Columbia World Projects | Thinking Doing Columbia Global

Hertie School Centre for Digital Governance

Digital Platform Governance at a Crossroads

Shruti Das
Graduate Student, Columbia School of International and Public Affairs

Josefina Piddo
Graduate Student, Columbia School of International and Public Affairs

Apolline Ancel
Undergraduate Student, Columbia University and Sciences

A summary of the 2025 Columbia-Hertie Digital Governance for Democratic Renewal conference

On October 30, 2025, Columbia World Projects, in partnership with the Centre for Digital Governance at the Hertie School, convened a conference on "Digital Governance for Democratic Renewal" at the Lee C. Bollinger Forum. Supported by the Knight Foundation, the conference examined the challenges of regulating digital platforms in ways that are both effective and democratically accountable. Across three closed, moderated sessions, tech policy researchers, digital regulators and civil society leaders analyzed how differing legal traditions, geopolitical incentives and institutional capacities shape, and often constrain, platform governance in the United States and Europe. This brief distills key insights from those discussions.

Takeaways

The transatlantic digital divide reflects governance choices.

Participants traced U.S. platform dominance, and its growing fragility, to decades of weakened antitrust enforcement and legislative paralysis, while the European Union has moved toward more assertive, rules-based regulation through the Digital Markets Act and Digital Services Act.

Opacity remains a driver of platform power.

Despite new disclosure and data access requirements, platforms retain unilateral control over what data becomes visible, leaving researchers and regulators with limited insight into systemic harms and reinforcing a baseline condition of extreme opacity.

Traditional antitrust tools are necessary but remain insufficient.

Competition frameworks grounded in narrow economic analysis struggle to address the broader effects of surveillance-based business models on innovation, user rights and democratic institutions, pointing to the need for complementary structural interventions such as interoperability mandates, access obligations and public-utility-style regulation.

Effective regulation depends on institutional capacity and coordination.

Fragmented oversight and under-resourced regulators across jurisdictions suggest that durable progress will require stronger intermediary institutions and sustained coalitions linking policymakers, researchers, technologists and civil society.

Conference Summary

The transatlantic digital divide

Across three conference sessions, participants traced the decline of meaningful U.S. oversight of digital platforms to two intertwined governance failures.

First, they pointed to a *long retreat from anti-monopoly principles*. Beginning in the 1980s, the Reagan administration abandoned decades of strict antitrust enforcement rooted in the New Deal view that concentrated power was inherently suspect. A hands-off approach followed, allowing companies to merge and expand with little oversight. Under this Chicago School market optimism, barriers to entry were treated as insignificant, monopoly was not seen as inherently harmful and the burden of proof for enforcement became increasingly difficult to meet. The internet matured under these permissive conditions, and technology giants learned to exploit them. As one participant put it, **"We have tools that can limit this power. We just haven't used them."**

Second, participants emphasized *legislative paralysis*. Congress has repeatedly identified the problem, most notably in the House's 2020 investigation of competition in digital markets, but has failed to translate those findings into law. Bipartisan antitrust bills advanced out of committee only to stall amid intense lobbying pressure. Participants noted that platforms have mastered regulatory obstruction: money flows, lobbyists mobilize and legislation quietly dies. One described how platforms manipulate user environments to reinforce their dominance: "Tech is flexible. Everything that the consumer experiences is determined by the design of the tech itself."

Meanwhile, the European Union has moved more decisively. The Digital Markets Act (DMA) and Digital Services Act (DSA) represent the most ambitious effort to date to curb excessive platform power, introducing obligations, prohibitions, systemic risk assessments and access rules for designated gatekeepers. In early December, Brussels issued its first DSA fine, penalizing X for transparency failures and misleading verification practices. The move prompted the company's owner to denounce the action as censorship and delete the European Commission's X ad account.

A turn to digital antitrust?

Both jurisdictions, particularly the United States, have relied heavily on litigation. With Congress gridlocked, filing lawsuits has often proved procedurally easier than advancing contested legislation. During the first Trump administration, and continuing through the Biden administration, prosecutors pursued a broad slate of antitrust actions against major platforms, including Justice Department lawsuits targeting Apple's smartphone ecosystem and Google's search and ad tech businesses, as well as the Federal Trade Commission's challenge to Meta's acquisitions of Instagram and WhatsApp. Federal courts have since ruled Google a monopoly three times. As one participant noted, **"Despite a flurry of lobbying, including from Mark Zuckerberg personally, the White House has not withdrawn the major antitrust cases. For a company like Meta, this is a big deal."**

These efforts have not produced decisive outcomes. Behavioral remedies proposed in the Google search case in September were widely viewed as inadequate, and the dismissal of the Meta case two months later underscored the difficulty of challenging platform power through the courts alone.

