

Governance of Visibility: How Social Media Interfaces Allocate Power

Zach Bastick

European University Institute & Harvard University

zach.bastick@eui.eu

May 2025 Preprint

Abstract

This article develops a theoretical account of digital platforms as infrastructures and advances the concept of governance of visibility - the strategic control over who can observe, measure, and know platformed publics. Bringing infrastructure studies into dialogue with critical political economy and platform governance, this paper argues that interface decisions (such as APIs, research tools, rate limits, and eligibility rules) act as infrastructural choke points that reallocate epistemic power under digital capitalism. Two recent trajectories - X's paywalled API and Meta's retirement of CrowdTangle - illustrate how visibility has been enclosed and monetized, with downstream effects for public-interest research and accountability. The paper then theorizes counter-infrastructures, mapping the distinct characteristics of dependent and independent counter-infrastructures. The discussion specifies design and policy levers, focusing on the EU Digital Services Act (DSA) Article 40 regime on vetted researcher access and the challenge of turning transparency from corporate favor into enforceable right. Findings are drawn from work undertaken during the EU-funded DIGIPOL project.

1. Introduction

In 2023, Twitter (now X) ended research-viable free access to its API and introduced costly tiers and tighter rate limits. Research centers and scholars publicly warned that the change would curtail a variety of public-interest uses - including crisis informatics, misinformation monitoring, and longitudinal audits - and could mark the end of an era for platform transparency (Freelon, 2018; Tromble, 2021). Many also described how pricing and terms made population-scale observation unaffordable for public institutions and initiatives (Newton, 2023). Some scholars argue that the cumulative effect has been to chill independent oversight by narrowing who can measure the platform at scale (Starbird, 2019; Tromble, 2021).

Likewise, in 2024, Meta decommissioned CrowdTangle, a widely used instrument for observing content diffusion on Facebook and Instagram. Although Meta introduced a replacement (the Content Library/API), journalists and watchdog organizations criticized reduced real-time observability and limits on eligibility, especially during election periods (Associated Press, 2024; Tow Center for Digital Journalism, 2024). Open letters urged Meta to maintain CrowdTangle through major election cycles (Tow Center for Digital Journalism, 2024).

This article makes sense of these developments by theorizing social media as infrastructures of digital capitalism. Rather than analyzing only ranking or moderation decisions, we foreground interfaces - APIs, research tools, documentation, rate limits, and eligibility rules - as infrastructural choke points through which platforms enact governance of visibility. We define 'governance of visibility' as the strategic control over the means of observability: who can see, at what granularity and latency, and under what legal and financial terms.

The findings from this paper are drawn from the «Digital Observatory of Political Discourse» (DIGPOL), an EU funded project seeking to provide transparency into speech controlled by highly used corporate platforms. The paper theorizes social platforms as infrastructures within digital capitalism, explores the mechanisms through which interfaces govern visibility and constrain public oversight, and examines the rise of counter-infrastructure as it exists today. It then situates this within recent EU legislative developments.

2. Theoretical framework: Platforms as infrastructures in digital capitalism

Infrastructure studies has conceptualized infrastructures as embedded, standardized, and often invisible systems that become visible at breakdown (Star, 1999). They are relational backbones that enable action across sites and scales; their politics are inscribed in standards, gateways, and dependencies. Reading social media as infrastructure foregrounds upstream control points - identity systems, schemas, developer policies, and interfaces - that are usually backgrounded when we only analyze feeds and moderation. Plantin and colleagues capture a contemporary shift as a dual movement: the infrastructuralization of platforms and the platformization of infrastructures (Plantin et al., 2018). Large platforms (e.g., Google, Facebook) acquire infrastructural characteristics - ubiquity, reliability, standard-setting - while traditional infrastructures adopt platform logics. The infrastructural lens matters because infrastructural status historically carried public obligations (interconnection, nondiscrimination, continuity, legibility). When private platforms perform infrastructural roles, interface decisions become matters of public concern (Plantin et al., 2018; Star, 1999).

