today, as these tools often threaten the rights of the American public.

The Blueprint for the AI Bill of Rights states, “Too often, these tools are used to limit our opportunities and prevent our access to critical resources or services” (OSTP, 2022). However, while these negative outcomes are well documented, the potential benefits of automated systems are also significant, from helping farmers grow food more efficiently to identifying diseases in patients.

To ensure that technology and data do not come at the price of civil rights or democratic values, the White House Office of Science and Technology Policy has identified five principles to guide the design, use, and deployment of automated systems in the age of artificial intelligence. These principles are designed to protect the American public from threats posed by automated systems that can meaningfully impact the public’s rights, opportunities, or access to critical needs” (OSTP, 2022).

The five principles outlines in the Blueprint are as follows:

1. Transparency: “Automated systems should be designed to provide all relevant stakeholders with clear information about how they work and what data they use and allow for meaningful public scrutiny” (OSTP, 2022, p.5).
2. Fairness and Non-discrimination: “Automated systems should be designed to be fair, unbiased, and to mitigate unjust impacts while increasing opportunities for all Americans” (OSTP, 2022, p.5).
3. Privacy and Security: “Automated systems should be designed to protect personal privacy, prevent data breaches, and minimize risks to personal safety and security” (OSTP, 2022, p. 6).
4. Accountability: “Automated systems should be designed to be accountable, auditable, and to allow for due process in the event of errors or harms” (OSTP, 2022, p. 6).
5. Participation and Empowerment: “Automated systems should be designed to enhance the ability of all Americans to participate in the democratic process and to empower individuals and communities to shape the decisions that affect their lives” (OSTP, 2022, p. 7).

The Blueprint is a response to the experiences of the American public and is informed by insights from researchers, technologists, advocates, journalists, and policymakers. The Blueprint is accompanied by *From Principles to Practice*, a handbook for anyone seeking to incorporate these protections into policy and practice, including detailed steps towards actualization.

The Blueprint for an AI Bill of Rights, along with its accompanying handbook, represents an attempt to provide a framework for the responsible use of AI in a digital society, ensuring the protection of all individuals (OSTP, 2022). However, the Blueprint is not immune to criticism, and questions about its implementation linger, similar to the concerns raised regarding the Digital Services Act.

The article "*Opportunities and Blind Spots in the White House's Blueprint for an AI Bill of Rights"* addresses the whitepaper's potential effectiveness and limitations and the need for congressional intervention to regulate digital spaces and ensure the ethical development of AI technologies. According to Nicol Turner-Lee, a Senior Fellow at the Brookings Institution, the Blueprint focuses on minimizing potential risks, but questions remain about its effectiveness. While some federal agencies, such as the Department of Defense (DOD) and the U.S. Agency for International Development, have implemented some guidance around government use of AI, there is still a lack of consistency (Lee, Malamund, 2022).

The Equal Employment Opportunity Commission (EEOC) has initiated its own AI and algorithmic fairness program, collaborating with the Department of Labor to "reinvent hiring and recruitment practices." However, there remains a disparity among federal agencies in terms of adherence to these activities, with variations on both timelines and expected outcomes (Lee, Malamund, 2022).

At least a dozen agencies have issued binding guidance for the use of automated systems in their industries, such as the Federal Trade Commission's business guidelines on using artificial intelligence and algorithms and the Food and Drug Administration's principles for Good Machine Learning Practice for Medical Device Development. However, as Turner Lee notes, there is a lack of consistency in adherence to these guidelines (2022).

The Blueprint calls for consistency in the interpretability and protection of civil rights in automated decisions, particularly in the areas of lending, housing, and hiring. However, there is still a lack of knowledge about how civil rights laws are followed within digital domains, given the opacity of the Internet and algorithmic applications.

Individuals often have little idea about how these algorithms work or what data they use, and more algorithmic literacy is needed. The Blueprint calls for consistency in the

interpretability and protection of civil rights. Yet, more work needs to be done to apply civil rights laws and protections when online malfeasance occurs.

The varying degrees of progress within the federal government in implementing the rights-based framework for AI can be attributed to factors such as the number of staff allocated for efficient execution and the different stages of implementing previous guidance during the Trump administration (Lee, Malamund, 2022). When administrations change every 4 to 8 years, an agency can remain apathetic without enforcement.

The current Blueprint relies on the private sector for self-regulatory management, adopting a consumer rights-based approach in governing AI products and services. This expectation might be overly ambitious for companies that profit from AI's opacity and the inferential data collected from users. Furthermore, the absence of mandatory guidelines, an enforcement regime, or a central governing body in the Blueprint renders self-regulation inadequate in safeguarding users against potential harm (Lee, Malamund, 2022).

The concern for lack of enforcement brings up the Blueprint's biggest criticism, the complete lack of regulation for law enforcement. The use of AI in law enforcement particularly faces recognition and "intelligence-led policing" (McGrory, Bedi, Clifford, 2020). AI can reinforce inequality and disproportionately affect people of color, leading to false arrests and detainment. Including law enforcement in the Blueprint could have provided new guardrails and agency for those affected by misidentification or scrutiny from AI technologies (Lee, Malamund, 2022).

The carving out of law enforcement was discussed in detail during a panel hosted by the Brookings Center for Technology Innovation. Experts recommended explicit inclusion of law enforcement, a sectoral approach to AI governance, and revisiting civil rights precedents to make them applicable to digital spaces (Lee, Malamud, 2022).

The OTSP should either offer an addendum to the existing Blueprint for law enforcement applications or include relevant agencies under federal government purview. Reviewing practices around AI use on human subjects and procurement policies is essential, and systems adopted under a "monolithic technology-procurement model" should be reevaluated, as they rarely take constitutional liberty into account (Lee, Malamud, 2022).

A sectoral approach would be critical for advancement and enforcement, as there is no single solution to AI governance. Maintaining flexibility in applying Blueprint's principles would enable tailored, innovative solutions for sectors such as healthcare, housing, and education, where AI often has an intersectional presence (Lee, Malamud, 2022). Taking on a sectoral approach is something the panel described as "what agencies could do but did not," even

under the pressure of two executive orders, the call to track how agencies used AI was all but ignored by everyone except the Department of Health and Human Services (Brookings Institution, 2022).

Agencies would benefit from understanding their inner workings. To achieve this, they require the authority to obtain company data and information before establishing rules. Some agencies possess this authority, while others do not. The lack of a single set of authority impedes the ability to enforce existing laws (Brookings Institution, 2022).

Existing civil rights regimes should be revisited to ensure applicability to new and emerging digital rules (Lee, Malamud, 2022). Historic civil rights laws and statutes pre-date the digital revolution. The panel experts suggested that the White House should create a new commission on civil rights to evaluate the agility of existing law in the digital environment, as unchecked data extrapolation can lead to biases and the disparate impact that have foreclosed opportunities for historically marginalized populations (Lee, Malamud, 2022).

Overall, The Blueprint for an AI Bill of Rights represents a step toward responsible AI use. Still, it may need revisions as it remains to be seen how it will be implemented and whether it will prompt necessary congressional action to govern the unregulated space. As Turner Lee notes, “The proof is going to be in the pudding, in the actualization of these principles and the effectiveness of the various agencies to execute them” (Lee, Malamud 2022).

In light of this growing interest in digital governance, the United States has begun to address specific issues, such as Section 230, and develop documents that set principles for this domain. This shift towards new and necessary policy directions has prompted self-reflection and criticism, which are essential for progress. As America moves forward with its digital mindset, it explores opportunities for shared agendas, as demonstrated by Dr. Alondra Nelson’s discussion at the INFORMED CONFERENCE 2022, hosted by the Knight Foundation.

The Office of Science and Technology Policy (OSTP) was established in 1976 to coordinate research infrastructure Its original focus was on specific research infrastructure topics, such as developing instruments for scientific missions (Knight Foundation, 2022). Over time, the OSTP’s emphasis shifted to data infrastructures and tools that are agnostic to the topic. The founding documents of the OSTP, including the 1976 statute, highlight the need to maximize the benefits of science and technology while minimizing foreseeable harms, aligning with the current Blueprint for the AI Bill of Rights.

