PUBLIC KNOWLEDGE

BUILDING THE DIGITAL PLATFORM COMMISSION: HOW TO DESIGN A REGULATOR TO REIN IN BIG TECH

2025 | MARCH

HAROLD FELD
LISA MACPHERSON

Building the Digital Platform Commission: How To Design a Regulator To Rein in Big Tech

Harold Feld
Lisa Macpherson

Acknowledgements

This Report and its recommendations are the culmination of over a year of work encompassing multiple events. It would not have been possible without the contributions of many people. The authors would like to particularly acknowledge the following individuals and thank them for their work making this possible. **Shiva Stella,** for designing the rubric for the listening sessions, managing the listening session process to ensure quality and consistency, editing and compiling materials for the Public Knowledge Policy Konclave, and editing this final report. **Michele Ambadiang**, for managing the logistics for both the listening sessions and the conclave. **Charlotte Slaiman**, for assisting in running the listening sessions and assistance processing the responses from them. **Patrick Yurky**, for serving as Rapporteur for the conclave and authoring the report on the conclave that is attached as the Appendix. **And, of course, all of the participants in our listening sessions and the Public Knowledge Policy Konclave, who contributed their considerable experience, expertise, and ideas to develop these recommendations.**

Table of Contents

I. Executive Summary

Since Public Knowledge first articulated the idea of a dedicated, sector-specific regulator for digital platforms in 2019, there has been increasing focus on the risks as well as the benefits of digital technologies. Propelled by the introduction of ChatGPT in November of 2022, this focus now extends into artificial intelligence and the prospect of artificial general intelligence. In addition to literally hundreds of legislative proposals to address distinct risks of digital technology, by the end of 2024 there were at least two legislative proposals from policymakers designed to spark conversation and debate about the regulation of digital platforms via a dedicated agency or commission.

To contribute to and advance the concept of a sector-specific regulator for digital platforms, Public Knowledge has conducted two types of stakeholder convenings. First was a series of listening sessions – essentially focus groups – among likely advocates for more assertive platform regulation. These were conducted in the fall of 2023 to explore the terrain and determine what types of questions would best spur dialogue about the potential structure, roles, and authorities of a digital regulator. Then in July 2024, Public Knowledge conducted its first-ever "PK Policy Konclave," focused on this topic. The conclave, titled "Building the Digital Regulator," brought together 25 subject matter experts from law, technology, policy, and academia to explore the need for a specialized digital regulatory agency in the United States. Discussions focused on identifying key regulatory challenges and developing frameworks and strategies for establishing and empowering such an agency.

After these consultations and other research (including review of early outcomes associated with new digital regulatory regimes in the European Union, United Kingdom, and elsewhere), **Public Knowledge concludes that it still supports creation of a sector-specific regulator for digital platforms with comprehensive jurisdiction over the sector and sufficient authority to adopt regulations that enhance competition and protect consumers.** However, its recommendations for such an agency's roles and authorities have evolved to factor in changes to administrative law. These recommendations and the rationale for them are contained in this report.

Public Knowledge recommends that a new Digital Platform Commission (DPC) be structured as an independent commission similar to the Federal Communications Commission, and that the DPC have broad powers in regard to competition, consumer protection, and research. The new agency would complement, and coordinate with, agencies with existing powers to address anti-consumer and anticompetitive conduct. Its role in research – both research it initiates on its own and the privacy-protected access to data it ensures for others – can help the agency develop expertise and set standards and best practices. The Digital Platform Commission must also have the power to impose effective remedies, monitor compliance, and enforce effective compliance. We also recommend that Congress permit the DPC to bring actions in court rather than require it

to use the Department of Justice as its litigator. Risk assessment and mitigation frameworks like those in the EU should be one tool – not the only tool – the DPC may adopt to regulate digital platforms. Lastly, we believe the relationship between digital platforms generally and evolving uses of powerful artificial intelligence tools appears sufficiently symbiotic that Public Knowledge recommends putting *both* under the authority of the same agency.

II. Introduction

Public Knowledge, in partnership with the Roosevelt Institute, initially brought forward the concept of a dedicated regulator for digital platforms in a book, "The Case for the Digital Platform Act," in May of 2019[1]. It was motivated by a recognition that since their creation in the late 20th century, digital platforms had come to play a central role in the global economy as well as in our everyday lives. The book's author, Public Knowledge Senior Vice President Harold Feld, took care to highlight how platforms had brought "many societal benefits and new opportunities for free expression and innovation." But he also pointed out what were already significant concerns about the impact of a handful of huge, largely unregulated digital platforms on privacy, free expression, innovation, personal and societal well being, and democracy. The purpose of the book was to unify what were already ongoing debates about the role of the platforms in respect to competition, content moderation, consumer protection, and public safety into an actionable whole. A subsequent report from the Shorenstein Center at the Harvard Kennedy School[2] also advocated for a "Digital Platform Agency" to promote competition and enforce a digital duty of care. In the years since, other academics and think tanks have created their own proposals for a sector-specific regulator.

Since Public Knowledge published this book, these debates have only increased in volume. Thanks to the work of journalists, researchers, academics, plaintiffs, and whistleblowers, we have more collective insight (although maybe not as much as we should) on the platforms' risks and impacts. We also have a pages-long ledger of attempts from both sides of the Congressional aisle to regulate them – with almost nothing to show for it. That is not for lack of effort. In fact, there have been at least two substantive efforts brought forward by earnest policymakers to define a digital regulatory entity that bears a resemblance to the one Harold Feld imagined. In 2022, U.S. Senators Michael Bennet and Peter Welch introduced the Digital Platform

[1] Harold Feld, *The Case for the Digital Platform Act* (Public Knowledge and Roosevelt Institute, 2019)
[2] Tom Wheeler, Phil Verveer, and Gene Kimmelman, "New Digital Realities; New Oversight Solutions in the U.S.: The Case for a Digital Platform Agency and a New Approach to Regulatory Oversight", The Shorenstein Center on Media, Politics and Public Policy (2020), https://shorensteincenter.org/new-digital-realities-tom-wheeler-phil-verveer-gene-kimmelman/

Commission Act[3], first-of-its-kind legislation to create an expert federal agency able to regulate digital platforms in the areas of consumer protection and competition. In 2023, Senators Elizabeth Warren and Lindsay Graham introduced the Digital Consumer Protection Commission Act[4], which would establish a new commission to regulate online platforms, promote competition, protect privacy, protect consumers, and strengthen national security. But so far, neither of these proposals have gotten across the legislative finish line.

To compound the ongoing legislative challenge, there have been significant changes in the legal context related to the creation of a new regulatory agency. The first is the Supreme Court decision in the case of *Loper Bright Enterprises v. Raimondo.*[5] In their June 2024 decision, the Court essentially overturned the long-standing "*Chevron* deference" doctrine, meaning that federal courts are now *required* to exercise their own independent judgment when interpreting statutes. That is, they can no longer "defer" to a regulator agency's interpretation, even if the relevant statute is ambiguous, the agency is expert, and their interpretation is reasonable. Additionally, even when the language of a statute is clear and unambiguous, a reviewing court may decide that the matter has such "economic and political significance" that the reviewing court should "hesitate" before concluding that Congress intended to delegate the agency the power to adopt the relevant regulations.[6] This is especially true when an agency seeks to apply an old statute to new circumstances, or apply an old statute in a different way. These two cases represent only the latest in a long trend of increasing hostility by the federal judiciary to agency regulation.

Critics argue that this represents a deliberate effort by unelected judges to arrogate power to the judiciary and undermine the ability of regulatory agencies to carry out their responsibilities.[7] Supporters maintain this is a long overdue corrective to the power of the administrative state.[8] In either case, these changes in administrative law have enormous implications for the design and feasible authorities of a new regulatory agency. At the same time, however, they make it harder for existing agencies to apply existing laws to digital platforms. As discussed below, as a result of these changes in administrative law, creating a new agency operating under a new statute – difficult as it is – is better than either trying to extend an existing statute to cover the current gaps in the law or expanding the authority of an existing agency.

---

[3] United States, Congress, Senate, Digital Platform Commission Act of 2023, S. 1671, 118th Cong., 1st sess., introduced May 18, 2023. https://www.congress.gov/bill/118th-congress/senate-bill/1671
[4] United States, Congress, Senate, Digital Consumer Protection Commission Act of 2023, S. 2597, 118th Cong., 1st sess., introduced July 27, 2023. https://www.congress.gov/bill/118th-congress/senate-bill/2597
[5] Loper Bright Enterprises v. Raimondo, 603 U.S. 369 (2024).
[6] Known as the "Major Question Doctrine" (MQD), *see West Virginia v. Environmental Protection Agency*, 597 U.S. 697 (2022).
[7] *See, e.g.,* Mark A. Lemely, "The Imperial Supreme Court," 136 Harv. L. Rev. F. 97 (2022).
[8] *See, e.g.,,* Eric R. Bolonder, "Fighting for Justice: The Legal and Moral Case for *Loper Bright*,"19 Liberty U. L. Rev. 357 (2024).

III. Stakeholder Consultation for a Digital Regulator

The recommendations contained in this report are the product of a two-stage stakeholder consultation process. Public Knowledge conducted a series of listening sessions, then used the findings to design an in-person "Public Knowledge Policy Konclave" focused on building the digital regulator.

A. Listening Sessions

In the fall of 2023, Public Knowledge hosted a series of listening sessions designed to both raise awareness of the need for a digital regulator and help inform the debate about its potential form and role. It was understood that the listening sessions were primarily designed to surface ideas and themes that would be used to construct a future convening to explore the themes in more depth. Listening sessions were composed of four different civil society constituencies that had been most active in the debate surrounding regulation of digital platforms. These include (a) antitrust advocates; (b) civil rights advocates; (c) consumer protection advocates; and (d) free expression advocates. The listening sessions were designed to be both similar and repeatable. All participants received a fact sheet in advance so they would have the same baseline knowledge of the concept and the assignment. All participants were promised anonymity and assured that Public Knowledge would present their feedback at only a high level in any report-out of the session. The sessions were conducted using a consistent introduction and set of opening questions, followed by a set of questions unique to their expertise (civil rights, consumer protection, and so on).

There were some consistent themes across groups. For example, the risk of regulatory capture was a chief concern in nearly every group. Participants questioned how a digital regulator – which relies heavily on talent with technical expertise and an understanding of how the internet functions – could be designed to prevent industry from capturing it. Participants indicated that this implies careful consideration of everything from staff salaries to how the digital regulator could be funded (appropriations, for instance). Another common concern was about the delicate interplay between a federal digital regulator and the states and whether more rigorous regulatory regimes (for example, in California) should be preempted. Some participants across groups also shared concerns about designing the digital regulator in such a way that it survives "in the courts" and can withstand a Supreme Court review without its actions being immediately dismissed. This concern would obviously be amplified by recent Supreme Court decisions.

Some participants across groups pushed for a more holistic view of the internet and for inclusion of the layers of the digital technology stack that are less visible or less topical. They argued that for a digital regulator to be effective, it must take the total view of tech and not just restrict itself to the Big Tech platforms – the brand names everyone knows. Some participants across groups

also shared concerns about designing the digital regulator so that it behaves in ways complementary to the Federal Trade Commission, Federal Communications Commission, and other agencies that touch on these same or similar issues. Would it cannibalize these complementary agencies or compete with them?

Some participants across groups expressed concerns over the massive growth in artificial intelligence and questioned if and how a digital regulator would oversee this new sector. (This became an area of particular dissension in the Policy Konclave.) There were also questions (prescient ones, it turns out) about whether the time and political environment were "right" for the creation of a new regulator from scratch. Participants wondered if smaller wins or a set of regulatory "tools" could address the problems of digital platforms with less political effort or capital.