In parallel, critical political economy explains why infrastructural control over interfaces is central to platform power. Srnicek (2017) situates platforms as intermediaries that extract data and generate network effects, turning ecosystem control into rents. Under this logic, programmability is valuable when it scales the ecosystem, but enclosure is attractive when it preserves proprietary advantage and turns access itself into a revenue line. Zuboff (2019) emphasizes asymmetric visibility: the unilateral capture of behavioral data behind corporate opacity. Platforms build one-way mirrors - near-omniscience over users and publics, themselves having minimal legibility about internal operations - so that prediction and control can be monetized. The enclosure of visibility (what outsiders can know) is thus not peripheral; it is constitutive of the accumulation model. Couldry and Mejias (2019) extend the critique historically: contemporary extraction reorganizes social life so that human experience becomes a continuous input to capital - an appropriation of life through data relations. In short, decisions to close or price APIs, retire tools, or vet researchers are not solely technical or policy decisions, but they are political-economic acts: they privatize the means of observation, protecting accumulation by limiting counter-knowledge (Couldry & Mejias, 2019; Srnicek, 2017; Zuboff, 2019).

Platform governance scholarship shows how firms curate content visibility (ranking, moderation) while presenting themselves as neutral “platforms” (Gillespie, 2010; Gorwa, 2019). We extend this to institutional visibility: who is permitted to see the platform itself - its data flows, interventions, and systemic risks. Pasquale (2015) warns that formal transparency can be performative and insufficient; complex systems can remain unintelligible without institutional arrangements that ensure independence, completeness, and contestability. Ananny and Crawford (2018) similarly argue that accountability is a sociotechnical process, not a property of a dataset or code dump. These insights motivate a conceptual shift from the generic “transparency” often cited in the literature to a governance of visibility.

3. The need for a governance approach

Between February and May 2023, Twitter/X ended research-viable free access, tightened endpoints and rate limits, and rolled out paid tiers whose enterprise pricing exceeded many academic budgets (Newton, 2023). Likewise, in August 2024 Meta retired CrowdTangle, replacing it with the Content Library/API. Journalists, watchdog organizations, and officials criticized the timing (election cycles) and scope (eligibility limits; reduced real-time features), and coalitions urged Meta to maintain CrowdTangle through 2024-2025 (Associated Press, 2024; Tow Center for Digital Journalism, 2024). Meta's replacement may improve access for vetted researchers but curtails a public-facing transparency instrument used by newsrooms and civil society.

Scholars cited impacts on crisis response, misinformation monitoring, and longitudinal analyses (Freelon, 2018; Tromble, 2021). Some scholars argue that the cumulative effect has been to chill independent oversight by making population-scale observability contractually constrained or unaffordable (Starbird, 2019; Tromble, 2021). From a framework of governance of visibility, these developments recalibrate the visibility regime through pricing, throughput controls, and legal constraints. Small-N audits remain possible, although mediated by algorithmic obscurity, but large-scale, real-time analysis becomes a paid privilege governed by terms the platform can change unilaterally. The net result is a redistribution of epistemic power toward the platform and its chosen partners. From our framework, tool deprecation resets the measurement instrument and moves visibility into a more curated channel. Even where replacements exist, latency, granularity, and eligibility are re-specified by the firm, shifting oversight from open instrumentation to a gated portal.

There are multiple modalities through which platforms govern visibility. These including pricing and rate-limit regimes, such as volume and throughput caps, which transform observability into a commodity, selectively affordable for well-resourced actors (Newton, 2023); Qualification and vetting, notably through access regimes delineate eligible observers, often with publication constraints; tool deprecation and substitution, which as in CrowdTangle, collapses measurement ecologies; and through terms of service modifications, which undermine reproducibility and add legal risk to independent data collection (Freelon, 2018; Tromble, 2021).