Today the OSTP focuses on digital governance, aiming to increase access to data and develop privacy-preserving technologies (Knight Foundation, 2022). The Federal government is increasingly emphasizing evidence-based policy work, which has led to new OSTP

appointments, such as Assistant Directors for Evidence and Policy and Data and Democracy (Knight Foundation, 2022). This development signifies a restructuring of the OSTP's work and a unique opportunity for partnerships between researchers and the government.

Availability and accessibility in science have become essential concerns for the OSTP. The Biden administration has acknowledged the need to create onramps and pathways for data access (Knight Foundation, 2022). Efforts to address accessibility include building platforms for data visualization, cleaning up large datasets, and updating the Public Access Policy for the Federal Government to ensure federally funded research is accessible to the public immediately for peer review (Knight Foundation, 2022).

Looking ahead, the OSTP will focus on a range of tech policy issues, including racial discrimination in healthcare, worker surveillance, and improving data on power grid outages. The OSTP aims to create a more inclusive STEM ecosystem, recognizing past exclusions and striving for a more equitable approach to digital policy (Knight Foundation, 2022).

The evolution of digital governance in the United States has demonstrated a growing awareness of commitment to addressing critical issues, developing guiding principles, and capitalizing on opportunities to create a more equitable digital landscape. Through examining the role of Section 230, the potential impacts of globalization versus fragmentation, and the development of initiatives like the "*Declaration for the Future Internet"* and the "*Blueprint for the AI Bill of Rights,"* we can appreciate the complexities of the American perspective on digital governance.

As the US engages with international regulations such as the Digital Services Act, it highlights the importance of collaboration among nations to ensure a cohesive, global approach to digital governance. As we move forward, continued efforts to foster innovation and protect individual rights will be essential to navigating the challenges and opportunities presented by an increasingly interconnected world.

Impact of the Digital Services Act on the U.S.

In a Brookings article, "The Digital Services Act's Lesson for U.S. Policymakers: Co-regulatory Mechanisms" (2022), David Morar explores the potential benefits of the Digital Services Act for the United States. The DSA offers valuable insights into alternative methods of digital governance that US policymakers can adapt without infringing on First Amendment rights.

Morar (2022) emphasizes that the DSA employs co-regulatory mechanisms, and governance structures that involve limited government involvement and primarily rely on stakeholder groups under government oversight. These mechanisms provide transparency and

inclusivity, creating a more balanced approach to digital governance. Co-regulatory mechanisms such as assessment, codes of conduct, and audits work to achieve the DSA's goals, focusing on transparent, standardized industry actions that involve society and third parties while maintaining external oversight (Morar, 2022).

Assessments examine how platform decisions on content moderation, recommendation systems, terms and conditions, and data practices contribute to systemic risk. Platforms must create these assessments independently. However, the DSA positions the European Commission and national regulators as backstops, granting them the power to issue guidelines and publish comprehensive annual reports on risk and mitigation efforts (Morar, 2022).

The DSA allows for the creation of multi-stakeholder structures to assess systemic risks related to large platforms and search engines and develop voluntary commitments to risk mitigation methods, reporting on frameworks, and access to data metrics (Morar, 2022). The drafting process includes large platforms, industry leaders, civil society, and competent, relevant authorities at the discretion of the EU Commission. While the government plays an active oversight role, the codes of conduct are still considered co-regulatory mechanisms, providing flexibility and collaboration in their development (Morar, 2022).

Independent yearly audits are mandated for large platforms to evaluate their compliance with DSA obligations and the new rules outlined in the code of conduct (Morar, 2022). While the DSA provides recommendations for audits, it does not dictate the audit design. Instead, it encourages the development of voluntary, presumably industry-based, standards for audits. The European Commission maintains oversight but does not directly intervene in the audit process (Morar, 2022).

In the United States, similar governance structures exist, such as the Digital Trust and Safety Partnership (DTSP), which includes major industry players and smaller entities (Morar, 2022); the DTSP has sought input from civil society actors and developed best practices (Morar, 2022). Institutions like the DTSP could either develop co-regulatory mechanisms independently or collaborate with other stakeholders to create more effective digital governance frameworks (Morar, 2022).

In addition, platform governance in the United States faces challenges due to the complexities of technology and the difficulties of legislating without infringing on First Amendment rights (Morar, 2022). Many current legislative proposals focus on revising section 230, which addresses intermediary liability, but this approach is indirect and risky.

The DSA offers an alternative approach by employing co-regulatory mechanisms that tailor regulations to large platforms without impacting the entire digital ecosystem. These

mechanisms can be adapted to the US without violating first amendment rights, unlike Section 230 (Morar, 2022).

These co-regulatory mechanisms within the DSA offer a more inclusive and transparent approach to digital governance, involving various stakeholders and maintaining government oversight. By incorporating these mechanisms, the United States can develop a balanced digital governance framework that respects First Amendment rights while fostering innovation (Morar, 2022).

The DSA's novel approach to regulation and its co-regulatory mechanisms have sparked vital conversations among digital policymakers in America, prompting them to consider alternative solutions to address the increasingly pressing issue of misinformation. As these discussions continue to evolve, it becomes crucial to gain insights from diverse perspectives, such as those presented in "*Can Regulation Solve the Problem of Misinformation?*"

This event brought together distinguished experts, including academics, industry insiders, and policymakers, to explore the regulatory landscape and analyze the impact of policy decisions in the context of online information. The insights shared in the discussion not only shed light on the challenges associated with misinformation but also offer potential solutions from the perspective of those who play roles in American digital policymaking.

The discussion began with an acknowledgment that current online systems are unregulated and that there is a need to promote better ways to build trust and safety online. Its focus was to consider the EU's Digital Service Act and if it could help solve digital governance issues in the United States. The DSA aims to require platforms to take greater responsibility for what is promoted to tier users and to "show their homework" (IFL, 2022) in terms of the steps taken to mitigate harm and risk for users online.

While The EU is setting standards and laws for the Internet, some see this as a make-it-or-break-it way to regulate the Internet. Suggestions from the panel include the US writing its own form of the DSA that accounts for the innate freedoms outlined in the US Constitution and, at the same time, avoiding what they considered pitfalls or sticking points within the DSA, such as attempting to regulate freedom of speech and hold very large platforms (VLOPs) accountable. These skepticisms come from the research side of the panel's anecdotes of Big Tech being noncompliant to data access and former OSTP advisors questioning Congress' willingness to debate free speech and platform indemnity when supported by lobbyists with hundreds of millions of dollars.

The panel agreed that it was time for the United States to join in some kind of leadership position when it comes to the digital space. As they pointed out, with prior legislation such as the

GDPR, what the EU is doing for online safety will eventually be done in the US. It would be more advantageous for America to be a part of the policy-making process.

A “content agnostic approach” was considered the best part of content rules coming out of the European Union. The panelists agree that instead of taking a content-specific approach, which is often seen in the US, it would be better to take a content-agnostic approach to moderation. This means lifting focus from identifying harmful content to looking at the system that is generating this content on a specific platform (IFL, 2020). In a metaphor, it would be akin to fixing the leak in a boat instead of slowly sinking while trying to throw the water out.

The DSA places obligations on platforms to not only be more accountable but to present the measures they take to mitigate online harms and risks, such as misinformation. Researchers discussed the issue of platforms based in America claiming to work against misinformation, even though it was rampant in their services. They made references to congressional hearings that companies like Facebook are a bit of a mystery to lawmakers, and their apologies and promises to combat misinformation seem ingenuine. Frustrated regulators want platforms to do more than reluctantly respond to public pressure.

A suggestion was made that digital products and services in the US should be built with people that oversee trust and safety. Instead of platforms building and releasing digital services and retroactively dealing with problems, they should coordinate more openly with oversight teams. It emphasizes that US agencies are responsible for asking platforms how they implement policies (IFL, 2020). Oversight regulation is parallel to the efforts of the DSA. However, the adoption of trust and safety officials is not likely to happen if it is not required. More recently, Elon Musk dissolved Twitter's Trust and Safety Council following his company purchase (Zakrzewski et al., 2022).

Former advisor to the White House Office of Science and Technology Policy, Suresh Venkatasubramanian, Ph.D., admits that the US is very far behind, partly by design. The political and structural landscape shaped by America’s free speech, media, and innovation concepts act as fundamental blockers that make it hard to think about these issues (IFL, 2022). Unlike the European Union, with its top-down approach, the United States has more opposition, making conversations around digital governance feel like indirect attempts to create forms of censorship.