There were also distinct themes surfaced in each of the listening sessions based on the specific expertise of the participants. For example, participants in the session focused on competition and antitrust were highly protective of the then-leadership of the FTC and its role as both an antitrust enforcer and regulator in this space. Participants in this group were most likely to recommend augmenting the FTC's authority rather than creating a new, sector-specific regulator. Conversely, participants in the group focused on consumer protection strongly endorsed the concept of a new federal regulator but expressed strong concerns about state preemption, citing progress in California and the desire of industry to develop federal laws expressly to preempt strong state action. The participants in the session focused on free expression were most suspicious of creating a new agency – or even new federal authorities – especially with regard to social media platforms. They expressed the concern that regulation that does not *explicitly* pertain to speech regulation could still be used to regulate speech. This group preferred different models of regulation that focused on standards, access to data, and research. The group of participants focused on civil rights were the most concerned of all the groups with how slow and deliberate setting up a new digital regulator would be; they also called for more transparency and warned that this new agency should be held accountable to the public. Finally, they were the group most interested in how a digital regulator could establish and maintain trust in a social environment where no one trusts anyone (or any institution or media source) anymore. Unfortunately, if anything, trust in democratic institutions has declined since the listening sessions were conducted.

Both the general themes and those specific to the various listening sessions were used to construct the participant list and discussion topics for the Public Knowledge Policy Konclave.

B. Public Knowledge Policy Konclave ("PKPK")

The Public Knowledge Policy Konclave "Building the Digital Regulator" was convened from July 14 through July 16, 2024. Prior to the event, participants were provided with a reading list to ensure a baseline understanding of the concept of a regulator and analysis and writing to date on the topics. To encourage open dialogue, participants were told the conclave would operate under a modified Chatham House rule (participants were free to use the information received, but neither the identity nor the affiliation of the speaker may be revealed). Participants attended in their individual capacities, contributing diverse perspectives aimed at advancing the discussion on digital regulation. The goal was to foster robust dialogue and generate concrete policy recommendations to guide the creation of an effective digital regulator in the United States.

The first full day of the conclave began with guided discussions led by participant subject matter experts, covering essential topics to understand the context for a digital regulator. Each discussion began with a brief introduction to the subject matter; these were designed to bring all participants to some baseline level of knowledge. These discussions provided the background information on critical issues and challenges that will inform the design of a digital regulator's structure and function. The topics and key conclusions of each discussion are highlighted here.[9]

a. Context for Designing the Digital Regulator

i. Digital Platform Regulation in Europe and the U.K.

This session examined the regulatory frameworks and approaches to digital technology in the EU and the U.K., focusing on the creation of specialized digital regulatory agencies. Participants discussed the Digital Services Act (DSA), the U.K. Online Safety Act (OSA), the AI Act, and the Digital Markets Act (DMA).

The key implications from these frameworks that may inform the creation of a specialized digital regulator for the United States were:

- The DSA emphasizes proactive regulation, requiring platforms to conduct risk assessments and audits *before* issues arise.
- The U.K.'s approach with the OSA relies on existing regulatory structures and emphasizes cooperation among agencies rather than creating new bodies.
- The AI Act categorizes risks and includes specific procedural requirements, but its decentralized enforcement model may pose challenges.
- The DMA is more focused and legally specific, with clear goals related to competition and fairness.
- Participants emphasized the need for ongoing evaluation of these regulatory frameworks to ensure they remain effective and avoid unintended consequences.

[9] The complete report from the Policy Konclave, including the list of participants, is attached as an Appendix.

ii. The Current Landscape in Congress

This session explored the political landscape in place in mid-2024 and its impact on technology regulation. Participants discussed the legislative environment, the influence of political dynamics, and the challenges associated with advancing technology-related legislation, including AI policy, privacy, and competition. The conversation also touched on the potential impact of the judicial decisions noted above.

The key themes of this session (some of which have been amplified since mid-2024) were as follows:

- The influence of political considerations, including the filibuster and the fragmented committee system, presents substantial challenges to the progress of technology-related legislation.
- Participants identified significant complexities in creating a new regulatory agency or empowering existing ones, particularly in a post-*Chevron* world.
- Participants emphasized the need for substantive, educational hearings to prepare Congress for the challenges of technology regulation, drawing on lessons from past legislative efforts, such as telecommunications.
- They stressed the importance of restoring independent, technologically aware analysis within Congress, along with comprehensive oversight mechanisms in regulating technology.

iii. The State of Artificial Intelligence Regulation

This session explored the state of AI regulation, focusing on various approaches in the U.S. and internationally. The discussion centered on categorizing regulatory efforts and defining the scope of regulation. Participants examined existing laws, new legislative initiatives, and soft-power efforts, discussing their implications for AI governance. The conversation also touched on AI's intersection with intellectual property (IP) issues, competition, and the potential role of a specialized digital regulator. Lastly, the session foreshadowed the differing views on the role of a dedicated digital regulator with respect to AI that would arise the following day.

The key themes from the discussion in this section were:

- There was a consensus on the need for a clearer problem definition: What problems is AI regulation intended to solve? Clarity is critical in defining the scope and authority of any potential AI regulatory agency.

- It is important to consider the secondary impacts of AI, rather than focusing solely on the technology itself.
- There is an ongoing debate over whether or how to integrate IP concerns into the broader framework of AI regulation.
- Given the role of training data in shaping AI behavior and its potential societal impacts, this is an important concern for regulation.
- The pervasive nature of AI across various sectors complicates the creation of a sector-specific regulator.

iv. Inter-Agency Cooperation in the Federal Government

This session focused on the dynamics of cooperation among U.S. government agencies (in which some of the participants had previously or currently worked), particularly regarding overlapping regulatory jurisdictions. The discussion aimed to provide insights into the challenges and benefits of interagency coordination. Participants explored different models of agency collaboration, identified obstacles to effective cooperation, and debated how a new, dedicated digital regulator could fit into the existing regulatory landscape.

The key themes from this session that inform our recommendations are:

- Participants acknowledged significant difficulties in inter-agency coordination.
- Participants emphasized that agencies must develop and maintain technical expertise, crucial for effective regulation, particularly in the rapidly evolving digital space. They raised concerns about the technical deficit within government agencies and how a new regulator could ensure it has the necessary expertise to handle complex digital issues.
- As in the listening sessions, participants in this session of the conclave highlighted regulatory capture as a significant risk. They noted that overlapping jurisdictions can sometimes serve as a safeguard against capture by ensuring multiple perspectives in enforcement actions.

v. Impact of Recent Supreme Court Cases

This session examined the implications of recent Supreme Court decisions for the structure and authority of regulatory agencies in the United States. In addition to the *Loper Bright* case noted above, the participants placed a particular focus on *Seila Law LLC v. Consumer Financial Protection Bureau*,[10] and *SEC v. Jarkesy*.[11] The group analyzed these cases to understand their potential impact on the creation and operation of independent agencies, the scope of agency authority, and the future of regulatory enforcement. The discussion primarily centered on

[10] Seila Law LLC v. Consumer Financial Protection Bureau, 591 U.S. 197 (2020).
[11] Securities and Exchange Commission v. Jarkesy et al., 609 U.S. 109 (2024).

Loper-Bright Enterprises v. Raimondo, as participants raised concerns that the overruling of the Chevron Doctrine and the subsequent weakening of agency authority might compel Congress to be more explicit in granting authority to agencies.

The key themes of this conversation that are reflected in our recommendations are:

- As the Supreme Court becomes more restrictive in interpreting agency authority, the need will grow for Congress to be very clear and specific in the language used to grant regulatory powers. It was also agreed that pragmatically, the breadth of powers of a new federal agency would probably not be able to exceed those of any current agency.
- The potential for federal regulatory actions to preempt state laws is a significant concern, with some participants arguing for the importance of leaving room for state-level regulation in certain areas.
- Participants highlighted the idea of using private rights of action to ensure compliance with regulations as a potential solution to the challenges posed by limited agency resources and the increasing complexity of regulatory environments. They suggested that this approach, possibly undertaken by state attorneys general, could offer an alternative to traditional regulatory enforcement, protecting against the susceptibility of agency action to challenges.

On the second day of the Policy Konclave, participants were divided into four working groups to address specific aspects of creating a dedicated digital regulator, building from the context provided on the first day. Each group prepared and presented its recommendations, which were then discussed and refined by the full group of participants. The topics and areas of the greatest consensus and disagreement in the full-group discussions are recapped here.

a. PKPK Recommendations for Building the Digital Regulator

i. Access to Research

This breakout session focused on recommendations regarding how a digital regulator should manage research and access to research data. Participants discussed how to grant researchers access to data while maintaining confidentiality and privacy protections, structuring research within the regulatory framework, and addressing liability and data misuse challenges. They focused on key issues like defining researcher qualifications, balancing data access with privacy concerns, and addressing First Amendment issues related to data use. The session aimed to provide recommendations on structuring data access to support effective research while maintaining safeguards.

In the ensuing full-group discussion, participants generally agreed on the importance of establishing clear confidentiality and privacy protections and the need for an advisory committee to guide the research agenda. They also supported embedding regulators within companies and creating a standard-setting process for application programming interfaces, or APIs. However, they disagreed over the scope of research access, liability issues, and the relevance of research to the agency's goals. Some participants felt the research framework the breakout group had proposed was too broad and could lead to unnecessary exposure of company data, while others argued for a more flexible approach allowing a wide range of research activities.

ii. Rules, Responsibilities, and Risk Assessments

This breakout session examined how a digital regulator should develop its regulatory framework, particularly regarding risk assessments, rulemaking, and liability standards. The primary focus was ultimately on the function and form of risk assessments, though the group also considered broader regulatory questions such as rulemaking, common law duties for regulated entities, and appropriate policy areas for a digital regulator. The session aimed to evaluate different models for these areas and provide recommendations for structuring the agency’s approach.

In the subsequent full-group discussion, participants generally agreed on the importance of clear standards for risk assessments and the need for external audits to ensure compliance and proper implementation. They also agreed on the necessity of involving third parties, although they debated the specifics of their role. The group concurred that the digital regulator should have the flexibility to adapt risk assessment requirements based on the specific policy areas it oversees, which would help address both systemic risks and product-specific issues effectively. However, participants disagreed substantially regarding the scope of obligation for conducting risk assessments and the extent to which individual companies should assess systemic risks versus relying on external auditors. They also expressed differing opinions on the appropriate timing of risk assessments and the integration of human rights considerations.

iii. Structure of the Agency

This breakout session focused on the proposed structure of a digital regulatory agency in the United States. The working group debated the merits of different models, including independent versus executive agencies, and considered the agency's potential scope of authority. The discussion also covered how the agency would coordinate with existing entities, especially if it were to function as an expertise-based agency rather than one with exclusive jurisdiction. The group also examined the legal and political constraints that would shape the creation of such an agency, particularly in light of recent Supreme Court decisions.

When the group convened as a whole, there was general agreement about the need for the new agency to have rulemaking and enforcement authority, along with the ability to conduct deep market research. However, there was disagreement about whether the agency should be independent or executive, with some emphasizing the importance of independence for issues like content moderation. Participants also debated whether privacy regulation should fall within the new agency's mandate. Some argued that privacy should be handled separately to avoid conflicts with competition enforcement, while others felt that combining these areas might be a political necessity. The session concluded with participants acknowledging that while the structure of the agency is important, the focus should be on its goals, operations, and powers.

iv. Artificial Intelligence

The final working group explored the potential role of a digital regulator in overseeing AI technologies. They examined AI as both a platform and a product, addressing regulatory challenges, accountability, and the scope of a digital regulator's authority. The group debated whether AI should be a central responsibility of the new agency or if it falls outside the scope of a digital regulator. Participants discussed how AI might be integrated into the agency's remit, distinctions between AI as a platform versus AI used within platforms, and the applicability of existing laws to AI.