Much public debate demands 'transparency' in online information ecosystems, but Pasquale (2015) shows that firms can satisfy transparency formally while defeating intelligibility (e.g., through selective disclosure, complexity, or NDAs). Ananny and Crawford (2018) recommend building institutional conditions for understanding - independence, replicability, and the ability to publish. Governance of visibility identifies the infrastructural locus (interfaces and associated rules) where such institutional guarantees must attach if transparency is to be meaningful.

4. Counter-infrastructures

This paper theorizes counter-infrastructure as any sociotechnical arrangement that seeks to *redistribute observability, control, and the capacity to intervene* away from incumbent platforms and toward publics, researchers, or communities. Building on infrastructure studies, counter-infrastructures can be read as attempts at infrastructural inversion - making the pipes and protocols of platformized communication newly visible and governable (Bowker & Star, 2000; Star, 1999). They also resonate with work on protocol politics, recursive publics in free and open-source cultures (Kelty, 2008), and media-infrastructure scholarship that treats pipes, standards, and gateways as sites of power and contestation (Plantin et al., 2018). In our framework, counter-infrastructures are not merely alternatives to "interfaces"; they are alternative visibility regimes designed to modify who gets to see platformed publics, with what granularity, latency, and independence.

Two dimensions help organize the landscape. First, dependency on incumbent interfaces: to what extent does a counter-infrastructure rely on the technical and legal affordances of dominant platforms (APIs, ToS carve-outs, tolerated scraping) versus operating on independent rails? Second, governance model: is the arrangement oriented to public interest/commons governance (e.g., scholarly oversight, community norms, protocol standards) or to partisan/ideological enclosure? These axes yield different failure modes vis-à-vis the governance of visibility elaborated earlier: dependency concentrates risk in corporate revocation; independence often trades centralized legibility for fragmented observability; and ideological forks may secure autonomy while narrowing accountability across publics (Benkler et al., 2018).

This paper also proposes three evaluative criteria, aligned with our theoretical aims: (a) independence (freedom from incumbent veto and capture), (b) coverage (ability to observe the arenas where publics actually assemble), and (c) continuity (stability and reproducibility of access over time). No family maximizes all three simultaneously.

Dependent counters operate on incumbent rails—through public APIs, research access programs, or tolerated scraping—to instrument platforms for public oversight. Examples include academic dashboards, watchdog pipelines, and newsroom tools that reconstruct content flows, engagement dynamics, and amplification patterns. Methodologically, they align with audit traditions that infer platform behavior from inputs/outputs (Sandvig et al., 2014), and with computational communication practices adapted to the “post-API” era (Freelon, 2018). Their democratic value lies in comparability and reach: because they observe the dominant arenas of discourse, they can evidence harms and effects at scale. Yet this very dependence exposes a structural fragility. As Bruns (2021) shows, the “APIcalypse” marks a broader turn in which platforms narrowed endpoints, raised costs, or retired data surfaces, shifting researchers from relatively open programmability to contingent, revocable access. Meta’s retirement of CrowdTangle - long a de facto public observability instrument - and Twitter/X’s paywalled API exemplify how visibility can be rescinded unilaterally, reasserting what we elsewhere term *infrastructural capture* (Bruns, 2021; Freelon, 2018).

Within the governance of visibility, dependent counters thereby sit at a paradoxical nexus: they can deliver high coverage and strong continuity *until* a policy or pricing change converts visibility into a corporate asset. Mitigations—legal entitlements to data (e.g., vetted researcher access regimes), redundancy across data sources, and publication independence - seek to re-publicize this visibility, but until such guarantees are enforceable, dependent counters remain foreclosure-prone (Ananny & Crawford, 2018; Pasquale, 2015).

Protocol counters relocate social networking off incumbent allowances and onto open, federated structures, thereby redistributing infrastructural chokepoints. Two prominent designs illustrate the strategy. ActivityPub (a W3C Recommendation) powers the Fediverse (e.g., Mastodon) via client-server and server-server federation, with governance distributed at the instance level through community norms, codes of conduct, and block/allow lists (W3C, 2018). AT Protocol/Bluesky modularizes the stack into Personal Data Servers (identity/graph portability), relays (a “firehose” of events), app views and custom feeds, and labelers for distributed moderation, explicitly designing for forkability and exit (Bluesky, 2024). The theoretical import is twofold. First, protocols instantiate governance-by-design: rules are embedded in standards and reference implementations rather than centralized corporate policy (fPlantin et al., 2018). Second, they relocate visibility governance from a single platform to a mesh of actors - instances, relay operators, client developers, and standards bodies—potentially reducing the risk of unilateral foreclosure.