Perhaps increased conversation and collaboration between public interest and lawmakers would spur policy, as we do in individual states. In February of 230, Utah passed a landmark bill, *S.B. 152 Social Media Regulation Amendments,* requiring social media platforms to verify the age of all social media users in Utah to prevent minors from signing up without parental consent. Before the panel, California had passed a privacy law that was not as expansive but similar to the EU’s GDPR (Wakabayashi, 2018).

While the government on the federal level has failed to govern the digital space, the proactive action taken by individual States has caused experts to express a lack of optimism for the country's capabilities (IFL, 2022). While hearings in the Senate have addressed the need for greater transparency, political barriers have prevented progress.

The US needs to improve its digital governance from the increasing importance of granting independent researchers access to data that platforms have been notorious for holding back. One panelist highlighted Ralph Nader's auto industry transformation by calling for safety regulations. The US could look to its auto industry to provide a model for sharing basic safety data with regulators. However, accessing data from tech platforms raises concerns about privacy and ethical consideration. It requires legal, ethical, and responsible frameworks (IFL, 2022).

The concept of platform indemnity and freedom of speech emerged amongst the panel. In the US context, there is a perception that algorithms amplify voices; therefore, both algorithms and content are a type of speech. This viewpoint tends to categorize digital regulation as a form of censorship. The panel joked that while people have the fundamental right to be idiots, amplified stupidity is dangerous (IFL, 2022).

Section 230 is a clause in a bill that existed pre-social media, and panelists suggested that while platforms should not be held liable for what people post, the poster of harmful content should be held liable. The question of where algorithmic content amplification is a form of free speech and therefore protected is big in US digital governance.

Regarding censorship, the panel felt that there is no agreed-upon definition of "illegal content." Defining illegal content and addressing misinformation online has been a failed attempt by the federal government. Public disapproval was clear after pushback against potential censorship led to the cancellation of Biden's Disinformation Governance Board was permanently paused after only three weeks (Lorenz, 2022).

Regulation of technology platforms should avoid being a knee-jerk reaction to current conversations on misinformation. Many platforms have adopted transparency reporting, but regulators must avoid setting metrics that do not genuinely protect users (IFL, 2022). Regulators must be familiar with emerging technologies and collaborate with experts and stakeholders to develop effective regulation that balances protection against harm with preserving free speech and competition (IFL, 2022).

Regulation is not censorship but rather a means to provide safety, similar to car seat belts (IFL, 2022). The Digital Services Act provides transparency that allows for greater free speech and bridges the information gap between those that know nothing and those that know everything (IFL, 2022).

The panel concluded by acknowledging that EU digital policy will eventually have a knockdown effect on US digital governance and, at the very least, motivate the US to take more

proactive measures to technological issues. Before ending, two questions were posed, “how do we access data safely?” and “How do we make people care about the collection of data?”

To answer the latter question, the experts stated that greater access comes with a tradeoff between access and privacy. They advocated for drafting a code for a risk assessment framework (IFL, 2022). This framework would evaluate the risk and research practicalities, ranking the risk as low, medium, and high. Mechanisms for data sharing based on risk levels are necessary, with both platforms and researchers being held accountable for any abuse of access (IFL, 2022). However, the most valuable data is the riskiest information, and access regimes must prioritize accountability and responsibility.

Perhaps a more pressing issue is getting the American public to care about data collection. One way to do that is to present how much of their lives are dictated by algorithms and moderated content.

Algorithmic ads on TikTok have drawn concern, and geofencing by law enforcement and private security companies raises ethical questions about the appropriate use of surveillance technology (IFL, 2022). Raising awareness about the risks of data collection must be balanced with avoiding scare tactics that may hinder productive conversations. Ethical guidelines and transparency reporting are important, but metrics that incentivize perverse outcomes or hinder competition.

The panel concluded that DSA offers valuable insights and alternative digital governance methods that can benefit the United States. The co-regulatory mechanisms outlined in the DSA provide a more transparent and balanced approach to digital governance while respecting First Amendment rights and fostering innovation.

Through careful analysis of the DSA and lessons learned from the EU’s implementation, US policymakers can adapt these mechanisms to create more effective digital governance. As the panel discussion on misinformation suggests, the US has much to gain from engaging in a more proactive and collaborative approach to digital governance. By leveraging co-regulatory mechanisms, American policymakers can address complex issues such as misinformation, data privacy, and platform accountability.

However, implementing such measures in the United States will require overcoming significant political and structural barriers and fostering a greater awareness and concern for data collection among the public. It is crucial for regulators, industry stakeholders, and researchers to collaborate to develop and adopt legislation that addresses the rapidly evolving landscape of digital governance.

Interview Methodology

Participant Selection

This study's participants are academic experts in technology, information, policy, and law. The entirety of the subject population will be adults over 18 who are located within the United States during the time of research, 1/11/2023-3/24/2023.

Recruitment

Participants were recruited directly through email by the primary investigator.

Location of Research

This study's research took place on the University of Michigan, Ann Arbor campus. Interviews will take place over Zoom video conferencing software or mobile phone. The primary investigator was on location at the University of Michigan, and the participant were interviewed remotely from their location within the United States.

Data collection

Before the interview began, participants were asked to consent to record audio. If the answer was yes, the recording began, and the participant was read the consent briefing by the primary investigator. The procedure continued after they confirmed that they understood the consent brief and consent to an interview.

If the participant did consent to record, answers were transcribed by hand. If the participant denied consent to an interview, the interviewer politely ended the meeting.

Participants were asked for verbal permission to share their identities during the research process and within the research paper. If they denied permission, their identity remained anonymous. If they granted permission, their identity was codified and stored on a separate device.

Once consent was established, the interview took place. The interview process was approximately 30 minutes long. It involved questions based on their knowledge of the Digital Services Act and how they perceive its impact on policy making in the United States. These open-ended and semi-structured questions encouraged participants to share their full opinions. The participants were not asked questions that revealed personal, sensitive, or confidential information.

Once concluded, the participants were thanked for their time, and the recording and communication ended. There was no compensation for the interview as mentioned in the consent form viewed prior to the interview.

Audio recorded to a device from Zoom meetings or mobile phone calls were saved on a secure hard drive with codified participant names. If an interview was recorded, the notes were transcribed into a text document and saved to the same drive. The codified list was stored in a separate, secured Google Drive. Research materials can only be accessed and viewed by the primary investigator or the faculty advisor.

For the full interview script and data management plan, see the Appendix.

Data analysis

The data derived from qualitative research and qualitative content analysis was meticulously coded to discern patterns of similarity and divergence among participants. Interviews were conducted via Zoom, employing the platform's record-to-computer functionality, and subsequently transcribed using an online transcription service (Happy Scribe). To ensure anonymity, all identifying information was expunged from the transcripts, and participants were allocated identification numbers (e.g., Participant One (P1), Particant Two (P2), and Participant Three (P3).

Accuracy of the transcripts were checked three times by the author. Following the accuracy checks, the transcripts underwent a manual coding process for analysis purposes. An iterative coding approach was employed to analyze the data, wherein the transcripts were coded to unveil prevalent themes across the entire data set. A data matrix was implemented to corroborate the accuracy of high-order themes for each participant. For the purpose of enhanced clarity, quotations were subjected to minimal editing.

Ethical Considerations

Participants in the research interview are experts in their respective fields and hold professional positions in academia. Their confidentiality, privacy, and autonomy must be respected during the interview process. Beyond the listed consent forms, the primary investigator reconfirmed their consent for quotations in the paper. Potential harm was reduced by reminding participants that they could stop or skip questions that created discomfort and could end the interview at any time.

Interview Findings

The findings from the interviews conducted during the research phase present the in-depth perspective of three experts in digital policy: One specializing in information policy law, another in data privacy, and a third in online disinformation. All three participants are academics who have significantly contributed to the conversation surrounding the development of the Digital Services Act (DSA).

These experts shared their insights on the DSA and its potential impact on digital policymaking in the United States through their interviews. This section will introduce each participant and summarize their responses concerning the research questions. The findings shed light on how American stakeholders perceive the DSA and how it may shape the future of digital policy in the United States.

Participant One (P1)

Participant One (P1) serves as the director of the technology, media, and communications specialization in an international affairs and public policy school of a private Ivy League university. With a Ph. D. focused on online disinformation, P1 lectures on global media, innovation, and human rights, turning attention towards finding solutions. They provide invaluable insight on the DSA and how its implementation will change the digital landscape in America.