The subsequent full-group session included some of the liveliest conversation of the Policy Konclave. The group generally agreed that while AI regulation is necessary, a digital regulator should not be the sole or primary agency responsible for AI oversight. Instead, they suggested that an expert body with specialized knowledge could play a consultative role to assist other agencies in regulating AI within their specific domains. Participants reached a consensus on the need for clear definitions and standards in AI regulation, particularly in distinguishing between AI platforms and products. However, they disagreed on how to approach the regulation of AI models versus products. Some argued for a centralized AI regulator, while others believed existing agencies could adapt to these new challenges. The debate on civil rights and discrimination in AI also revealed significant divisions, particularly regarding the practicality of enforcing existing laws in the context of AI technologies. The session concluded without a clear resolution on several key issues, such as the best approach to regulating AI models and the appropriate scope of a digital regulator's authority.

IV. Recommendations

Taking the results of our ongoing discussions with stakeholders and experts, the various forms of regulation implemented abroad, and continued efforts to address the competition and consumer protection problems raised by digital platforms in the United States, Public Knowledge continues to support the creation of a sector-specific regulator for digital platforms. As discussed below,

Public Knowledge continues to believe that this sector-specific regulator should have comprehensive jurisdiction over the sector, and should have sufficient authority to adopt regulations that enhance competition and protect consumers.[12] Public Knowledge believes that despite the challenges presented by recent changes in administrative law, Congress can still create a comprehensive regulator with sufficient authority to ensure that digital platforms serve the public interest as well as the private interests of their shareholders. Ironically, the changes in administrative law which make it more difficult to create a new regulator create such significant barriers to applying existing law or expanding existing agencies that starting from scratch with a new law and a new agency is actually the path of least resistance and greatest likelihood of success (which is not to suggest that it will be easy to do).

Public Knowledge does have some changes to recommend from the initial skeletal outline of the Digital Platform Commission proposed in 2019. The importance of an agency that serves as a center of expertise emerged as an increasingly important theme to counterbalance the current lack of such expertise at either the agency level or in Congress. So did the role of the agency in collecting data and facilitating research, while recognizing that the agency must protect confidential information and ensure that access is not granted for unfair or unethical purposes under the guise of research. Discussion suggests that different types of agency structures, such as standard setting and research agencies (like the National Institute of Standards and Technology) or those more dependent on guidelines and voluntary recalls (such as the Consumer Product Safety Commission) may be worth exploring.

Finally, the issue of generative AI has emerged since 2019 as an issue of singular importance. Digital platforms are rushing to include generative AI in their products, and the proliferation of AI content is significantly impacting the operation of digital platforms. It is impossible in 2025 to ignore the question of generative AI when considering how to regulate the digital platform sector. But it is also impossible to make any recommendation with certainty given the rapid development of the technology and the relatively short time to debate how best to regulate AI in the public interest. Public Knowledge therefore recommends that, to the extent consensus exists for some sort of federal oversight of generative AI, it should be placed in the DPC.

A. The Continued Need for a New Sector-Specific Regulator

While all experts involved in our discussions agreed that digital platforms have in many ways improved our lives, they also agreed that the law as it exists today does not cover all the ways

[12] PKPK did not address the issue of content moderation, and we do not address it here. Public Knowledge has recently released a "Policy Primer for Free Expression and Content Moderation" (Lisa Macpherson and Morgan Willsman 2024).

that digital platforms impact our lives for the worse. This is particularly true in the realm of civil rights protection and consumer protection, where individuals have little ability to either avoid platforms or protect themselves. This situation is aggravated by the recent introduction by the Supreme Court of the Major Question Doctrine[13] and repeal of *Chevron* deference to agencies as a result of *Loper Bright*.[14] Previously, agencies like the Federal Trade Commission operating under broad, general authority could argue successfully that new forms of discrimination or anti-consumer conduct fell within their broad scope – precisely because they impacted so many people who would otherwise be left defenseless. But *Loper Bright* removes any obligation of a reviewing court to defer to the agency's analysis as to its jurisdiction or overall authority. More importantly, MQD now suggests that courts should reject – or at least, view with suspicion – new claims of authority governing matters of "economic and political significance." But asserting jurisdiction over new behavior by digital platforms, or even over digital platforms themselves, requires agencies to interpret their statutes in new ways – in effect creating a potential MQD challenge to *any* action by an existing agency using its general statutory authority.

This is not to say that every agency attempting to apply an existing statute of general applicability will fail. But in an area already rife with confusion and "gaps," recent Supreme Court decisions have made enforcement efforts by agencies much more difficult. That in some cases several different agencies may arguably have jurisdiction makes the matter more confusing. In such cases where an agency seeks to act, digital platforms trying to avoid regulation can argue that Congress intended a different agency to address the problematic conduct.

Even where courts have acknowledged jurisdiction, such as in the field of antitrust, it takes years of litigation before even reaching a verdict. Assuming a successful prosecution, implementing and overseeing remedies to prevent a monopoly from simply continuing its monopolistic practices has proven extremely difficult.[15] While no breakups have yet occurred, antitrust scholars have wondered aloud how generalist judges and antitrust litigators could handle the complicated disentanglement of digital platforms such as Google.[16] Finally, antitrust does *not*

---

[13] West Virginia v. EPA supra note 6.
[14] Loper Bright Enterprises v. Raimondo supra note 5.
[15] For example, as part of the enforcement of the Digital Markets Act, European regulators required Apple to permit downloading applications from sources other than the Apple's own app store and required Apple to eliminate the mandatory 30% fee for in app purchases. Apple responded by providing an alternative with complicated new rules and new fees that – according to rivals – eliminated the utility of the alternatives. *See* Jacob Kasternakes, "Here's the New Apple Tax Every Developer is Going to Hate," The Verge (January 26, 2024); https://www.theverge.com/2024/1/26/24051823/apple-third-party-app-stores-50-cent-fee Emma Roth, "Epic's Tim Sweeny Call Apple App Store Changes 'Hot Garbage,'" (January 25, 2024) https://www.theverge.com/2024/1/25/24050696/epic-games-tim-sweeney-apple-app-store-response.
[16] Mark MacCarthy, "Google's Antitrust Troubles Demonstrate the Need for a Federal Regulator," Brookings (Sept. 30, 2024),

create regulations to enhance competition. Affirmative obligations to encourage new entrants and protect new entrants from entrenched incumbents with market power require new laws and ways to implement and enforce those laws.

Attempting to modify an existing agency has several drawbacks. As an initial matter, courts interpreting any authorizing statute will inevitably interpret an expansion of authority against the background of the agency's history and underlying authorizing statute. Creating a new agency allows Congress to start fresh – a critical consideration in light of the new realities of administrative law. Additionally, given the difficulties in coordinating policies and actions between existing agencies, it is easier to simply start with one designated central agency that could serve as a center of expertise and as the one central coordinating point for overlapping jurisdictions.

To be clear, Public Knowledge does *not* recommend rescinding existing agency authority, and does *not* intend to discourage agencies from using their existing powers to address anti-consumer and anticompetitive conduct. Congress has previously created agencies with overlapping jurisdictions. This frequently allows agencies to bring together their distinct expertise and enforcement authorities. But as we have seen since Public Knowledge first proposed a comprehensive sector-specific regulator in 2019, multiple agencies with fragmented jurisdiction attempting to coordinate cannot function or fill existing gaps in the law. Only a newly created sector-specific agency can bring together adequate authority and expertise.

B. Power and Structure of a New Agency

In light of the above, Public Knowledge continues to recommend that the proposed agency be structured as an independent commission similar to the Federal Communications Commission, the Federal Energy Regulatory Commission, and several other expert agencies which oversee important sectors of the economy. In recent cases, the Supreme Court has invalidated the creation of new independent agencies – in particular the ability to insulate members by limiting the ability of the president to fire members.[17] Those cases, however, involved different structures, such as agencies with a single head,[18] or where the new commission was itself under the authority of another independent commission, creating a "double layer" of protection against the president's authority.[19] In these cases, the majority categorized the new commissions as departures from precedent that sought to expand the ability of Congress to create independent agencies. A new

---

https://www.brookings.edu/articles/googles-antitrust-troubles-demonstrate-the-need-for-a-digital-regulator/

[17] See, e.g., Free Enterprise Fund v. Public Company Accounting Oversight Board, 561 U.S. 477 (2010).
[18] Seila Law LLC v. Consumer Financial Protection Bureau supra note 10.
[19] Free Enterprise Fund v. Public Company Accounting Oversight Board supra note 17.

Commission that simply replicates already approved structures should therefore pass constitutional review.[20]

Similarly, Public Knowledge continues to recommend that this new Digital Platform Commission have broad powers to impose pro-competitive regulations as well as power to limit anticompetitive practices. The DPC should also have adequate authority to protect consumers. Finally, the DPC should be explicitly authorized to conduct research on areas relevant to its jurisdiction, and to determine how to provide access to researchers consistent with protecting privacy and proprietary information.

This has acquired new difficulty in light of the Supreme Court's recent decisions. Traditionally, Congress could make broad delegations of authority with broad language. For example, the FCC has traditionally regulated broadcasters and other licensees under the broad language of requiring them to follow rules which serve "the public interest."[21] In light of recent cases undermining the concept of broad language delegating broad authority, however, Congress must be much more specific in terms of what it has actually authorized the agency to do, and the scope of its authority.

Unfortunately, Congress has traditionally granted broad authority to sector-regulating agencies because the dynamic nature of the field makes it difficult to be overly specific. Legislation, of necessity, reflects a snapshot in time in a field that is expected to evolve. It reflects the consensus of generalist lawmakers who cannot be expected to have necessary expertise to draft legislation as if Congress were an expert regulatory agency. (That these statutes are now subject to the interpretation of generalist judges with no responsibility to defer to the agency, and whose education on the subject comes from a handful of briefs with strict word limits, further aggravates the problem.) This was, of course, why Congress traditionally delegated to expert agencies rather than attempt to pass legislation to address every possible contingency.

The *Loper Bright* decision provides two avenues for Congress to delegate necessary authority to the proposed DPC. First, Congress may simply require by statute that courts defer to the agency. Congress does, from time to time, instruct courts on the relevant standard of review. Indeed, Congress may go so far as to expressly prohibit judicial review – although that would not be appropriate here. *Loper Bright* rested on the reasoning that the Administrative Procedure Act did

[20] Public Knowledge recognizes that this area of the law is subject to ongoing challenge. Even if a Commission cannot be wholly independent in the sense of limiting removal, no one has challenged the ability of Congress to structure Commissions so that no more than a bare majority may be from the party of the president.

[21] *See, e.g.,* 47 U.S.C. §§ 303(r), 307(a), 309(a). National Broadcasting Co. v. United States, 319 U.S. 190, 216-19 (1943).

not mandate a deferential standard of review and that, therefore, Congress intended courts to review statutory interpretation without deference to the agency's interpretation.[22]

Additionally, *Loper Bright* acknowledged that Congress may explicitly grant discretion to an agency.[23] For example, Congress may specify that "X shall have the definition given to it by the agency." In such cases, the grant of authority is clear, rather than assumed as it was under *Chevron*. Courts should therefore defer to the agency's determination – subject to the usual constraints against arbitrary and capricious actions under the Administrative Procedure Act.