However, autonomy introduces observability dilemmas. In the Fediverse, logs are fragmented across instances; federation is selective and dynamic; and research ethics (consent, scraping norms, cross-instance aggregation) vary and remain contested (Wähner et al., 2024). In AT Protocol's early federation, the practical topology of data flows is shaped by which relays are active and which allowlists are in force, raising questions about where new chokepoints emerge (Bluesky, 2024). Protocol counters thus tend to maximize independence and, once mature, continuity, but trade away canonical telemetry: there is no single vantage point from which to reconstruct system-wide dynamics.

For the governance of visibility, the implication is that observability must be co-governed—through shared research feeds, common event schemas, opt-in aggregation, and federated ethics—rather than dictated by a single firm. In short, protocolization resists enclosure but demands new institutions of measurement and consent (Plantin et al., 2018; Wähner et al., 2024).

A third family comprises ideological or forked counters (e.g., Gab, Truth Social): autonomous stacks that minimize dependency on incumbents by building parallel hosting, moderation, and distribution infrastructures. In infrastructural terms, they succeed at independence and often continuity (no incumbent can “turn off” access). Yet they typically produce sectarian visibility—publics that are internally legible while opaque across ideological boundaries—thereby narrowing accountability and complicating cross-public verification (Benkler et al., 2018; Marwick, 2018). The literature on asymmetric ecosystems shows how such enclaves can stabilize parallel knowledge infrastructures with distinct epistemic authorities, amplification networks, and incentives, reducing the *bridge visibility* needed for democratic contestation (Benkler et al., 2018). From our perspective, these counters demonstrate that autonomy is not equivalent to publicness: infrastructural independence can coexist with visibility narrowing that undermines the broader conditions of accountability.

5. Legislative paths

The DSA Article 40 delegated act aims to convert data access for vetted researchers from benevolence to entitlement, clarifying documentation, formats, and the role of Digital Services Coordinators, and announcing a data-access portal (European Commission, 2025). To align with our framework, three guardrails are crucial: independence (no NDAs on core findings; freedom to publish), reproducibility (versioned datasets; changelogs), and timeliness (latency limits; service-level expectations enforceable by regulators). Implementation risks - vetting criteria, privacy safeguards, platform under-delivery - will determine whether Article 40 yields intelligible transparency rather than compliance theater (Ananny & Crawford, 2018; Pasquale, 2015). For protocols, communities should co-design opt-in research feeds, ethical guidelines for cross-instance aggregation, and mechanisms that respect blocklists while enabling federated observability (Wähner et al., 2024; W3C, 2018).

Public funders should back independent observatories and data trusts not reliant on platform grants. Journals should require methodological disclosures on data provenance, access constraints, and versioning so reviewers can assess dependency risks. Civil society coalitions can align transparency demands across jurisdictions and election cycles, amplifying accountability beyond single-firm arenas (Gorwa, 2019; Pasquale, 2015).

6. Conclusion

Treating social platforms as infrastructures clarifies that governance is not only about content rules or ranking tweaks; it is fundamentally about who is permitted to see the system at scale, at what cadence and cost, and with what independence to publish. API paywalls, tool deprecations, vetting programs, and policy churn are infrastructural levers by which platforms govern visibility, privatizing the means of observation and, with it, much of the capacity for public oversight.

Counter-infrastructures exist and matter. Dependent dashboards scale oversight but are foreclosure-prone; protocol alternatives resist foreclosure but complicate observability; ideological forks illustrate how infrastructural independence can coincide with narrowed public accountability. Regulation - exemplified by the DSA Article 40 regime - points toward a public reassertion over visibility governance, but realization will hinge on whether intelligibility (independent, reproducible, timely access) is achieved in practice.