P1 responded optimistically to the Digital Services Act. They stated, “This is an amazing policy and something that needs to be enacted in the US" (Participant One, March 22nd, 2022). As P1 disclosed, their support of the bill may not be shared among organizations in the US that have not spent time understanding it.

Participant One saw great potential in the DSA, yet cautioned that some academics believe it is too robust and difficult to implement, especially in the United States, where freedom of speech topics are often contested. Regardless of opinion, it is apparent to P1 that US stakeholders have a “wait and see attitude” (Participant One, March 22nd, 2022).

When ruminating on US Stakeholder perceptions of the DSA, P1 stated, “The gazillion dollar question is are they going to say, ‘look [is the EU] going to do it for the whole world or not? If so, will we even comply?’” (Participant One, March 22nd, 2022)

P1 also reflected on the fact that US stakeholders can witness the DSA’s new obligations spreading all over Europe, and policymakers should be tracking their progress. Similar legislation is popping up in the UK, opening up similar opportunities for transparency, data access, and algorithms while responding to online harm done to individuals and society.

Participant One stated that it all comes down to how much pressure the European Commission will place on American organizations and will that pressure be effective enough to elicit their response. In the United States, policymakers will most likely remain unresponsive until their hand is forced. (Participant One, March 22nd, 2022). Although they recognize the push for more digital regulation in Europe, there is less and less accountability in America.

The lack of accountability for large platforms was further explained by P1 after they remarked, “Twitter fired many compliance people” (Participant One, 2022). P1 shared a piece of their current lecture to highlight Twitter's heavy workload ahead of the DSA’s implementation efforts.

Twitter must reinforce content moderation, limit targeted advertising, and tackle disinformation, including Elon Musk’s own “fun polls” that the EU Commission sees as biased and harmful. Participant One pointed out that Musk must also prepare for an independent auditor in 2023 and appoint a DSA Compliance Officer. These requirements may be a burden for Twitter, given an EU report in 2022 found Twitter to be far behind other social media platforms in content moderation, only removing 45.4% of flagged hate speech (Participant One, March 22nd, 2022).

Participant One also highlighted that the DSA would impose stricter platform regulations, banning harmful messaging and biased algorithms all over Europe. Furthermore, The EU’s Child Sexual Abuse Materials proposal will force Twitter to screen private messages for child sex abuse imagery and grooming activities (Participant One, March 22nd, 2022).

The future influence of the DSA on US policymakers is up for debate. However, Participant One clarified that US stakeholders would feel the impact regardless. Given that Elon Musk has dissolved the compliance counsel at Twitter, the overall perspective on the DSA may not be serious enough. Ireland has already fined Twitter for its behavior, and P1 does not foresee enforcement taking a backseat with the wider European Union. (Participant One, March 22nd, 2022).

Regarding digital governance, P1 stated, “Legislators in the US have short attention spans. The European Union is much more attentive and thoughtful toward impending issues. We see this with the DSA surveys and extensive planning. In the US, privacy and data access are more possible things.” (Participant One, March 22nd, 2022).

The European Commission has the power to impose large fines, and they are setting up agencies to enforce independent audits on organizations and digital intermediaries. Participant One remarked, “In the United States, we do not have that specific system in place, and we could benefit from the structure” (Participant One, March 22nd, 2022).

The United States could take inspiration from the DSA and apply it to its existing regulation structures. P1 gave an example, “In the US, we have banking regulations that obligate institutions to show that their systems can identify harmful actions” (Participant One, March 22nd, 2022). These actions are similar to the DSA’s new obligations for accountability. By finding commonalities, we might inspire US policymakers.

As the DSA is implemented, Participant One calls for a careful approach to digital governance in the United States. They shared a concern that we (in the US) do not always use tech tools and digital policy correctly. Because we are so politicalized, the power behind informational control may be corrupted by a hyper-focus on ideology or conspiracy that will only hinder progress. P1 shared a viewpoint among American academics: "In the US, the Govt could focus on ‘Woke culture’ for four years and then ‘Q-anon’ for the next four years” (Participant One, March 22nd, 2022).

Participant One suggested that US policymakers recognize the DSA as a call to action. They stated, “We have spent so long defining the problem. We should now legislate, and we know such legislation is possible if we look at the EU" (Participant One, March 22nd, 2022). P1 emphasized that the best summary of the DSA is the simple quote, "process over outcomes" (Participant One, March 22nd, 2022). If US policymakers were to consider those three words, they might share the same optimism for The DSA as Participant One.

Participant Two (P2)

Participant Two (P2) is a policy fellow with New America’s Open Technology Institute, focusing on tech privacy issues. P2 is a visiting scholar with the Schar School of Policy and Government, and serves as a Fellow of the Internet Law and Policy Foundry and Guest Researcher at the Hans Bredow Institut. P2 is an associate editor of a communications technology journal and sits on a committee group at ICANN. They provide a high level expertise on digital policy in both Europe and the United States.

P2 expressed pleasant surprise when asked about their initial reaction to the Digital Services Act. P2 was concerned that the EU might make drastic changes to the E-Commerce Directive, significantly impacting the current state of the Internet (Participant Two, March 27th, 2023).

P2 commended the productive stakeholder engagement and extensive conversation with various parties, ultimately leading to the development and passage of the DSA. They stated, “Most of the time when something like this gets officially proposed, it will go through changes. It will go through a lot of public comment periods, but it will eventually pass.” (Participant Two, March 27th, 2023).

Participant Two believes that most users are not very concerned about the DSA, as it does not have the same hold on people's imaginations as the GDPR did when it was first introduced (Participant Two, March 27th, 2023). However, P2 noted that industry groups, civil society organizations, and those with offices in Brussels are more engaged in conversations surrounding the DSA.

Participant Two described the US reaction as "Well, here is the EU regulating things again" (Participant Two, March 27th, 2023). However, for US Stakeholders tasked with observing these issues, it is a very relevant thing on their mind. P2 explained, "The way that the DSA works is that while it is passed now, there is another giant piece of an unknown puzzle, which is the implementation" (Participant Two, March 27th, 2023).

According to P2, parts of the DSA might not easily fit together with the US system, primarily due to concerns about anti-industry sentiments or First Amendment issues (Participant Two, March 27th, 2023). "It is important to look at it holistically because some things like codes of conduct may not work outside the broad ecosystem created by the DSA. You cannot just import the things you like without also importing the structure that makes them efficient, effective and include mechanisms of accountability" (Participant Two, March 27th, 2023).

Participant Two emphasized the difficulty in drafting a bill similar to the DSA in America, considering the complexity of the US political system, especially in digital governance. P2 stated that in the US, "There would be so much more political horse-trading. There would be a lot more that needs to happen behind closed doors, and then in the open, for it to go anywhere" (Participant Two, March 27th, 2023).

Introducing DSA-like legislation in the US would require a significant shift in how the legislation is written to accommodate the differences in legal perspectives between the EU and the US. A prime example is the American Data Privacy and Protection Act (ADPPA), a bipartisan bill introduced at the end of 2022. Morar noted, "The Biden Administration was not part of the conversation. They were supportive to an extent once it got out, but the administration did not drive it. So, then the conversation becomes, who should be drafting it? Who should be introducing it? This goes back to the previous question about how difficult it would be for something like this to go through, A, unscathed, which is practically impossible, and B, in a big comprehensive manner the way that the DSA is" (Participant Two, March 27th, 2023).

Participant Two's observations highlight the challenges in passing comprehensive federal privacy laws due to political reasons, even when both partisans have reached a consensus on critical issues. P2 believes that smaller pieces of the DSA may end up as parts of standalone bills, but the effectiveness of such an approach is uncertain. Co-regulatory mechanisms of the

DSA, such as codes of conduct, assessments, and audits, could potentially be more appealing to US policymakers. “These mechanisms do not put the government in the driver's seat, making them more likely to withstand First Amendment conversations and align with the US perspective on entrepreneurship and the free market” (Participant Two, March 27th, 2023).

Participant Two emphasized the importance of learning from the EU’s approach and building upon its success and failures. He suggested that the US focus on privacy by passing a bill like the ADPPA and then pivot to promoting platform accountability and addressing secondary issues with a cohesive system. (Participant Two, March 27th, 2023).