Despite recent Supreme Court decisions, Congress still has the tools to create a robust agency capable of the flexibility and functions necessary to oversee the sector. It will require more precise drafting than previously. Broad, general language must be supplemented by more specific language with regard to jurisdiction and authority. Congress must state clearly when it expects a court to defer to the agency's determination. Finally, where Congress recognizes that an agency may need some level of flexibility in a dynamic and rapidly evolving field, Congress must state clearly that it has delegated the authority to make relevant determinations to the agency – even where the agency subsequently reverses a previous position.

C. Enforcement

Without enforcement, rules are simply suggestions. A constant complaint is that large companies can simply treat fines as a "cost of doing business." Antitrust authorities have faced the further problem of "compliance theater" (pretending to comply with no actual change in anticompetitive impact) or "malicious compliance" (behavior that technically complies, but moves so slowly or requires so many conditions as to make it extremely difficult to achieve the intended effect). An agency must have the power to impose effective remedies, monitor compliance, and enforce effective compliance.

Congress should therefore authorize the agency to issue a wide range of remedies, ranging from injunctions and other forms of equitable relief; the ability to seek restitution and disgorgement;[24] and the ability to impose fines of sufficient magnitude that they act as a genuine deterrent.

Pursuant to the Supreme Court's recent decision in *SEC v. Jarkesy*[25], fines for violations analogous to common law actions require a jury trial, whereas actions in equity and those involving "public rights" rather than "private rights" may be decided by an agency. It is not

---

[22] Loper Bright Enterprises v. Raimondo supra note 5 at 391-96.
[23] *Id.* 395-96.
[24] Disgorgement here means the return of illegally obtained revenues to the government, as distinct from restitution, which means returning money to individuals so that they are restored to their original position before the illegal conduct.
[25] Securities and Exchange Commission v. Jarkesy supra note 11.

entirely clear how to distinguish between these categories. Injunctions, for example, are purely equitable. Fines designed to punish or deter are, under *Jarkesy*, almost certainly actions at law requiring the jury to act as fact finder and to determine the damage award. But the Court indicated that actions for restitution or disgorgement might be considered equitable actions rather than "actions at common law" requiring a jury trial. Congress should clearly allow the DPC to issue injunctive relief and other forms of equitable relief – including restitution and disgorgement[26] – on its own authority. Assuming restitution and disgorgement are equitable in nature, it is unclear the extent to which these include other payments necessary to make the parties whole, or where this may cross the line into suits at common law analogous to breach of contract damages. But determining what actions are suits at law versus suits at equity, or what constitutes public rights versus private rights, is a complicated question. Congress must decide whether to commit this determination to agency discretion (with subsequent review by courts as to whether the agency made the proper determination), or limit the authority of the agency to grant relief to those matters that are clearly equitable and require the DPC to pursue other complaints in district court.

In any event, Congress should permit the DPC to bring actions in court rather than require it to use the Department of Justice as its litigator. Requiring the DPC to use the Department of Justice has the effect of limiting cases to those the DOJ considers an appropriate use of resources. But the DPC may consider particular enforcement cases important for precedential reasons or reasons of policy, where the DOJ would consider the prospective return too small (or where it regards the likelihood of a successful prosecution as too small) to justify the expenditure of resources. Congress should leave judgments about whether or not to bring an enforcement action entirely to the DPC.

D. Facilitating Research, Center of Expertise, and "Soft Power"

There was general consensus that an important function of the DPC should be to monitor the developments in the digital platform sector and to engage in research on important questions, such as the impact of differential pricing, "addiction by design," and other impacts on health, safety, and the economy. This power should not be limited to the agency itself, but should also facilitate research by others. Stakeholders suggested that the DPC serve as a center of expertise for Congress and other agencies – as well as a means for educating the general public. Indeed, it was suggested that if Congress did not wish to create an agency with broad regulatory powers, it could still create an agency with broad powers to research and set standards and best practices for platforms on matters such as information collection and privacy by design, or technical matters such as interoperability.

[26] Language in *Jarkesy* suggests that restitution and disgorgment are equitable remedies, as opposed to damages or fines which are remedies at law. But as the Court found that the damages imposed by the SEC were clearly "to punish" rather than to "restore the status quo," the Court did not provide a clear statement one way or the other. *Id.*at 123.

These standards could become a source of "soft power" by establishing liability for violating these standards, educating agencies with enforcement power, or facilitating voluntary cooperation in a way that would prevent collusion or anti-competitive conduct. It was noted that other agencies such as the National Institute of Standards and Technology exercise quasi-regulatory power by standard setting. Other agencies use standards as a form of "soft power," where the agency rarely invokes its enforcement authority but encourages voluntary compliance instead. Examples include food safety and consumer product recalls, where violation of standards may trigger civil liability in the absence of voluntary remediation.

Unfortunately, the PKPK participants did not explore these alternatives in detail and were unable to come to consensus on specific details. One suggestion was that DPC employees be "embedded" in digital platforms so that they can have a better understanding of the actual, day-to-day operations of digital platforms. Public Knowledge recommends that Congress explore this suggestion further.

Public Knowledge recommends that the DPC have investigatory powers similar to those invested in the Federal Trade Commission under Section 6 of the Federal Trade Commission Act.[27] The agency should also have authority to subpoena documents and individuals associated with digital platforms. This power should not be limited to civil or criminal investigations, but should be included as part of the DPC's research and reporting authority. Congress should investigate other mechanisms used by different agencies.

E. Risk Assessment, Duty of Care, and Other Duties Based on Traditional Fiduciary Relationships

As reflected in the PKPK discussion, there are many models of risk assessment used in regulatory practices. For example, in the EU, covered digital platforms are required under the Digital Services Act to conduct a risk assessment of their services for various potential harms, and to design and implement a risk mitigation plan. The EU Council (in the case of very large online platforms, or VLOPs[28], like Facebook) reviews the risk assessment and, if it finds the assessment or proposed mitigation insufficient, returns it to the VLOP to address the concerns.

Public Knowledge echoes the consensus of the PKPK that the DPC should have flexibility to adopt risk assessment and mitigation as one available tool. This should not, however, be the primary tool for regulating digital platforms. As described in the report from the Public

[27] 15 U.S.C § 46.
[28] The Digital Services Act defines VLOPs as online platforms with at least 45 million monthly users in the EU (approximately 10% of the EU population).

Knowledge Policy Konclave, effective risk assessment depends on a number of factors, most notably clear standards for identifying risks of concern, for evaluating them, and for mitigating them. Public Knowledge also recommends that risk assessment and risk mitigation compliance requires regular audits. Public Knowledge recommends that where risk assessment is used, failure to adopt an approved mitigation plan should open the digital platform to liability for negligence or product safety violations in addition to enforcement by the agency.

In this context, some scholars and advocates have recommended adoption of a common law duty of care, or other duties (such as a duty to protect from disclosure or misuse of personal information) derived from traditional common law fiduciary duties. This has been proposed, for example, in privacy bills such as the American Data Privacy Protection Act.[29] Public Knowledge recommends against this approach. As an initial matter, basing a statutory obligation on a common law obligation and right of action certainly brings the law under *Jarkesy*, which would require a jury trial for any enforcement action involving a fine.

More importantly, using a common law basis for regulation will import into the subsequent rulemaking and enforcement all of the traditional common law limitations and interpretations of the duty, limiting agency flexibility in rulemaking and enforcement. While common law duties may make good basic analogies to guide legislators when thinking about how to approach the problems of digital platforms, creating a new, comprehensive sector-specific regulator is necessary because the issues that arise in the digital platform space do not fit easily into traditional common law categories. Finally, common law duties generally arose independently in different contexts. They are not designed to work together as part of a comprehensive regulatory regime that addresses both competition and consumer protection.

F. Artificial Intelligence

Artificial intelligence was the topic of greatest contention and least consensus at this PKPK. Stakeholders had strongly held views on the extent to which AI should be regulated at all. All participants agreed that the proposed DPC should not be the *only* regulator of AI, but at the same time, it should have *some* role (even if only as a center of expertise). Part of the problem, of course, is that AI covers such a large range of tools and products that it is difficult to say what it means to "regulate" AI.

Nevertheless, Public Knowledge believes that there is sufficient developing consensus around basic principles that to the extent we are regulating "artificial intelligence" at all – whether by directly imposing rules on development of conduct, by imposing standards and developing best

[29] American Data Privacy and Protection Act, H.R. 8152 Sec. 102 (117th Congress) (creating "duty of loyalty").

practices, or through some other model – at least part of this oversight responsibility belongs in the proposed Digital Platforms Commission. There is a clear relationship between the largest digital platforms in developing and adopting complex AI tools, and in cases such as ChatGPT, the AI essentially functions as a digital platform itself.

Two analogies from the history of regulating telecommunications are helpful here. In 1910, under the Manns-Elkin Act, Congress initially placed the regulation of telephone and telegraph networks under the Interstate Commerce Commission, which regulated railroads. Congress reasoned that it made sense to place all common carriers under one regulatory agency. Approximately 25 years later, Congress created the Federal Communications Commission by transferring the regulation of telecommunications common carriers regulated by the ICC and combining it with the Federal Radio Commission in recognition that the appropriate sector for common regulation was communication, not common carriage. On the surface, one would think that telephones as common carriers had more in common with railroads than with radio broadcasters (who were expressly forbidden from being regulated as common carriers). But the importance of both telephones and radio broadcasting as media of electronic communication, as well as the importance of telephone lines to creating national broadcasting networks and the use of wireless spectrum for many forms of communications, made regulation by one comprehensive regulator of electronic communications the better policy

It is unclear at this point whether the relationship between digital platforms and evolving models of artificial intelligence will prove to be more like putting telephone regulation and railroad regulation in the ICC, or more like putting telephone and radio regulation together in the FCC. But for the time being, the relationship between digital platforms generally and evolving uses of powerful artificial intelligence tools specifically appears sufficiently symbiotic that Public Knowledge recommends putting *both* in the same agency.

V. Conclusion

Over the more than five years since Public Knowledge first proposed Congress create a regulator for digital platforms, the need for oversight has grown. The need to coordinate among multiple agencies ensures "gaps" will persist in the law and that no agency will have the necessary focus, resources, or expertise to oversee the sector. Indeed, the continued consolidation and consumer harm over the last five years demonstrate the failure of this piecemeal approach.

Paradoxically, while recent Supreme Court cases have made it somewhat more difficult for Congress to create an independent agency with suitably broad and flexible authority, they have also made it increasingly questionable that existing agencies operating under statutes that long predate the internet, let alone digital platforms, have the necessary authority to adequately promote competition or protect consumers. Rather than try to modify an existing statute to

expand the authority of an existing agency, Congress can better achieve the goals of promoting competition and protecting consumers by drafting an entirely new statute and creating a new agency.

No one expects Congress to create such an agency overnight – especially given the prevailing political winds. But the problems will only continue to grow until Congress, in some way or another, acts. Congress therefore faces a choice. It can continue to cede oversight to the states and to foreign countries. Or it can take action to create a regulatory regime consistent with American values, designed explicitly to protect Americans. Hopefully, the discussion and recommendations presented here will move the debate forward.

APPENDIX

Public Knowledge Policy Konclave Report:
Building the Digital Regulator
Patrick Yurky – Rapporteur

Table of Contents

Introduction and Parameters

Introduction: Why A Digital Regulator?