Participants emphasized that surveillance-based advertising continues to fuel scale and lock-in. As long as large-scale data extraction remains lightly constrained, enforcement victories when they occur, only nibble at the edges of platform power. As one participant put it, **"The internet did not kill the news. Platformization and consolidation did. These are not technology companies. They are digital advertising firms that have developed more intense forms of surveillance."**

As a result, many called for reviving other regulatory tools, including public utility-style obligations, structural separation and clearer oversight mandates. One participant argued that governing cloud infrastructure like a public utility would prevent firms from operating across incompatible lines of business, while another cautioned that without enforceable pricing rules, such models risk reinforcing dominance rather than dismantling it.

Such hybrid measures, the group agreed, are necessary to rebuild democratic resilience in digital markets and to prevent power from remaining concentrated in a handful of private platforms. As one participant warned in the closing session, **"We talk about democratic renewal, but we need to worry about democratic survival."**

Privacy and transparency: a baseline of opacity

Platform-to-researcher data access emerged as a concrete illustration of digital power in practice, shaping who collects data, who can study it and who remains shielded by opacity. During the 2019–2020 congressional antitrust investigation into digital markets, researchers could not obtain even basic platform data, prompting proposals such as the **ACCESS Act**. Privacy advocates raised legitimate concerns at the time, asking how data could be shared safely without a comprehensive federal privacy law.

Participants challenged the assumption that privacy and transparency are inherently opposed. Instead, the real task at hand is meaningful institutional design. Responsible data-sharing models are possible, particularly when built on privacy-enhancing technologies (PETs) and privacy-preserving tools (PPTs). These approaches can enable vetted research access while minimizing exposure of individual-level data, shifting the central question from "privacy versus transparency" to how systems can advance both simultaneously.

Even as privacy tools improve, platforms retain unilateral control over **what counts as "public" data** and how much operational or financial information becomes visible. Under Article 14 of the DSA, large platforms must provide data access to vetted researchers. Early enforcement experiences, however, suggest that disclosures are often minimal, highly aggregated or strategically opaque. Revenue breakdowns, system architecture and metrics necessary to assess systemic harms remain largely inaccessible. The result is a baseline of extreme opacity, in which modest gains in transparency appear as major victories but still fall short of democratic oversight needs. A **delegated act** published in July 2025 seeks to standardize broader access, but its effectiveness will hinge on the capacity and political will of EU Digital Services Coordinators (DSCs), the national agencies responsible for DSA enforcement.

Portability vs. interoperability

Across the European Union, the United Kingdom and the United States, regulators are experimenting with tools that govern personal data and system design. A recurring theme was the need to clearly distinguish between portability, which allows users to move data from one service to another, and interoperability, which enables systems to work together in real time. Conflating the two risks weak enforcement and missed opportunities. Participants emphasized that portability can facilitate user exit from platforms, while interoperability reshapes markets by enabling entry, multihoming and competition, thus dampening the network effects that entrench incumbents. Each requires distinct legal frameworks, technical standards and enforcement strategies, and both are necessary to shift power away from dominant gatekeepers.

Momentum is nonetheless building. In Europe, the DMA's data portability provisions, described by one participant as "the least contested" elements of the law, are taking effect. In the United Kingdom, the **Smart Data initiative** was cited as opening new pathways for personal data access across sectors. In the United States, a growing number of state-level digital choice laws aim to give users greater control over how their data moves between services.

As these regimes develop, participants stressed that trust has become the central barrier to adoption. Data transfers increasingly fail not because of technical limitations but because users, developers and regulators lack confidence in how data will be handled once it moves. The rise of AI agents heightens these stakes. In an AI-mediated ecosystem, users risk becoming locked into a single tool simply because their history and preferences are embedded within it.

Institutional capacity and coalition building

Participants emphasized that understanding where power sits in the platform data access ecosystem requires mapping overlapping layers of control that extend far beyond Silicon Valley boardrooms. Congressional committee staff, for instance, are catastrophically under-resourced. The House Energy and Commerce Committee, which oversees the technology sector, may have only one or two dedicated technology staff members among dozens covering energy, telecommunications, pharmaceuticals and consumer safety. As one participant noted, privacy issues often become the default focus not because they are most urgent, but because overextended staffers are instructed to prioritize them amid limited capacity.