Works like the Blueprint for the AI Bill of Rights are described by P2 as significant conversation starters, even if they may not be immediately translated into legislation (Participant Two, March 27th, 2023). He recognizes the value of such efforts in guiding discussions and getting stakeholders on the same page, ultimately serving as a “North Star” or trailblazer for future policy development (Participant Two, March 27th, 2023).

P2 explained that the DSA would most immediately influence organizations that include VLOPs and CLOSEs. They must comply with EU regulations because they may lead them to implement similar changes for all their products. (Participant Two, March 27th, 2023).

Civil society will benefit from some of the DSA’s articles, particularly those related to researcher access to data and assessments that involve stakeholders. There are also several provisions on voluntary novel governance mechanisms like codes of conduct. P2 was positive in their statement that “it will have a significant impact because whatever companies have to do to satisfy the regulators in the EU, they will basically have to do for all their products. That will fundamentally mean that they will change their tune based on what they must do for the EU" (Participant Two, March 27th, 2023).

The conversation with Participant Two suggests that while elements of the EU’s DSA may be incompatible with the US system, there are still opportunities for the US to learn from the EU’s approach and adapt it to its own context. By focusing on privacy and platform accountability within a cohesive framework, the US may be able to increase its efficiency in developing digital governance policies.

Participant Three (P3)

Participant Three (P3) is an expert in information policy law with research interests in areas such as algorithmic governance, platform policies, and transparency policies. P3 co-founded and currently co-directs an institute on information policy and law at a distinguished law school. P3 is a Senior Fellow at the Digital Innovation & Democracy Institute at the German Marshall Fund and Knight Foundation grantee, where they work at innovative approaches to

platform regulation and transparency. P3 has also served as an expert before the National Academies of Science and Technology and the Federal Communications Commission.

P3 stated that unless US stakeholders have been following digital governance in the EU closely, they are mostly unaware of the Digital Services Act. However, it would only be a matter of time before the DSA became part of the collective discussion among US policymakers, thanks to the "Brussels Effect" (Participant Three, March 24th, 2023). The term refers to the common observation that European regulation's extraterritorial effects, like the GDPR, change the digital landscape even though it does not directly apply to the United States.

Participant Three expects a similar effect to play out with the DSA, but some United States stakeholders think they should take their own approach. P3 noted that the US is focusing more on child safety, stating, "It's really interesting; we have focused very much on the safety of kids, so there is a lot of state law that's happening" (Participant Three, March 24th, 2023). The state laws were in reference to Utah's governor recently signing off a bill meant to curb children's social media use with identification requirements or parental permission.

The Utah state legislation is a step toward more digital policy. Still, the bill is not exactly clear on how large platforms should comply, and critics of the bill argue that it is an invasion of data privacy for social media users. The DSA is similar in its intention to regulate social media with its ban on targeted ads, especially for children.

Although parallels can be drawn between the DSA and recent state laws, Participant Three pointed out that there is potential friction. From the American perspective, a ban on target ads for adults could potentially be a first amendment violation (Participant Three, March 24th, 2023). Another perspective on the DSA is that there may be a difference in the American sense or definition of trade secrets, which US stakeholders would most likely want more safeguards around (Participant Three, March 24th, 2023).

Large platforms, like social media companies in the US, will be required to follow the DSA's obligations when operating in the EU's single market. "So, for the very large platforms, there is definitely going to be an impact. They are going to have to do risk assessments. They're going to have to be transparent. They're going to have to have access for researchers" (Participant Three, March 24th, 2023).

Defining access, protocols, and privacy protection for users could be a challenge when it comes to researcher access to data. P3 made the observation, "So you're going to have anonymized data where researchers can trace the flow of information from and to people without knowing who those people are, without being able to reconstruct who those people are. But I may need to know the characteristics of those people, right? If you're looking for bias, you may

need to know the characteristics. For a kid's protection, you need to know their age" (Participant Three, March 24th, 2023).

Participant Three does not limit the nuances of complying with data transparency and access to US Stakeholders, predicting that it will also be an issue in Europe. "It's going to be hard, I think, to define what access means, what the protocols are, and how you protect the privacy of users" (Participant Three, March 24th, 2023).

P3 reflects, "And so I think it's going to be quite interesting. It all can be done, but I am sure there will be disputes about [platforms] not giving us enough, and platforms will respond with 'We can't give it to you'" (Participant Three, March 24th, 2023).

P3 pointed out parallel action in Congress, where politicians have been willing to work together when it comes to AI regulation. These efforts could include more general requirements. "We're actually moving on to AI regulation. I think there's a lot of bipartisan support for having requirements around research access, transparency, data" (Participant Three, March 24th, 2023).

The interview with Participant Three conjured up images of America's auto industry as a way to explain the sensibilities and points of view of US stakeholders. As described by P3, the digital systems we are regulating are opaque and have a huge outside influence on individuals, communities, and society in general (Participant Three, March 24th, 2023).

Those in Congress working on digital governance "don't actually know what's under the hood, and the DSA opens up that hood somewhat and lets people in" (Participant Three, March 24th, 2023). US stakeholders, including the general public, "Want to understand the machinery of their lives, and they want to know how even if they can't fix them, they want to know how they work. And this is a huge, essential machinery of our lives, and we have no idea how it works other than we know it's engagement-driven" (Participant Three, March 24th, 2023).

It is clear that the US will be influenced by the bill; however, defining research access, data privacy, and transparency is perceived to be an immediate challenge. As the United States continues to work on its own forms of digital governance, it may find it beneficial to consider how the DSA's framework "opens up the hood" on digital regulations.

Discussion

Perception of the DSA by American Stakeholders

The perception of the Digital Services Act among American stakeholders, as evidenced by the diverse findings of the expert interviews, is a mix of optimism, caution, and uncertainty. While all three experts recognize the potential impact of the DSA on large platforms and the

need for better digital governance, they also acknowledge the inherent complexities and challenges involved in implementing the legislation in the United States.

In the context of Zittrain's three eras of digital governance, the DSA can be seen as an attempt to address the challenges of the legitimacy era by creating a more inclusive and deliberative process for regulating digital services. This includes learning from the successes and failures of previous legislation, such as the European Union's General Data Protection Regulation (GDPR) and Germany's NetzDG law.

Participant One (P1) held optimism towards the DSA, tempered by an awareness of the "wait and see attitude" of US stakeholders and the potential reluctance of American organizations to comply with the policy. P1 highlights the importance of European Commission pressure to elicit a response from US policymakers and the necessity for effective enforcement measures to ensure compliance. P1 also acknowledges the potential burden of the DSA on platforms like Twitter, which may struggle with content moderation and, in turn, carry resentment toward the new obligations.

A perceived benefit of the DSA came from Participant Two (P2) who commended its' development process and stakeholder engagement. P2 also expressed surprise that the EU did not make more drastic changes to the E-Commerce Directive. It was pointed out by all experts that US stakeholders are less concerned about the DSA compared to the GDPR, but anticipate a significant impact on VLOPs who will have to comply with and later design for the DSA's new obligations. P2 suggests that the US could learn from the EU's approach and adapt it to its own context by focusing on privacy, platform accountability, and the adoption of co-regulatory mechanisms like codes of conduct and assessments.

Professor Three (P3) offered a more cautious view on the DSA, noting that many US stakeholders may not be concerned with European policies and are more focused on specific issues like child safety. P3 expects the "Brussels Effect" to bring the DSA into the collective discussion among US policymakers. P3 highlights potential friction between the EU and US approaches to issues like targeted ads and trade secrets. There will likely be challenges in defining access, protocols, and privacy protection for users and researchers, suggesting that disputes may arise between platforms and regulators.

Perceptions of US stakeholders concerning the Digital Services Act (DSA) present a "wait and see" attitude that passively observes the EU setting global standards. The US has yet to create digital legislation like the DSA, that sets the bar for Big Tech, However, its federal government has expressed the perceived need for globalization and harmony in digital governance. Through this analysis of the DSA's ambitious rollout, legal experts in information law and digital policy highlight their perceptions of the DSA by outlining key challenges.

As Wheeler (2023) suggests, the US has taken a more passive stance compared to the EU and UK's proactive approach to digital regulation. This hands-off approach might result in a loss of trust and legitimacy in the digital sector, and as other nations establish global digital risk management standards, the US may struggle to participate in their development. Consequently, American platforms may find themselves in a future where others define the rules, and the US government is forced to adopt these standards after the fact.