Digital platforms – dominant online services open to the public – form the center of today's life. Services such as Facebook, Amazon, Netflix, Apple, and Google have fundamentally transformed modern life, revolutionizing communication, commerce, entertainment, and access to Information.

Despite how pervasive digital platforms are and how quickly they – and their problems – evolve and expand, there is no one piece of legislation or enforcement scheme protecting people and communities from their risks and potential harms. That is why we need a digital regulatory agency.

Public Knowledge first called on Congress to create a digital regulator in 2019, in the form of a book by Harold Feld, Senior Vice President of Public Knowledge, "The Case for the Digital Platform Act." A subsequent report from the Shorenstein Center at the Harvard Kennedy School advocated for a Digital Platform Agency to promote competition and enforce a digital duty of care. In 2022, US Senators Michael Bennet and Peter Welch introduced the Digital Platform Commission Act, first-of-its-kind legislation to create an expert federal agency able to regulate digital platforms in the areas of consumer protection and competition. In 2023, Senators Elizabeth Warren and Lindsay Graham introduced the Digital Consumer Protection Commission Act, which would establish a new commission to regulate online platforms, promote competition, protect privacy, protect consumers, and strengthen national security. Our goal is to continue and advance the dialogue by identifying key regulatory challenges and developing more detailed frameworks and strategies for establishing and empowering such an agency.

It wouldn't be the first time Congress has stepped in to resolve complex issues in a particular industry. Congress has created many targeted regulators – the Consumer Financial Protection Bureau, the Equal Employment Opportunity Commission, the Department of Justice, the Federal Communications Commission, and more – all staffed with experts to ensure American companies can push the bounds of innovation and competition without harming the public.

Parameters of the Policy Konclave on a Digital Regulator

On July 15, 2024, Public Knowledge hosted a policy conclave titled “Building the Digital Regulator.” The event brought together 25 subject matter experts from law, technology, policy, and academia to explore the need for a specialized digital regulatory agency in the United States. Discussions focused on identifying key regulatory challenges and developing frameworks and strategies for establishing and empowering such an agency.

To encourage open dialogue, the conclave operated under a modified Chatham House rule.[1] Participants attended in their individual capacities, contributing diverse perspectives aimed at advancing the discussion on digital regulation. The goal was to foster robust dialogue and generate concrete policy recommendations to guide the creation of an effective Digital Regulator in the US.

Participants delved into issues relevant to the scope of a dedicated regulator such as consumer protection, competition, and AI regulation.[2] The sessions were designed to identify new strategies and opportunities for policy development. Participants were all given an opportunity to review a draft version of this report and provide feedback. Public Knowledge, dedicated to the idea of a Digital Regulator, hopes that this conclave will push forward the conversation about what is possible for such an agency.

The event's discussions will be the basis of a detailed set of policy recommendations from Public Knowledge, derived from the insights shared during the sessions.

Day 1: Guided Discussions

The conclave began with guided discussions led by subject matter experts, covering essential topics to understand the context for a US Digital Regulator. Each discussion began with a brief introduction to the subject matter; these were designed to bring all participants to some baseline level of knowledge. The five sessions were:

1. Comparative approaches to digital platform regulation in Europe and the UK.
2. Legislative and political considerations regarding Congress.
3. The state of AI regulation in the US.

---

[1] Under Chatham House rule, participants are not made public and the participants themselves, while allowed to use the information, are not allowed to identify participants or affiliation. In the interest of transparency, Public Knowledge is listing the participants and their affiliations, but not ascribing any specific views, quotes or comments to any individual participant.

[2] The discussion explicitly excluded content moderation.

4. Dynamics impacting interagency cooperation within the federal government.
5. Recent Supreme Court rulings affecting the structure and powers of government agencies.

These discussions provided the background information on critical issues and challenges that will inform the design of a Digital Regulator's structure and function.

1. Digital Platform Regulation in Europe and the UK

Overview

This session examined the regulatory frameworks and approaches to digital technology in the EU and the UK, focusing on the creation of specialized digital regulatory agencies. Participants discussed the Digital Services Act (DSA), the UK Online Safety Act (OSA), the AI Act, and the Digital Markets Act (DMA). They compared the different regulatory philosophies, structures, and implementation strategies, exploring how these institutional decisions influence regulatory outcomes. The goal was to draw lessons from these frameworks to inform the potential creation of a specialized Digital Regulator in the United States. Participants also discussed the challenges of balancing regulatory measures with fundamental rights and ensuring proactive compliance from companies.

Presentation of Background Information

Participants began with an overview of the regulatory landscape in the EU, focusing on the DSA. They described the DSA as an extension of the EU's framework for illegal content and intermediaries, harmonizing laws across member states. The act emphasizes proactive measures, requiring platforms to conduct audits and risk assessments and to publish their findings. This approach aims to address issues before they escalate, contrasting with the traditional reactive regulatory model.

Participants also discussed the UK's approach through the OSA, which imposes duties on platforms regarding illegal harms and user protection, especially for children. They highlighted the act's clear definition of "illegal" content as reducing human rights issues by limiting government interpretation. However, participants noted that the vague language around child protection has led to implementation challenges.

Participants then covered the AI Act, which categorizes risks into four levels: unacceptable, high, low, and minimal. They pointed out that the AI Act includes more procedural requirements and a decentralized enforcement model, contrasting with the more centralized DSA. Unlike the OSA, the AI Act lacks a strict "illegal" designation.

Finally, participants discussed the DMA, focusing on its regulation of gatekeepers—large online platforms with significant market impact. The DMA imposes strict prohibitions, such as preventing the bundling of services, and relies on a collaborative enforcement approach

involving joint teams. Participants noted that its specificity in legislative language has led to numerous court rulings and regulatory findings, creating prohibitions that align directly with legislative goals.

Q&A and Discussion

During the discussion, participants raised questions about the measurement and evaluation of risk assessments under these frameworks. One participant questioned whether the assessment should include a cost/benefit analysis considering both harms and benefits. The response suggested that while the EU frameworks consider fundamental rights, they may weigh them differently than what might be expected in the US context. Participants also expressed concerns about whether the risk assessments under the DSA are sufficiently comprehensive.

The conversation also explored the differences between the EU and UK regulatory approaches. While the EU has centralized the DSA's implementation, the UK relies on existing agencies and structures, coordinating efforts through a joint council. Participants debated the merits of these approaches, particularly in the context of whether the US should create a new regulatory body or enhance existing agencies' powers. They also raised concerns about the effectiveness of such coordination compared to a focused regulatory body.

Participants discussed the rapid pace of regulatory development in Europe, expressing concerns about potential politically-motivated regulatory overreach and challenges in ensuring effective enforcement. They noted that while the DMA is more specific and legally grounded, the DSA and AI Act required building multiple institutions to handle transparency, settlement, and other issues, which involved significant institutional overhead. In contrast, participants noted that the American system tends to seek a "silver bullet" approach due to the difficulty of passing legislation, raising doubts about whether the EU's multi-faceted regulatory approach could be replicated in the US.

The session concluded with a discussion on the broader implications of these regulatory frameworks, including the potential for political influence and the need for ongoing evaluation to ensure their effectiveness. Participants noted that while the EU's approach is more structured, it may also be more complex and challenging to implement effectively, particularly given the varying levels of institutional capacity across member states.

Key Ideas:

- The DSA emphasizes proactive regulation, requiring platforms to conduct risk assessments and audits before issues arise.
- The UK's approach with the OSA relies on existing regulatory structures and emphasizes cooperation among agencies rather than creating new bodies.
- The AI Act categorizes risks and includes specific procedural requirements, but its decentralized enforcement model may pose challenges.
- The DMA is more focused and legally specific, with clear goals related to competition and fairness.

- Participants emphasized the need for ongoing evaluation of these regulatory frameworks to ensure they remain effective and avoid unintended consequences.

2. The Current Landscape in Congress

Overview

The session titled "The State of the Hill" explored the current political landscape and its impact on technology regulation, with a particular focus on the potential creation of a specialized Digital Regulator agency in the United States. Participants discussed the legislative environment, the influence of political dynamics, and the challenges associated with advancing technology-related legislation, including AI policy, privacy, and competition. The conversation also touched on the potential impact of recent judicial decisions, such as the Supreme Court's overruling the doctrine of Chevron deference, on the legislative process and regulatory frameworks.

Presentation of Background Information

The session began with participants acknowledging the significant role that political considerations on Capitol Hill play in tech regulation. Both Republicans and Democrats have an interest in this area, though their approaches differ. They focused on key areas including national security, elections, online competition policy, and the emerging debate on AI, liability, and copyright issues. Participants highlighted the Digital Platform Commission Act (DPCA) as a legislative proposal that would establish a new agency to regulate major digital platforms, taking a comprehensive approach to regulation.

Participants noted an increasing awareness among newer members of Congress regarding the potential and risks of technology. However, this awareness has not yet translated into cohesive legislative action, as evidenced by the fragmented approach to tech, AI, and privacy issues across various committees. They also addressed the implications of the post-Chevron world, where the role of agencies like the Federal Trade Commission (FTC) may be redefined. Some participants argued that Congress might empower the FTC, while others suggested that a new, specialized agency might be more effective.

Q&A and Discussion

Participants delved into the practical challenges of advancing technology regulation on Capitol Hill. They expressed concerns about the difficulty of passing comprehensive legislation, citing a divided Congress, the persistence of the filibuster, and the fragmented nature of committee work

as significant obstacles. They generally agreed that political and legislative progress is slow and complicated, with many bills stalling in committees.

They also explored the potential impact of the Chevron overturn and related judicial decisions on the regulatory landscape. Participants worried that these changes could increase the complexity and time required to pass effective legislation, potentially leading to more fragmented and less effective regulatory outcomes. They discussed the need for a new legislative approach that considers the evolving nature of technology and the complexities of regulating it.

The conversation emphasized the importance of educating legislators about the nuances of technology regulation, drawing parallels with the historical development of telecommunications legislation. Participants stressed the need for detailed, substantive hearings that go beyond performative politics to truly inform and prepare Congress for the challenges ahead.

They highlighted the need for expertise in educating Congress, suggesting the reinstatement or creation of bodies to provide independent, expert analysis to legislators. Participants noted that the current expertise in Congress is often provided by technology fellows, primarily funded by tech companies, raising concerns about regulatory capture (some speculated that this was the purposeful outcome of the dissolution of the Office of Technology Assessment).

They also discussed the potential role of states as regulatory actors, especially in light of shifting dynamics post-Chevron. Some participants suggested that Congress should consider the implications of state-level regulation and its impact on federal policy.

Finally, participants underscored the importance of having independent, technologically aware analysis within Congress, lamenting the loss of resources like the Office of Technology Assessment (OTA). They concluded the discussion with a call for greater expertise and oversight in regulatory matters, emphasizing the need for a comprehensive approach to technology regulation that includes input from a wide range of stakeholders.

Key Ideas:

- Participants noted that the influence of political considerations, including the filibuster and the fragmented committee system, presents substantial challenges to the progress of technology-related legislation.
- They identified significant complexities in creating a new regulatory agency or empowering existing ones, particularly in a post-Chevron world.
- Participants emphasized the need for substantive, educational hearings to prepare Congress for the challenges of technology regulation, drawing on lessons from past legislative efforts, such as telecommunications.

- They stressed the importance of restoring independent, technologically aware analysis within Congress, along with comprehensive oversight mechanisms in regulating technology.