This resource gap creates cascading failures. States face constraints under the **Interstate Commerce Clause** and cannot easily reference international standards for platform regulation. While the United States relies on the National Institute of Standards

and Technology (NIST) for broad technical guidance, it lacks a well-resourced institution dedicated specifically to platform governance comparable to EU sector-specific bodies. Key oversight offices operate with a handful of staff despite handling sensitive data protections. One former senior staff member noted that only three people at the Department of Health and Human Services oversee all certificates of confidentiality, the primary mechanism researchers use to block government subpoenas for sensitive data.

Research oversight structures also remain misaligned. Institutional Review Boards (IRBs) operating under the Common Rule often treat platform and social media research as analogous to biomedical or survey research, limiting their ability to assess risks associated with large-scale behavioral data, recommender systems and algorithmic exposure. This approach leads to an overemphasis on individual consent while providing few tools to evaluate systemic harms.

Across the Atlantic, DSCs possess formal authority but often lack the capacity to translate research findings into policy or to mediate between academic communities and political decision-makers. Participants stressed that without dedicated translation functions and sustained relationships among regulators, researchers and civil society, even strong legal mandates may underperform.

Consequently, participants noted that the core challenge is not enforcement capacity alone but coalition building. Effective governance will require alliances linking under-resourced staff members, researchers, technologists and advocates across jurisdictions. Some urged the creation or the strengthening of existing intermediary institutions, including data trusts, research consortia and standing advisory bodies, to aggregate expertise, negotiate access and provide policymakers with credible, actionable evidence.

The imagination deficit

Discussions of public-ready AI infrastructure pointed to a recurring absence: product managers and machine learning researchers. While they shape system behavior, they rarely sit at the center of policy conversations. Participants noted that many individuals within large technology firms seek better outcomes, but current legal and institutional arrangements give them few realistic ways to act on these commitments, especially when whistleblowing laws and internal protections remain weak.

In turn, the group called for two shifts. The first is *articulating affirmative goals*, including benchmarks for systems and social outcomes that public-interest AI should advance. The second is *creating institutional structures that make ethical action easier than expedience*, including protections for internal dissent and safe channels to raise concerns without career-ending consequences.

As one participant put it, **"We don't have the people in this room to answer questions about power,"** underscoring how concentrated control over data, infrastructure and expertise sidelines those best positioned to challenge it. Participants linked this imagination deficit directly to market concentration: when a small number of platforms define defaults for AI and digital services, alternative models, including public, cooperative or commons-based approaches, struggle to register as plausible contenders.

An uncertain future

Participants agreed that the system in which a small number of U.S. firms control global digital infrastructure is under strain, even as viable alternatives remain uncertain.

Some identified openings at the international level. Without the persistent threat of tariffs, countries could revisit anti-circumvention laws such as Section 1201 of the Digital Millennium Copyright Act, which criminalizes bypassing technological restrictions on products consumers own and which the U.S. has promoted abroad through a range of pressure tactics.

Others focused on the security risks this concentration poses for sovereign states. In The Hague, Microsoft terminated the International Criminal Court prosecutor's accounts after President Trump denounced an arrest warrant, erasing email archives and working files. In Crimea, Russian forces stole Ukrainian tractors only to have John Deere remotely disable them.

Participants noted that any actor with leverage over these companies can disrupt critical systems worldwide.

Seven tech giants now comprise more than 30% of the S&P 500. According to one participant, these companies **"Spend $700 billion in capital expenditures that, using their own extremely dubious accounting, generate $60 billion a year."** The economics are troubling, with several noting that **each new generation of AI technology costs more to operate while each additional customer often increases losses**. DeepSeek's recent demonstration of comparable performance using far less computing power suggested that prevailing models may not be inevitable.

Throughout the day, participants returned to a set of unresolved questions: Will substantive regulation take hold? Will antitrust cases produce meaningful structural change? Will other countries seize the opportunity to build alternativedigital systems? And what happens if the AI investment bubble bursts, leaving behind an industry that has spent itself into a crisis larger than that of 2008?

One conclusion was clear. The problems shaping the digital ecosystem are structural, and structural problems demand structural solutions. Transparency requirements, interoperability mandates, limits on cross-market leverage, access obligations, public options and business model restrictions must operate together as a unified policy toolkit. As participants emphasized, competition policy does more than shape markets; it also safeguards democratic resilience.

For years, Silicon Valley's dominance appeared unassailable. For the first time in recent memory, that assumption is being tested. The giants remain giants, but they now operate in an environment that is far less predictable.