The NASEM report (Columbia University, 2023) emphasizes the importance of understanding the broader implications of regulations. As the digital landscape becomes increasingly interconnected, early detection of trends and a commitment to harmonization in digital governance will be critical in fostering global cooperation and avoiding fragmentation along national lines. The report's stance that over-regulation may lead to mistrust in the government runs parallel to Wheeler's point that US stakeholders are cognizant of the need for digital governance in careful amounts. Their 'wait and see attitude' suggests that their perception of the DSA is that it is a working prototype for their future policies.

US stakeholders perceive the DSA as a trailblazer, with challenges and complexities that will need to be overcome and later analyzed before being adopted in the US. The panel discussion in "Session IV, Part 1: Regulating Online Speech: Between the First Amendment and the Digital Services Act" (Columbia University, 2023) highlights the difficulties in defining illegal content, potential abuses in fragile democracies, and questions surrounding the idea of "trusted flaggers" for decentralized content moderation. Opinions from legal experts on the DSA underscore the nuance of implementing DSA obligations while upholding the principles of freedom of expression and protecting individual privacy.

Given these challenges, US stakeholders need to engage in ongoing dialogue and collaboration with their international counterparts to promote transparency and access in the digital landscape. Although the DSA's implementation and enforcement will face obstacles, it offers an opportunity for international cooperation and learning, allowing US stakeholders to better understand how to shape their digital governance in a way that balances individual liberties and democratic values.

The DSA may "not hold the imagination" of US policymakers (Participant Two, 2023), but it is no doubt in the minds of US platforms that will have to comply with the new rules. As Participant One pointed out "Twitter has fired a lot of people" (2023) even though the EU Commission will obligate independent audits and the hiring of a Digital Services Coordinator, even though it recently dissolved its trust and safety board. Twitter's CEO Elon Musk has committed to meeting the new obligations regardless of the massive downsizing. These actions from VLOPs support the observation that US stakeholders perceive the DSA as an inevitable regulation that they will "wait out and see" rather than rush into preparation.

The US stakeholders' perception of the DSA underscores the need for a more proactive and collaborative approach to digital governance. By closely observing and learning from the experiences of the EU and UK, the US can better understand the challenges and opportunities that lie ahead in digital regulation. As the digital landscape continues to evolve, US stakeholders must prioritize harmonization, transparency, and international cooperation to prevent misguided regulation and retroactive changes to technologies from fostering a sense of mistrust towards the government.

The DSA's Influence on Digital Governance in the US

The Digital Services Act (DSA) has piqued the interest of policymakers and experts in both Brussels and Washington, D.C., due to its potential impact on digital governance. When evaluating the likelihood of the DSA influencing digital governance in the United States, the perspectives of three academic experts were considered, along with insights from a comprehensive literature review. Experts generally agreed that while adopting the DSA wholesale in the United States is unlikely, its influence on digital governance could still be significant.

Participant One (P1) underscored the importance of monitoring the DSA's progress in Europe, as US stakeholders will inevitably face the new obligations imposed on all intermediaries operating in the EU single market. The United States could adopt specific aspects of the DSA, especially those related to accountability and regulation, by drawing parallels between the DSA's new obligations and existing US regulatory structures. However, P1 warned against politicizing digital governance, which could hinder progress in this area.

Participant Two (P2) suggested that although the DSA may not resonate with most US users as the GDPR did, stakeholders in digital industries and groups overseeing the DSA's implementation are actively engaged in discussions. P2 recommended that the United States first focus on passing privacy legislation like the American Data Privacy and Protection Act (ADPPA) before tackling platform accountability and other secondary issues. P2 proposed that smaller, standalone bills incorporating elements of the DSA could be a viable approach, though their effectiveness remains uncertain.

In contrast, Participant Three (P3) takes a more cautious stance on the DSA's potential impact in the United States. P3 observed that US stakeholders may be unaware of the legislation and prefer to concentrate on specific digital governance issues such as researcher access, data privacy, and child safety. P3 warned of potential challenges such as defining access for researchers and privacy protection for users, suggesting disputes may arise between platforms and regulators. This friction may hinder the DSA's influence on American policymakers.

Despite its challenges, The Digital Services Act is likely to have a significant influence on digital governance in the United States. The DSA offers opportunities for effective digital governance through its co-regulatory mechanisms, which involve minimal government intervention and rely on stakeholder groups under government oversight (Morar, 2022). These mechanisms, including codes of conduct and audits, promote transparency and inclusivity, fostering a more balanced approach to digital governance that is compatible with American perspectives on entrepreneurship and free markets.

By adopting the DSA's co-regulatory mechanisms, the United States can create a balanced digital governance framework that respects First Amendment rights while encouraging innovative regulation. In this way, the United States can bridge the gap between the current development of the Blueprint for the AI Bill of Rights and the Declaration for the Future Internet with the initiatives to protect innovation, which has been a core tenet of American digital policy for the last three decades, regardless of the political party in charge.

However, implementing strategies similar to the DSA in the United States would face challenges, such as navigating a complex political landscape (IFL, 2022). During the interviews, Participant Two supported this notion with their expert opinion that "It would be [difficult] for something like [the DSA] to go through, A, unscathed, which is practically impossible, and B, in a big comprehensive manner the way that the DSA is" (2023). However, US digital policy will likely move forward with small digestible pieces of the DSA, such as risk management, codes of conduct, and audits.

Despite these challenges, the DSA's influence on US digital governance will be significant. The bill's co-regulatory mechanisms provide a more inclusive and transparent approach to digital governance, involving various stakeholders and maintaining government oversight (Morar, 2022). Big Tech has shown a willingness to build these mechanisms with public stakeholders as seen with the formation of the Digital Trust and Safety Partnership that Morar points to in the Literature Review (2022). To fully realize the potential benefits of the DSA, US policymakers should also consider the bill's process of inviting the government to observe the collaboration and aid in the drafting of co-regulatory mechanisms.

The panel discussion on misinformation underscores the need for a proactive and collaborative approach to digital governance in the United States, taking into account the complex interplay between political, structural, and ethical considerations (IFL, 2022). By engaging in informed discussions and collaborating with diverse experts, regulators, and industry stakeholders, the United States has an opportunity to develop and adopt legislation that takes on issues of digital governance in a way that reaches solutions by focusing on a process rather than a single issue (Morar, 2022).

Ultimately, the “Brussels effect” will have a significant influence on the US, and American policymakers will most likely move forward pieces of the DSA that can be adapted to fit American ideals like free speech and innovation, such as co-regulatory mechanisms. However, the benefits of the DSA’s “process over outcomes” will depend on the willingness of American policymakers and public stakeholders to collaborate and adopt its principles, as well as their ability to overcome the political challenge of passing such legislation in a country resistant to regulating digital innovation (IFL, 2022).

Conclusion

The Digital Services Act presents a complex mixture of optimism, caution, and uncertainty among American stakeholders, as evidenced by the diverse perspectives of expert interviews and literature. Although the DSA is unlikely to be adopted wholesale in the United States, it is poised to significantly influence digital governance, particularly through its co-regulatory mechanisms and focus on accountability, transparency, and access. Defining rights and standard practices under those three terms align with the purposes behind the digital policy whitepaper developed under the Biden administration. US stakeholders will need to navigate the challenges of adapting platforms to the DSA’s obligations without overstepping American values of free speech, innovation, and minimal government oversight.

As this study has demonstrated, the DSA offers valuable opportunities for the United States to develop a more balanced and effective digital governance framework. By closely monitoring the DSA's progress in Europe, learning from its implementation strategies, and considering the adoption of specific aspects of the legislation that align with American values and practices, the United States can contribute to a more harmonized and inclusive digital landscape. Doing so would maintain trust in the government and ensure that the influence of the DSA is positive.

Despite potential challenges and compatibility issues, the DSA's influence on US digital governance will likely be substantial, thanks to its inclusive and transparent co-regulatory mechanisms that will be placed on VLOPs and VLOSes who reach over from the US to operate in the EU internal market. To fully harness the potential benefits of the DSA, American policymakers, and stakeholders must engage in collaborative efforts to overcome the nation’s historical resistance to regulating digital innovation. In doing so, the United States can participate in the global leadership of digital governance.