3. The State of AI Regulation

Overview

The session explored the current state of AI regulation, focusing on various approaches in the US and internationally. The discussion centered on categorizing regulatory efforts and defining the scope of regulation. Participants examined existing laws, new legislative initiatives, and soft-power efforts, discussing their implications for AI governance. The conversation also touched on AI's intersection with intellectual property (IP) issues, competition, and the potential role of a specialized Digital Regulator.

The session provided insights into whether and how a new Digital Regulator should address AI, given the complexity and rapid evolution of the technology. Participants categorized approaches to AI regulation into three tiers: interpretations of existing laws, new legislative initiatives, and soft-power initiatives. They also explored the scope of AI regulation, distinguishing between regulating AI as a technology and its use in specific sectors. The discussion emphasized the institutional challenges of designing an appropriate regulatory structure without clear definitions of what and who needs to be regulated.

Presentation of Background Information

The session began with an overview of AI regulation, organized around two main framing devices.

The first framing device categorized AI regulation into three tiers: interpretations of existing laws, new legislative initiatives, and soft-power initiatives. Participants highlighted that some existing sectoral laws are being extended to cover AI, particularly in areas like finance. They cited the Biden Administration's Executive Order as an example, which relies on existing statutory authority, such as the Defense Production Act. The discussion then shifted to new legislative initiatives, with participants emphasizing the significance of the EU AI Act. They noted that this Act establishes new institutional structures, like the AI Office, to oversee compliance. Additionally, participants mentioned that over 400 AI-related bills have been introduced at the state level in the US this year. In the third tier, participants discussed soft-power initiatives, including efforts like the National Institute of Standards and Technology (NIST) framework for voluntary compliance and global safety summits. They also acknowledged the

role of institutes focused on AI safety in the US and UK, although these efforts currently lack statutory authority.

The second framing device examined the scope of AI regulation through different approaches. Participants noted that some regulations focus on specific aspects of AI, such as disclosure requirements for AI use in election ads, while others take a broader approach, attempting to regulate AI either at the application level or the model level. They highlighted the crucial distinction between regulating AI as a product versus as a technology.

Q&A and Discussion

Participants debated the intersection of AI regulation with IP issues, questioning how IP concerns, particularly those related to training data and AI outputs, should be handled within the AI regulatory framework. Some argued that safety could encompass protecting IP rights, while others warned against conflating the two. They mentioned the EU's approach of regulating AI without directly addressing IP issues as a possible model.

The discussion also covered the potential role of a Digital Regulator in overseeing AI. Participants focused on competition issues and AI's broader impacts on various industries. They debated whether AI's effects, rather than the technology itself, should be the focus of regulation. Some suggested that AI regulation, particularly at the model level, might be better suited to technical bodies like NIST. Concerns were raised about potential gaps in expertise and the risk of industry capture if existing agencies, such as the FTC, were tasked with AI regulation.

Participants emphasized the importance of training data and privacy in AI development, expressing concerns about the impact of training data on AI behavior, particularly in terms of representational issues and the quality of data sources like Reddit or YouTube. They highlighted the need for public oversight and standards for training data, along with the privacy implications of training data quality and sources. The discussion also addressed the potential for discriminatory or biased outcomes based on training data choices, especially if limited to public domain data.

Participants discussed the geopolitical context of AI regulation, particularly the US-China competition, noting that this competition could constrain the political feasibility of some regulation and have a broad impact on the regulatory landscape.

Key Ideas:

- There was a consensus on the need for a clearer problem definition: What problems is AI regulation intended to solve?

- Clarity is critical in defining the scope and authority of any potential AI regulatory agency.
- It is important to consider the secondary impacts of AI, rather than focusing solely on the technology itself.
- There is an ongoing debate over whether or how to integrate IP concerns into the broader framework of AI regulation.
- Given the role of training data in shaping AI behavior and its potential societal impacts, this is an important concern for regulation.
- The pervasive nature of AI across various sectors complicates the creation of a sector-specific regulator.

4. Inter-agency Cooperation in the Federal Government

Overview

This session focused on the dynamics of cooperation among US government agencies, particularly regarding overlapping regulatory jurisdictions. The discussion aimed to provide insights into the challenges and benefits of interagency coordination, offering lessons for creating a specialized Digital Regulator agency. Participants explored different models of agency collaboration, identified obstacles to effective cooperation, and debated how a new Digital Regulator could fit into the existing regulatory landscape.

Presentation of Background Information

The session began with an exploration of how government agencies collaborate—or struggle to collaborate—when jurisdictions overlap. Participants highlighted several taxonomies of agency coordination, ranging from significant overlaps between economy-wide regulators to the dynamics between general and sector-specific regulators.

Participants examined potential models for a Digital Regulator, considering the possibility of creating an agency with specific authority to address issues like competition, privacy, and content moderation. They emphasized the need for clear jurisdictional boundaries to minimize conflicts with existing agencies like the FTC. They also stressed that the new agency must embed technical expertise to avoid reliance on industry-provided knowledge.

The discussion included examples of overlapping jurisdictions, such as the FTC and Department of Justice (DOJ), where even strong collaboration, like in antitrust enforcement, can lead to clearance fights—conflicts over who has jurisdiction. These conflicts can delay enforcement actions and complicate regulatory processes, with companies potentially exploiting differences

between agencies to avoid stricter regulations. Participants also covered the dynamics between sector-specific regulators, like the Department of Transportation (DOT), and general regulators like the DOJ. Sector-specific regulators often possess deeper industry knowledge but may lack expertise in competition principles or consumer protection issues. Participants highlighted instances where overlapping authority served as a safeguard against industry capture, enabling more aggressive enforcement when one agency's leadership was hesitant.

Another key discussion point involved the interaction between general regulators without competition authority and sector-specific regulators. Participants cited the Department of Health and Human Services (HHS), which focuses primarily on goals like quality and access, often sidelining competition concerns. Such agencies can be challenging to coordinate with due to their distinct regulatory goals and potential for regulatory capture. Participants emphasized the need to integrate competition and safety goals into a new Digital Regulator while addressing the risks of regulatory capture.

They also discussed the high coordination costs associated with overlapping jurisdictions, particularly in enforcement. Participants identified regulatory arbitrage, where entities exploit differences between agencies, as a significant challenge.

Q&A and Discussion

Participants discussed strategies for improving coordination between agencies, emphasizing the importance of maintaining institutional structures for stability and using political moments to formalize collaboration through Memorandums of Understanding and data-sharing agreements. They highlighted the role of political leadership in fostering shared learning processes as a successful approach in some contexts.

They cited the collaboration between the FTC and Department of Labor (DOL) as a positive example of agencies enhancing their understanding and enforcement capabilities. Participants also mentioned the White House Competition Council as a recent effort to improve interagency coordination on competition issues. However, they expressed concerns about how to institutionalize such coordination across different administrations.

Participants focused significantly on the technical deficits within government agencies, particularly in regulating complex technologies. They emphasized the need for regulatory bodies to have embedded technical expertise to avoid reliance on industry specialists and lobbyists. They expressed concerns that a new Digital Regulator might rely on areas of familiarity rather than fully understanding the technical background of the issues.

The session concluded with participants discussing the need to clearly define the policy areas for which a new Digital Regulator would be responsible, to balance regulatory goals. They debated the potential benefits and drawbacks of consolidating multiple regulatory areas—such as competition, privacy, and content moderation—under a single agency. Participants raised concerns about balancing these areas and ensuring the agency has the capability to manage these competing interests effectively.

Key Ideas

- Participants acknowledged significant difficulties in inter-agency coordination.
- Participants emphasized that agencies must develop and maintain technical expertise, crucial for effective regulation, particularly in the rapidly evolving digital space. They raised concerns about the technical deficit within government agencies and how a new regulator could ensure it has the necessary expertise to handle complex digital issues.
- Participants highlighted regulatory capture as a significant risk. They noted that overlapping jurisdictions can sometimes serve as a safeguard against capture by ensuring multiple perspectives in enforcement actions.
- Participants reached a consensus on the importance of clearly defining the roles and responsibilities of a new Digital Regulator to minimize coordination issues and ensure the agency can effectively manage its various regulatory goals.

5. Impact of Recent Supreme Court Cases

Overview

This session examined the implications of recent Supreme Court decisions for the structure and authority of regulatory agencies in the United States, with a particular focus on three significant cases: *Seila Law LLC v. Consumer Financial Protection Bureau*, *SEC v. Jarkesy*, and *Loper-Bright Enterprises v. Raimondo*. The group analyzed these cases to understand their potential impact on the creation and operation of independent agencies, the scope of agency authority, and the future of regulatory enforcement, especially in relation to a proposed Digital Regulator agency. The discussion primarily centered on *Loper-Bright Enterprises v. Raimondo*, as participants raised concerns that the overruling of the Chevron Doctrine and the subsequent weakening of agency authority might compel Congress to be more explicit in granting authority to agencies. This, coupled with political challenges, led participants to question the flexibility and scope of a new Digital Regulator.

Presentation of Background Information

Participants examined *Seila Law LLC v. Consumer Financial Protection Bureau*, discussing how it reflects the Supreme Court's stance on independent agencies, particularly regarding their expansion. While independent agencies are unlikely to disappear, participants anticipated that any efforts to expand their powers will likely face significant constitutional challenges. The Court's decisions indicate a reluctance to broaden the scope of these agencies, suggesting that any such attempts may be deemed unconstitutional.

In discussing *SEC v. Jarkesy*, participants focused on agency enforcement and the increased requirements for jury trials when agencies seek damages. The Supreme Court's ruling identified certain categories of actions that do not fall under suits at common law, thereby exempting them from requiring a jury trial. However, participants noted that most agency actions seeking damages will now necessitate a jury trial if they resemble common law suits. This poses challenges for agencies like the FCC, where the common law analogs for tech-related regulations are unclear, potentially complicating enforcement.

Participants also thoroughly discussed *Loper-Bright Enterprises v. Raimondo*, considering the implications for regulatory authority, particularly regarding how explicit statutory language must be to grant agencies the power to regulate new and emerging technologies. They debated the ruling's impact on the major questions doctrine, questioning whether statutes can now be reinterpreted in light of this doctrine. The conversation also touched on the potential shift of regulatory authority to the states, especially in scenarios where federal statutes are ambiguous or where courts favor broad agency authority to preempt state actions.

The session also addressed the possibility of the Supreme Court expanding the Non-Delegation Doctrine, which participants believed could further restrict Congress's ability to delegate broad regulatory authority to agencies. As with the ruling in *Loper-Bright*, participants agreed that this would require any new Digital Regulator to operate under very specific statutory mandates.

Q&A and Discussion

During the discussion, participants focused on the potential expansion of the Non-Delegation Doctrine by the Supreme Court, which they believed would require more explicit delegation of authority from Congress to agencies. They expressed concern that this could severely limit the flexibility of agencies like the proposed Digital Regulator, which may need broad discretion to effectively regulate rapidly evolving technologies. Participants emphasized the need for Congress to clearly define the scope and authority of a Digital Regulator to avoid legal challenges. The debate also extended to whether Congress should create a new agency or expand the authority of existing agencies like the FTC.

Participants noted the importance of Article III judges in interpreting the law, arguing that this could limit Congress's ability to delegate interpretative authority to agencies. They linked this point back to the *Loper-Bright* case, where the Court suggested that judges must have the final say on legal interpretations, even with congressional delegation.

The conversation also highlighted the tension between quick regulation and enforcement. While regulation provides clarity, it is often slow and vulnerable to legal challenges. Enforcement, on the other hand, can be quicker but may lack the same level of authority or permanence. Participants argued for developing new enforcement tools to address specific conduct areas without resorting to lengthy regulatory battles.