Taken together, the three families reveal a trilemma for counter-infrastructures under digital capitalism: one can reliably maximize at most two of independence, coverage, and continuity. Dependent counters deliver coverage and continuity until infrastructural capture revokes access; protocol counters deliver independence and, eventually, continuity but face coverage and legibility challenges absent shared observability primitives; ideological forks deliver independence and continuity within enclaves while sacrificing cross-public accountability. Recognizing this trilemma clarifies why policy and standards—from enforceable research-access rights to protocol-level observability conventions—are necessary complements to technical design. Counter-infrastructures can redistribute who gets to see; only institutional guarantees can stabilize that redistribution over time (Ananny & Crawford, 2018; Pasquale, 2015; Plantin et al., 2018).

The core theoretical move is to center governance of visibility - the infrastructural allocation of the right to know - within digital capitalism. If visibility remains privatized, oversight persists as a patchwork of keyholes. If visibility is re-publicized, through enforceable access rights, technical observability primitives, and independent institutions, we can rebuild the epistemic conditions for democratic accountability in a platformed public sphere.

Funding statement

Funded by the European Union. Views and opinions expressed are, however, those of the author only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.



References

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3), 973–989.
<https://doi.org/10.1177/1461444816676645>

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Bluesky PBC. (2024). *AT Protocol: Federation architecture* (developer documentation).
<https://docs.bsky.app/>

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT press.

Bruns, A. (2021). After the 'APIcalypse': Social media platforms and their fight against critical scholarly research. *Disinformation and data lockdown on social platforms*, 14-36.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

European Commission. (2025, July 2). *Delegated act on data access under the Digital Services Act (DSA)* [Commission Delegated Regulation C(2025) 4340 final]. <https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa>

Freelon, D. (2018). Computational research in the post-API age. *Political Communication*, 35(4), 665–668. <https://doi.org/10.1080/10584609.2018.1477506>

Gillespie, T. (2010). The politics of “platforms.” *New Media & Society*, 12(3), 347–364. <https://doi.org/10.1177/1461444809342738>

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, 22(6), 854–871. <https://doi.org/10.1080/1369118X.2019.1573914>

Kelty, C. M. (2008). *Two bits: The cultural significance of free software*. Duke University Press.

Marwick, A. E. (2018). Why do people share fake news? A sociotechnical model of media effects. *Georgetown Law Technology Review*, 2(2), 474–512.

Ortutay, B. (2024, August 14). Meta kills off CrowdTangle despite pleas from researchers and journalists. *AP News*.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310. <https://doi.org/10.1177/1461444816661553>

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2014, May). Auditing algorithms: Research methods for detecting discrimination on internet platforms. In *Data and Discrimination: Converting Critical Concerns into Productive Inquiry* (ICA 2014 preconference), Seattle, WA. <http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf>

Srnicek, N. (2017). *Platform capitalism*. Polity.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377–391. <https://doi.org/10.1177/00027649921955326>

Starbird, K. (2019). Disinformation's spread: Bots, trolls and all of us. *Nature*, 571(7766), 449. <https://doi.org/10.1038/d41586-019-02235-x>

Gotfredsen, S. G., & Dowling, K. (2024, July 9). Meta is getting rid of CrowdTangle—and its replacement isn't as transparent or accessible. *Columbia Journalism*. https://www.cjr.org/tow_center/meta-is-getting-rid-of-crowdtangle.php

Tromble, R. (2021). Where have all the data gone? A critical reflection on academic digital research in the post-API age. *Social Media+ Society*, 7(1), 2056305121988929.

W3C. (2018). *ActivityPub* (W3C Recommendation). <https://www.w3.org/TR/activitypub/>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Calma, J. (2023, May 31). Twitter just closed the book on academic research. *The Verge*.

<https://www.theverge.com/2023/5/31/23739084/twitter-elon-musk-api-policy-chilling-academic-research>