References

Albert, J. (2023). *A guide to the Digital Services Act, the EU's new law to rein in Big Tech*. AlgorithmWatch. Retrieved March 2, 2023, from https://algorithmwatch.org/en/dsa-explained/

Associated Press. (2022, December 13). *Musk's Twitter has dissolved its Trust and Safety Council*. NPR. Retrieved March 11, 2023, from https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk

Baghdasaryan, M., & Gullo, K. (2021, November 23). *The UN Human Rights Committee criticizes Germany's NetzDG for letting social media platforms police online speech*. Electronic Frontier Foundation. Retrieved March 5, 2023, from https://www.eff.org/deeplinks/2021/11/un-human-rights-committee-criticizes-germanys-netzdg-letting-social-media

Barrett, C. (2020). Emerging Trends From the First Year of EU GDPR Enforcement. SciTech Lawyer, 16(3), 22-25, 35. https://www.proquest.com/docview/2369804193?parentSessionId=h%2F%2BIjURIjuGLsrWL07FaRtBBoS%2BP9G5ajUaLaAUlu30%3D

Beal-Cvetko, B. | P.- F. 15. (2023, February 15). *Utah Senate passes Social Media Regulation Bill without government ID verification requirement*. KSL. Retrieved March 112, 2023, from https://www.ksl.com/article/50580296/utah-senate-passes-social-media-regulation-bill-without-government-id-verification-requirement

Belanger, A. (2022, November 11). *Twitter quietly drops $8 paid verification; "tricking people not ok," Musk says*. Ars Technica. Retrieved March 5, 2023, from https://arstechnica.com/tech-policy/2022/11/twitter-quietly-drops-8-paid-verification-tricking-people-not-ok-musk-says/

Brookes, J. (2021, August 4). *Facebook blocks researchers from scrutinizing data*. InnovationAus.com. Retrieved November 28, 2022, from https://www.innovationaus.com/facebook-blocks-researchers-from-scrutinising-its-data/

Brookings Institution. (2022, December 5). *Unpacking the white house blueprint for an AI Bill of Rights*. YouTube. Retrieved January 24, 2023, from https://www.youtube.com/watch?v=1HnrDu54spg

Columbia SIPA. (2022). *Digital Services Act: What Can the US Learn from the EU?* Retrieved March 12, 2023, from https://www.youtube.com/watch?v=h-YZIMu2EMA

Columbia University. (2023, January 19). Regulating the Online Public Sphere: From Decentralized Networks to Public Regulation. Global Freedom of Expression. Retrieved February 20, 2023, from https://globalfreedomofexpression.columbia.edu/events/regulating-the-online-public-sphere-from-decentralized-networks-to-public-regulation/

Danziger, J. (2021). *EU Digital Services Act: Regulation or Over-Regulation?*. Computer Fraud & Security, 2021(2), 10-14.

Edelson, L., Graef, I., & Lancieri, F. (2023, March 20). *Access to data and algorithms: For an effective DMA and DSA implementation*. CERRE. Retrieved March 25, 2023, from https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsa-implementation/

European Commission. (2020). *Digital Services Act: Ensuring a Safe and Accountable Online Environment*. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Commission. (2022, April 23). *Digital Services Act: Commission Welcomes Political Agreement on Rules Ensuring a Safe and Accountable Online Environment*. European Commission. Retrieved November 20, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545

European Commission. (2022, November 21). *Questions and Answers: Digital Services Act**. Press Corner. Retrieved March 5, 2023, from https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348

European Commission. (2023, March 2). *Digital Services Act: Commission sets rules on supervisory fees for very large online platforms and very large online search engines*. Shaping Europe's digital future. Retrieved March 8, 2023, from https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-sets-rules-supervisory-fees-very-large-online-platforms-and-very

European Commission. (2023, February 1). *DSA: Guidance on the requirement to publish user numbers*. Shaping Europe's digital future. Retrieved February 28, 2023, from https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers

European Democracy Action Plan. (2020, December 3). Retrieved November 20, 2022, from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

European Union. (2020). Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 200/31/EC. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=EN

Gorwa, R., Binns, R., & Katzenbach C. (2020). *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*. Big Data & Society, 7(1), 1-15. Retrieved from https://journals.sagepub.com/doi/full/10.1177/2053951719897945

Harvey, S. (2022, December 16). *Who's Enforcing GDPR?* Kirkpatrick Price. Retrieved March 5, 2023, From https://kirkpatrickprice.com/blog/whos-enforcing-gdpr/

Information Future Labs. (2022). *Live discussion: Can regulation solve the problem of misinformation? YouTube*. Retrieved November 28, 2022, from https://www.youtube.com/watch?v=CkxtsAYIZtM

Jeong, S. (2019, July, 26). *Politicians Want to Change the Internet's Most Important Law: They Should Read It First*. The New York Times. Retrieved February 22, 2023, from https://www.nytimes.com/2019/07/26/opinion/section-230-political-neutrality.html

Kingsbury, K. (ed.). (2020, January 17). *Joe Biden Says Age Is Just a Number*. The New York Times. Retrieved February 12th, from https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html

Laidlaw, E. (2017). *A Framework For Identifying Internet Information Gatekeepers*. International Journal of Law and Informational Technology, 25(4), 278-302. https://doi.org/10.1093/ijlit/eax015

Lee, N. T., & Malamud, J. (2022, December 19). *Opportunities and Blind Spots in the White House's Blueprint for an AI Bill of Rights*. Brookings. Retrieved April 5, 2023, from https://www.brookings.edu/blog/techtank/2022/12/19/opportunities-and-blind-spots-in-the-white-houses-blueprint-for-an-ai-bill-of-rights/

Lorenz, T. (2022, May 18). *How the Biden Administration let right-wing attacks derail its disinformation efforts*. The Washington Post. Retrieved February 14, 2023, from https://www.washingtonpost.com/technology/2022/05/18/disinformation-board-dhs-nina-jankowicz/

McGrory, K., Bedi, N., & Clifford, D. R. (2020, September 3). *A futuristic data policing program is harassing Pasco County Families*. Pasco's sheriff created a futuristic program to stop crime before it happens. It monitors and harasses families. | Investigations | Tampa Bay Times. Retrieved February 15, 2023, from https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/

Modzelewska, A. (2020, October 14). *The Impact of the German Netzdg Law*. CEPS. Retrieved March 10, 2023, from https://www.ceps.eu/ceps-projects/the-impact-of-the-german-netzdg-law/

Morar, D. (2022, August 23). The Digital Services Act's Lesson for U.S. Policymakers: Co-Regulatory Mechanisms. Brookings. Retrieved January 15, 2023, from https://www.brookings.edu/blog/techtank/2022/08/23/the-digital-services-acts-lesson-for-u-s-policymakers-co-regulatory-mechanisms/

National Science Foundation. (2023, January 24). *National Science Foundation - Where Discoveries Begin*. National Science Foundation. Retrieved February 20, 2023, from https://www.nsf.gov/cise/national-ai.jsp

Proton Technologies AG. (2020). *General Data Protection Regulation (GDPR)*. Retrieved March 2, 2023, from https://gdpr.eu/tag/gdpr/

Rutgers. (2023). Ellen P. Goodman. Rutgers. Retrieved February 20, 2023, from https://law.rutgers.edu/directory/view/1020

Simonite, T. (2018, May 31). *Obama's US Digital Service Survives Trump–Quietly*. Wired. Retrieved April 26, 2023, from https://www.wired.com/story/obamas-us-digital-service-survives-trumpquietly/

Shefet, D. (2020). *The Right to be Forgotten*. SciTech Lawyer, 16(3), 26-29.