With the likely requirement under *Jarkesy* for more cases to go to jury trials, participants expressed concerns about the practicality of enforcing digital regulations.

The debate also covered the balance between state and federal authority, particularly given the current conservative Court's tendency to favor state power over federal preemption. Participants discussed how much authority should be left to states versus a federal Digital Regulator.

Participants raised concerns about standing to challenge agency actions, especially in light of *Loper-Bright*'s implications for the timing of challenges. They noted that the Court's ruling that the statute of limitations for challenging agency rules begins when an entity sustains an injury could lead to significant instability in agency rulemaking, as challenges could arise long after a rule is established. Participants expressed concern about the expanded potential for retroactive challenges to regulations, where new entities could challenge regulations that were enacted before the entity existed.

Finally, participants considered the potential for private rights of action as a mechanism for enforcing compliance with regulatory standards. They viewed this approach as a way to supplement limited agency enforcement capabilities, particularly in the context of a Digital Regulator dealing with rapidly evolving technologies.

Key Ideas

- As the Supreme Court becomes more restrictive in interpreting agency authority, participants emphasized the growing need for Congress to be very clear and specific in the language used to grant regulatory powers. It was also agreed that pragmatically, the breadth of powers of a new federal agency would probably not be able to exceed those of any current agency.
- The potential for federal regulatory actions to preempt state laws is a significant concern, with some participants arguing for the importance of leaving room for state-level regulation in certain areas.

- Participants highlighted the idea of using private rights of action to ensure compliance with regulations as a potential solution to the challenges posed by limited agency resources and the increasing complexity of regulatory environments. They suggested that this approach, possibly undertaken by state attorneys general, could offer an alternative to traditional regulatory enforcement, protecting against the susceptibility of agency action to challenges.

Day 2: Team Proposals

On the second day, participants divided into working groups to address specific aspects of creating a Digital Regulator. Building on the context from Day 1, the groups discussed and made recommendations on:

1. The role of an agency in managing research and access to data.
2. Rules, risks, and responsibilities in the agency's regulatory framework.
3. The organizational structure of the agency.
4. The role of the Digital Regulator concerning AI.

Each group presented their findings, which were then discussed and refined by the larger group of participants.

1. Access to Research

Overview

The session focused on Group 1's recommendations regarding how a potential US Digital Regulator should manage research and access to research data. Participants discussed how to grant researchers access to data while maintaining confidentiality and privacy protections, structuring research within the regulatory framework, and addressing liability and data misuse challenges. They focused on key issues like defining researcher qualifications, balancing data access with privacy concerns, and addressing First Amendment issues related to data use. The session aimed to provide recommendations on structuring data access to support effective research while maintaining safeguards.

Initial Recommendations

The working group presented several recommendations to enhance research capabilities within the proposed digital regulatory framework:

Regulatory Access to Data: The group recommended regulations to grant researchers access to both internal studies conducted by companies and the underlying data, which they considered crucial for informed regulatory decisions.

Advisory Committee: They proposed establishing an advisory committee, primarily composed of researchers, to guide the agency's agenda and implementation strategies, ensuring alignment with research needs and agency goals.

Embedding Regulators in Workflows: Drawing from financial industry models, the group suggested embedding regulators within companies to gain insight into internal workflows that could ensure compliance.

Standard-Setting Process for APIs: To facilitate data access, the group recommended a standard-setting process for APIs, led by the agency with input from the private sector, to standardize and control data access.

Preventing Data Misuse: Responding to concerns about data misuse, such as the Cambridge Analytica case, the group proposed corporate confidentiality exclusions and individual privacy protections. This approach would negate the need to distinguish between researchers and academics.

Long-Term Research and Accountability: The group emphasized the need for the agency to fund long-term research, countering financial incentives favoring quick, high-impact results. They also recommended ongoing evaluation of research effectiveness to ensure accountability and potentially provide authority to follow up on previous actions.

Discussion and Debate

Participants questioned the scope of entities overseeing the research process, including which companies would be regulated and how data access would be managed. They discussed the complexities of differentiating between types of research and ensuring data is not used for commercial purposes. Some participants suggested the agency should have broader powers to collect data from various sources, not just regulated entities.

They debated whether existing US federal agency models could be adapted for the Digital Regulator or if new structures were necessary. Participants referenced other regulatory frameworks, such as the FTC’s approach to liability and privacy, and considered whether these could inform the new agency's design.

Privacy emerged as a significant concern, particularly the need to protect individual communications and sensitive data. Participants considered Fourth Amendment implications and how different data sensitivity levels might require varying access levels. They focused on liability issues, raising concerns about who would be liable in data breach or misuse cases—companies or researchers. Some suggested the agency could act as a data repository, with researchers accessing data through the agency under strict safeguards, such as on-site equipment use or external facility inspections.

Participants highlighted the importance of public input in setting the research agenda, stressing the need for a process that includes diverse perspectives and addresses topics affecting marginalized groups. They also debated the relevance of research to the agency's regulatory goals. Some argued that research should directly relate to the law, with the agency having discretion over permissible research. Others raised concerns about overly broad research mandates forcing companies to expose too much information. Participants compared international models like the DSA, which has specific requirements for researcher access to data. They emphasized the need for a vetting process to determine who qualifies as a researcher, considering differences between US and European approaches to data access, privacy, and law enforcement.

Consensus and Disagreement

Participants generally agreed on the importance of establishing clear confidentiality and privacy protections and the need for an advisory committee to guide the research agenda. They also supported embedding regulators within companies and creating a standard-setting process for APIs.

However, they disagreed over the scope of research access, liability issues, and the relevance of research to the agency's goals. Some participants felt the proposed research framework was too broad and could lead to unnecessary exposure of company data, while others argued for a more flexible approach allowing a wide range of research activities.

Concluding Remarks

The session concluded with participants acknowledging the complexities involved in balancing data access with confidentiality and privacy protections. They recognized the need for further discussion to refine the recommendations, particularly regarding liability, research relevance, and public input. The group acknowledged the potential of the proposed framework but emphasized the need for careful consideration and ongoing dialogue to address the challenges and concerns raised during the discussion.

2. Rules, Risks, Responsibilities (but Mostly Risk Assessments)

The session focused on the work of Group 2, which examined how a potential Digital Regulator agency in the United States should develop its regulatory framework, particularly regarding risk assessments, rulemaking, and liability standards. The primary focus was on the function and form of risk assessments, while also considering broader regulatory questions such as rulemaking, common law duties for regulated entities, and appropriate policy areas for a Digital Regulator. The session aimed to evaluate different models for these areas and provide recommendations for structuring the agency's approach.

Initial Recommendations

The working group outlined the scope of their discussion, focusing on the integration of rulemaking and risk assessments, common law duties for regulated entities, and the fit between a Digital Regulator's policy and structure. They concentrated primarily on risk assessments, noting that the policy areas were too broad to tackle comprehensively in a single session. Different fields may require distinct forms of risk assessments, with varying needs for coverage and participation.

Focus of the Digital Regulator: The group discussed the appropriate focus areas for the Digital Regulator, emphasizing that the correct mix of foci remains unclear and depends on the assigned policy areas, such as consumer protection and data protection. They stressed that the effectiveness of risk assessments would largely depend on these focus areas.

Spectrum of Risk Assessment Models: The group identified a spectrum of risk assessment models, ranging from strict regulatory obligations (e.g., DSA/CPPA agency style) to co-regulatory models (e.g., examples from the UK) to the Global Network Initiative (Ruggie principles, HR due diligence), and finally, pure self-regulation. They centered the discussion on the first three models, without strictly preferring any single approach.

Obligation Scope: The group considered who would be obligated to conduct risk assessments under a Digital Regulator framework. They discussed options such as Very Large Online Platforms, medium and large entities, or potentially all entities, with criteria based on factors like revenue thresholds or the number of data subjects. They did not reach a definitive conclusion on this matter.

Liability Issues: The group debated several liability issues, including whether liability should be linked directly to the risk assessment or only to substantive compliance obligations. They also discussed the possibility of liability for failing to complete or submitting poor-quality risk assessments, suggesting that the regulator set clear standards. The IRS tax enforcement model

served as an example, where assessment submission can trigger audits but does not guarantee compliance.

Disclosure of Risk Assessments: The group debated whether risk assessments should be fully public, disclosed only to the regulator, or available in an abridged version. They suggested that the agency might have the authority to request full or internal versions as needed.

Information Sources for the Regulator: The group identified various information sources that a Digital Regulator might rely on, including risk assessments, investigatory authority, regulatory prospecting, and sectoral cases.

Purpose of Risk Assessments: The group described the ultimate goal of risk assessments as integrating internal processes within companies to mitigate risks, including avoiding the deployment of systems with unmitigatable risks. They emphasized that these assessments must be purposeful and practical, avoiding dense paperwork that fails to serve the public interest.

Discussion and Debate

Participants debated the timing of risk assessments, questioning whether they should tie them to specific products or services or apply them more broadly. They acknowledged the complexity of the issue, with different approaches potentially applicable depending on the regulatory focus.

Participants discussed the role of third parties in developing standards and frameworks for risk assessments or evaluating their results. They expressed varying opinions on the benefits and challenges of involving external auditors, with some noting the potential cost burdens and the risk of audits lacking thoroughness.

The group also debated various approaches to systemic risk assessment, including the potential role of independent auditors and standards for auditors. Some participants questioned whether companies could effectively assess systemic risks on their own or if external methodologies would be necessary. They raised concerns that individual companies might struggle to grasp cumulative risks across the broader digital ecosystem. Additionally, participants discussed how to ensure that companies have the right internal teams to address systemic risks effectively.

Participants noted the difficulties in defining the scope of risk assessments, particularly in the context of ongoing processes or incremental changes within companies. They also highlighted the challenges of setting standards for auditors and ensuring that risk assessments are comprehensive and practical.

The discussion touched on whether human rights and other ethical concerns should be included in risk assessments. Participants argued for the inclusion of these considerations, advocating for

them to be a core part of the process, while others noted the complexities of integrating them into existing regulatory frameworks.

Consensus and Disagreement

Participants generally agreed on the importance of clear standards for risk assessments and the need for external audits to ensure compliance and proper implementation. They also agreed on the necessity of involving third parties, although they debated the specifics of their role. The group concurred that the Digital Regulator should have the flexibility to adapt risk assessment requirements based on the specific policy areas it oversees, which would help address both systemic risks and product-specific issues effectively.

However, participants disagreed substantially regarding the scope of obligation for conducting risk assessments and the extent to which individual companies should assess systemic risks versus relying on external auditors. They also expressed differing opinions on the appropriate timing of risk assessments and the integration of human rights considerations.

Concluding Remarks

The session concluded without reaching definitive conclusions on many of the issues discussed. Participants acknowledged the complexity of the topics and the need for further discussion and exploration of potential models and standards for risk assessments under a Digital Regulator framework. They emphasized the importance of continuing to develop and refine these ideas in future sessions.

3. Structure of the Agency

Overview

The session focused on the proposed structure of a digital regulatory agency in the United States. The working group debated the merits of different models, including independent versus executive agencies, and considered the agency's potential scope of authority. The discussion also covered how the agency would coordinate with existing entities, especially if it were to function as an expertise-based agency rather than one with exclusive jurisdiction. The group also examined the legal and political constraints that would shape the creation of such an agency, particularly in light of recent Supreme Court decisions.

Initial Recommendations

Feasibility of Independent Agencies: The group agreed that, while existing independent agency structures could survive or be replicated, the current political environment is unlikely to tolerate the creation of new independent agencies, particularly those with administrative law judges (ALJs).

Potential Agency Structures: The group explored different structures for the Digital Regulator, weighing the pros and cons of independent agencies (e.g., FCC, FEC, Commission on Civil Rights) versus executive agencies. They noted that independent agencies generally adhere strongly to processes and procedures, especially when minority members are present, while executive agencies might be more agile in policy implementation but could face challenges in balancing authority with other agencies.

Agnosticism About Form: The group remained largely agnostic about the agency's form, recognizing the benefits of both commissions and executive agencies. They considered the possibility of the new agency having research and standard-setting functions similar to NIST or the US Commission on Civil Rights, which focus on fact-finding and standard-setting without enforcement powers.

Rulemaking and Enforcement Authority: The working group emphasized the importance of granting the new agency rulemaking and enforcement authority, along with the ability to conduct deep market research, similar to the UK's Competition and Markets Authority. They also discussed whether the agency should defer to or incorporate multi-stakeholder standard-setting or industry efforts.

Flexibility in Design: The group agreed that while the agency's specific structure remains undecided, it must have rulemaking and enforcement authority. They emphasized the need for flexibility in the agency's design to enable it to adapt to emerging technologies and regulatory challenges.

Coordination with Existing Agencies: The group concluded that, at a minimum, other agencies should give substantial deference to the new agency's expertise, particularly in areas like digital markets and competition.

Privacy Jurisdiction: The group questioned whether privacy should be housed within the new agency or remain under the FTC's jurisdiction. They expressed concerns about how the new agency would coordinate with other entities, especially given the lack of formal mechanisms to enforce cooperation between independent and executive agencies. If authority is displaced, they believed it would likely be from the FTC regarding privacy.

Discussion and Debate

The discussion delved into the challenges of integrating competition policy, privacy protections, and content moderation within a single agency. Participants debated whether the agency should have jurisdiction over privacy law and content moderation, and how this would interact with existing powers held by agencies like the FTC. Some participants expressed concern about the potential for political interference if the agency were placed within the executive branch, particularly regarding content moderation.

Participants weighed the potential risks of placing the agency within the executive branch against the benefits of a more streamlined decision-making process. They also discussed the integration of privacy into the new agency's scope, considering potential conflicts with existing regulations like HIPAA.

The group explored the EU's approach to competition, where entire market sectors, rather than individual companies, are scrutinized. They considered this model as potentially adaptable for the US, giving the agency the authority to propose structural remedies, such as divestitures, even when no laws are technically violated. Some participants viewed this as a radical but necessary approach to address concentration issues in the tech industry.

The debate also touched on whether the agency should include privacy regulation. Some argued that it could create conflicts between competition and privacy enforcement, while others suggested that combining these areas might be a political necessity, despite the imperfect structure it might create.

Participants emphasized the need for cooperation between the new agency and existing agencies, with some stressing the importance of ensuring that the new agency's expertise receives "substantial weight" from others to prevent conflicts and promote effective coordination.

The group also discussed balancing transparency with effectiveness, with some expressing skepticism about the true independence of any federal agency. They acknowledged the challenges of creating a new agency in the current political environment, with some questioning the feasibility of establishing a regulatory body with broad powers. Participants discussed the potential need for a "coral reef" approach, where the agency fills gaps in existing regulations, though this approach was also criticized for potentially leading to fragmented and ineffective oversight.

Consensus and Disagreement

Participants generally agreed on the need for the new agency to have rulemaking and enforcement authority, along with the ability to conduct deep market research. However, they disagreed on whether the agency should be independent or executive, with some emphasizing the importance of independence for issues like content moderation.

Participants also debated whether privacy regulation should fall within the new agency's mandate. Some argued that privacy should be handled separately to avoid conflicts with competition enforcement, while others felt that combining these areas might be a political necessity.

Concluding Remarks

The session concluded with participants acknowledging that while the structure of the agency is important, the focus should be on its goals, operations, and powers. They recognized that compromises might be necessary, including potentially adopting a "coral reef" approach where the agency takes on various functions not covered elsewhere. Participants agreed that creating this agency would likely require balancing effectiveness with transparency and accountability, and any final decisions would need to consider both legal constraints and political realities.

4. Artificial Intelligence

Overview

The working group on AI explored the potential role of a Digital Regulator in overseeing AI technologies. They examined AI as both a platform and a product, addressing regulatory challenges, accountability, and the scope of a Digital Regulator's authority. The group debated whether AI should be a central responsibility of the new agency or if it falls outside the scope of a Digital Regulator. Participants discussed how AI might be integrated into the agency's remit, distinctions between AI as a platform versus AI used within platforms, and the applicability of existing laws to AI.

Initial Recommendations

The working group presented several key recommendations regarding the interaction between AI and a potential Digital Regulator:

AI as a Platform vs. Product: The group questioned the presupposition of AI as a platform, noting that most AI applications are treated as products. While existing laws generally apply to AI, they suggested adjustments might be necessary to cover unregulated areas.

Regulatory Scope: The group highlighted the need to consider whether vendors to AI companies should fall under existing regulatory authority. Participants stressed the importance of aligning public interest frameworks, such as the draft OMB memo on rights-harming and safety-harming AI systems, with new regulatory approaches.

AI Model Regulation: The group debated whether to regulate AI models or products and discussed the possibility of expanding NIST's remit to develop independent AI safety standards. However, they did not reach a clear consensus on the best approach.

Alternative Agency Structures: The group suggested creating an expert agency with deep AI expertise to consult with other regulators rather than giving a single Digital Regulator expansive regulatory authority over AI. They referenced the National Transport and Safety Authority as an example of an agency that could benefit from such an expert body.

Testing and Safety: The group acknowledged the challenges of regulating AI models, particularly in determining what constitutes a new model for regulatory purposes. Participants recognized the importance of developing rigorous standards and testing mechanisms, potentially through collaboration with agencies like NIST.

Discussion and Debate

Participants debated the feasibility of regulating AI at the model level, given the complexities involved in testing and potential overlaps with existing regulatory frameworks. They discussed whether to regulate AI based on inputs and outputs rather than defining AI as a platform or product.

The group explored the distinction between AI as a standalone platform (e.g., ChatGPT) and AI embedded within existing platforms (e.g., recommendation systems). While most AI applications are treated as products, they debated whether AI should be regulated as a platform or part of broader digital ecosystems.

Participants did not reach a consensus on regulating civil rights and discrimination in AI. Some argued for "red lines" based on existing privacy and civil rights laws, while others emphasized the challenges of revisiting and settling these complex issues.

The group thoroughly debated liability and accountability, particularly the allocation of responsibility between AI developers and deployers. They expressed concerns about potential gaps in accountability, especially with open-source AI models. The discussion also covered the feasibility of regulating AI models versus products, with participants acknowledging the complexity involved, particularly with open-source models.

Some participants supported centralizing AI expertise in a dedicated agency that could consult with other regulators. However, others raised concerns about the risk of such an agency becoming a target for lobbying, similar to other specialized bodies.

The scope of a Digital Regulator's authority over AI was a significant point of debate. Some participants advocated for a narrow focus on issues like competition, privacy, and content moderation, while others suggested a broader mandate might be necessary to address AI's unique challenges. They also discussed whether it is easier for market experts to learn AI concepts or for AI experts to understand market dynamics.

Participants agreed on the importance of holding both developers and deployers responsible for AI-related outcomes, but they noted that the exact mechanisms for this require further exploration.

Consensus and Disagreement

The group generally agreed that while AI regulation is necessary, a Digital Regulator should not be the sole or primary agency responsible for AI oversight. Instead, they suggested that an expert body with specialized knowledge could play a consultative role to assist other agencies in regulating AI within their specific domains.

Participants reached a consensus on the need for clear definitions and standards in AI regulation, particularly in distinguishing between AI platforms and products.

However, they disagreed on how to approach the regulation of AI models versus products. Some argued for a centralized AI regulator, while others believed existing agencies could adapt to these new challenges. The debate on civil rights and discrimination in AI also revealed significant divisions, particularly regarding the practicality of enforcing existing laws in the context of AI technologies.

Concluding Remarks

The session concluded without a clear resolution on several key issues, such as the best approach to regulating AI models and the appropriate scope of a Digital Regulator's authority. Participants acknowledged the complexity of the challenges ahead and suggested that further discussion and consultation would be necessary to refine these recommendations. They emphasized the importance of aligning any new regulatory frameworks with the public interest and adequately addressing the unique risks posed by AI technologies. The session ended with the recognition that more work is needed to determine the appropriate allocation of liability and accountability in AI regulation.

Closing

Final Reflections

The closing session reflected on the discussions from the previous two days and identified next steps for advancing the creation of a specialized Digital Regulator in the United States. Key themes included:

- The complexity of creating such an agency and whether to pursue a broad or narrow regulatory scope.
- The importance of coordination among existing agencies to avoid regulatory gaps.
- The desirability of seeking insights from subject matter experts that work or worked in other executive and independent agencies to tap their expertise and experience.
- The need for flexibility in the regulatory framework to adapt to changing market conditions and technological developments.

Participants recognized that current regulatory systems are inadequate for addressing issues like competition, consumer protection, and the information ecosystem that are unique to digital markets. There was consensus that a flexible, agile Digital Regulator is necessary, but further discussions are needed to define its scope and ensure coordination with existing agencies.

The session concluded with agreement on the importance of ongoing dialogue to refine these ideas as political and technological landscapes evolve.

List of Participants

The Policy Konclave gathered 20+ experts from a range of fields with subject matter expertise relevant to the question. Invitees were also selected to provide diversity of age, race, and gender, as well as profession: invitees included academics, public interest advocates, Hill staffers, current and former government employees, and lobbyists from both large digital platforms and smaller competing platforms. Importantly, invitees participated in their individual capacity as experts, not as representatives of their company or institution. Not all participants attended all sessions of the event. Our participants included:

Charles Duan, Assistant Professor at American University Washington College of Law

Katherina Kopp, Deputy Director at the Center for Digital Democracy

Tom Wheeler, Former Chairman of the Federal Communications Commission

Louisa Imperiale, Chief Advancement Officer at Issue One

Gene Kimmelman, Senior Policy Fellow at the Harvard Kennedy School and Yale's Tobin Economic Policy Center

John Davisson, Director of Litigation & Senior Counsel at EPIC

Christine Bannan, Senior Public Policy Manager at Proton

Matt Perault, Fellow, Center on Technology Policy, New York University

Emma Llanso, Acting Deputy Associate Administrator at the National Telecommunications and Information Administration (NTIA)

Karen Kornbluh, Senior Fellow and Director of German Marshall Fund

Nicol Turner Lee, Director at the Center for Technology Innovation (CTI)

Elizabeth Wilkins, Senior Fellow at the American Economic Liberties Project

Adam Conner, Vice President for Technology Policy at the Center for American Progress

Jeff Van Oot, Policy Advisor at United States Senate

Julie Cohen, Professor of Law & Technology at Georgetown Law Center

Mark MacCarthy, Adjunct Professor at Georgetown University

Aalok Mehta, Responsible AI Policy Lead at Google

Eli Weiner, Legislative Assistant at United States Senate

Liana Keesing, Campaigns Manager, Technology Reform at Issue One

Christabel Randolph, Associate Director at the Center for AI and Digital Policy (CAIDP)

Public Knowledge participants:

Chris Lewis, President & CEO

Harold Feld, Senior Vice President

Lisa McPherson, Policy Director

Final recommendations for the structure, roles, and authorities of the Digital Regulator will be the product of Public Knowledge. Participation in the Policy Konclave in no way implies agreement with the final product.