Syed, N. (2023, February 25). *Section 230 is a load-bearing wall-is it coming down? – the markup*. Section 230 Is a Load-Bearing Wall-Is It Coming Down? – The Markup. Retrieved March 10, 2023, from https://themarkup.org/hello-world/2023/02/25/section-230-is-a-load-bearing-wall-is-it-coming-down

Thierer, A., & Haaland, C. (2019, November 21). *The Clinton-Bush-Obama-Tump Innovation Vision*. Mercatus Center. Retrieved April 26, 2023, from https://www.mercatus.org/economic-insights/expert-commentary/clinton-bush-obama-trump-innovation-vision

The Knight Foundation. (2022). Research and Policy: Opportunities for a Shared Agenda. Vimeo. Retrieved January 24th, 2023, from https://vimeo.com/776430184?embedded=true&source=video_title&owner=430486

The White House. (2021). Executive Order on Promoting Competition in the American Economy. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/

The White House. (2022, January 22). Fact Sheet: Executive Order on Promoting Competition in the American Economy. The White House. Retrieved from March 5, 2023, from https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/

The White House. (2023, February 3). Fact Sheet: Chips and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. The White House. Retrieved April 3, 2023. from https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

The Office of Science and Technology Policy. (2022, October). Blueprint for an AI Bill of Rights. The White House. Retrieved March 20, 2023, from https://www.whitehouse.gov/ostp/ai-bill-of-rights/

U.S. Department of State. (2022, April 29). *Launch of the declaration for the future of the Internet - United States Department of State*. U.S. Department of State. Retrieved December 10, 2023, from https://www.state.gov/briefings-foreign-press-centers/launch-of-the-declaration-for-the-future-of-the-internet

U.S. Department of State. (2022, May 23). *Declaration for the Future of the Internet - United States Department of State*. U.S. Department of State. Retrieved December 10, 2023, from https://www.state.gov/declaration-for-the-future-of-the-internet

Vedova, H. (2023, February 3). *Children's Online Privacy Protection Rule ("COPPA")*. Federal Trade Commission. Retrieved March 5, 2023, from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Vedova, H. (2022, May 24). *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act*. Federal Trade

Commission. Retrieved March 5, 2023, from https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection

Volden, C. (2022). *Highlights from the New 116th Congress Legislative Effectiveness Scores*. Center for Effective Lawmaking. Retrieved April 2, 2023, from https://thelawmakers.org/legislative-effectiveness-scores/highlights-from-the-new-116th-congress-legislative-effectiveness-scores

Wakabayashi, D. (2018, June 28). *California passes sweeping law to protect online privacy*. The New York Times. Retrieved March 12, 2023, from https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html

Wheeler, T. (2023, March 8). The UK and EU Establish Positions as Regulatory First Movers While the US Watches. Brookings. Retrieved March 15th, 2023, from https://www.brookings.edu/blog/techtank/2023/03/08/the-uk-and-eu-establish-positions-as-regulatory-first-movers-while-the-us-watches/

WSJ. (2021, October 5). *Facebook's documents about Instagram and teens*. The Wall Street Journal. Retrieved November 28, 2022, from https://www.wsj.com/livecoverage/facebook-whistleblower-frances-haugen-senate-hearing/card/eFNjPrwIH4F7BALELWrZ

Zakrzewski, C., Nix, N., & Menn, J. (2022, December 13). *Twitter dissolves Trust and Safety Council*. The Washington Post. Retrieved March 11, 2023, from https://www.washingtonpost.com/technology/2022/12/12/musk-twitter-harass-yoel-roth/

Zittrain, J. L. (2019, October 2). Three Eras of Digital Governance. SSRN. Retrieved March 2, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3458435

Appendix

Research Interview Protocol

Data Management and Security Questionnaire

1. What was the nature of the data?

- Electronic audio recording of Zoom video conferences, and text documents transcribed by the primary investigator.

- Data did not contain protected health or sensitive information. It solely contained the personal identity (upon consent) for the sole purpose of citing the quotations and opinions of relevant experts. Participants were asked to give verbal consent to disclose their identity for data collection purposes.

- Identifiers were codified; the codification key remained on a separate drive. Only the primary researcher had access to the codification list and subsequent data.

- The data and its identifiers were stored on separate hard drives while research was conducted.

- Identifiers were delinked from data using a codified list to store their identity. The data was stored on an offline hard drive, and a codified list key was stored on a private Google Drive. Only the primary investigator could access data or the codified list key.

2. Where and how was data stored, and what were the security measures?

    - Zoom interviews were conducted on a campus computer in the Duderstadt Center, part of the U-M North Campus. The recordings were transferred to a separate hard drive and deleted from the campus computer. A code key identified participants in the UM Google Drive.

    - The hard drive was offline and protected by a password. Google Drive uses a password and 2-factor authentication. The Google doc was restricted.

    - Only the primary investigator, Nicholas Sidor, and the faculty advisor, Irene V. Pasquetto, had access to the Google Document and hard drive containing research data.

3. How was data transmitted or transported?

    - Transmission of data occurred when audio transfers of Zoom recordings and Google Doc notes were saved to a password-protected external hard drive. Once transferred, the files were immediately deleted from the student's account on the campus computer.

    - Hard copy files were transported immediately to the student's home office and stored behind a locked door.

- Files and data will be encrypted and saved on a password-protected external hard drive. The data will be transported immediately to a home office, where it will live behind a locked door until it is destroyed.

4. When and how were data or records be deleted?

    Data and records were stored in a locked home office indefinitely until the primary investigator deemed the study to be complete.

5. Were cloud-computing resources used?

    Yes, minimal cloud computing resources was used when audio was recorded over a Zoom meeting.

6. What was the resource, and what is the privacy policy for the resource?

    University of Michigan's Google Drive under the primary investigator account was used to store a participant code key and record interview notes that were immediately transferred to an external drive. The privacy policy for using UM's Google environment is to limit the amount of research data stored on it and to log in and out of the service using 2-factor authentication. For this study, only the participant code identifier was stored on UM's google drive, and all other data was stored on an external drive. When using this resource, the primary investigator logged in and out of the cloud service using DUO Mobile's 2-factor authentication.

7. Were online data collection services used?

    Online data collection services were not used. Data collection was in the form of Zoom recordings and typed notes.

- Research data in the form of Zoom recordings and typed notes were recorded on a campus computer. The computer used campus wifi and was logged into the primary investigator's student account.

- Data was transmitted from the desktop of the student's account to an external hard drive that was directly connected to the computer. The process was repeated onto a second backup hard drive that will remain with the original drive.

- Once the data was transferred to the secondary backup drive, the original downloads were deleted from the campus computers and student accounts.

- Each participant was asked for consent to share personally identifiable information limited to their name. This identification was codified during research and only referenced when writing the research paper. No third party viewed or consulted over this information. Only the primary investigator and the faculty advisor had access to data.

8. Were any datasets used?

   No data sets were used.

Consent Brief

CONSENT FORM
THE DIGITAL SERVICES ACT

HUM00228651

Principal Investigator: Nicholas Sidor, MSI, University of Michigan School of Information
Faculty Advisor: Irene V. Pasquetto, Ph.D., the University of Michigan School of Information

You are invited to participate in a research study about The Digital Services Act and its potential impact on the United States.

If you agree to be part of the research study, you will be asked to participate in a brief interview regarding your thoughts on the Digital Services Act.

The benefits of the research include providing your expert opinion on significant Internet governance issues.

Risks and discomforts are limited to answering questions about the DSA that you do not wish to answer. If this occurs, you may skip the question or end the interview.

There is no compensation involved in this interview.

Participating in this study is completely voluntary. Even if you decide to participate now, you may change your mind and stop anytime. You may choose not to answer a particular interview question and may stop the interview for any reason.

I will protect the confidentiality of your research records by storing your name and/or other identifiers separately from the research data.

Information collected in this project may be shared with other researchers. Still, we will not share any information that could identify you unless verbal permission is given during the interview process.

The sole purpose of disclosing your identity in the research paper is to cite expert opinion. It is not required, and your identity will be withheld if you wish.

If you have questions about this research study, please contact:

Nick Sidor (primary investigator - student)
nsidor@umich.edu

As part of their review, the University of Michigan Institutional Review Board Health Sciences and Behavioral Sciences has determined that this study is no more than minimal risk and exempt from on-going IRB oversight.

Interview Script

Study: The Digital Services Act
(HUM00228651)

Principle Investigator: Nicholas Sidor

Interview Questions

1. What was your initial reaction to the Digital Services Act (DSA)?
2. How do stakeholders in the U.S. perceive the DSA?
3. What sort of impact will the DSA have on stakeholders, such as American tech companies, and how do you expect them to respond?

4. How will the DSA influence digital governance in the U.S.?
5. Should the U.S. draft a bill similar to the DSA?
6. Do you think any specific parts of the DSA will inspire U.S. policy?
7. Are there any parts of the DSA that you consider incompatible with the DSA?
8. If you were to speak to Congress about the DSA, what is the major takeaway from the DSA that you would express?