The Administrative Architecture of Scientific Trust

Pre-Content Filtering and Institutional Email in Digital Research Platforms

Florian Morin
Independent Researcher
quietexclusion.org
ORCID: 0009-0004-7301-8524

Mai 15, 2026

Abstract

Scientific platforms increasingly rely on institutional affiliation as a low-cost trust signal for managing moderation, verification, spam prevention, and reputational risk at scale. This paper introduces the concept of *pre-content filtering*, in which infrastructural trust proxies, particularly institutional email domains, influence access before scientific content itself is evaluated. Across repositories, preregistration systems, and research platforms, institutional emails frequently function as mechanisms of accelerated access and reduced verification burden, while personal email domains are associated with additional friction such as manual review, delays, or verification requests.

The paper further proposes the concept of *normalized quiet exclusion*, a form of status-based filtering embedded within ordinary administrative procedures and presented as operationally neutral. Rather than operating through explicit rejection, these systems produce cumulative access asymmetries that mechanically favor institutionally affiliated researchers through reduced infrastructural uncertainty and moderation cost.

1 Introduction

Scientific platforms increasingly rely on institutional affiliation as a low-cost trust signal for managing moderation, verification, spam prevention, and reputational risk at scale (Gillespie, 2018; Striphas, 2015).

Building on previous work on infrastructural asymmetry in scientific participation (Morin, 2026), this paper introduces the concept of pre-content filtering, in which infrastructural trust proxies, particularly institutional email domains, influence access before scientific content itself

is evaluated. Across repositories, preregistration systems, and research platforms, institutional emails frequently function as mechanisms of accelerated access and reduced verification burden, while personal email domains are associated with additional friction such as manual review, delays, or verification requests. The claim is not that institutional-email filtering is always illegitimate, but that it relocates scientific access from epistemic assessment to infrastructural compatibility.

Institutional affiliation operates as a shallow but scalable trust heuristic. This is consistent with broader analyses of digital governance infrastructures in which scalable administrative systems increasingly rely on compressed trust proxies and probabilistic classification mechanisms under conditions of high moderation complexity (Amoore, 2020; Greene, 2021). While institutional email domains do not directly guarantee scientific quality, methodological rigor, or honesty, they substantially reduce administrative uncertainty and moderation cost within large-scale digital infrastructures.

The paper proposes the concept of normalized quiet exclusion, a form of status-based filtering embedded within ordinary administrative procedures and presented as operationally neutral. Rather than operating through explicit rejection, these systems produce cumulative access asymmetries that mechanically favor institutionally affiliated researchers through reduced infrastructural uncertainty and moderation cost (Star, 1999; Bowker & Star, 2000).

Clarification of Scope

The paper does not argue that scientific platforms are intentionally attempting to exclude independent researchers. Rather, it argues that modern scientific infrastructures increasingly rely on pre-content trust estimation mechanisms designed to reduce moderation burden, spam risk, fraud exposure, and verification uncertainty at scale. Under these conditions, institutional affiliation functions as an administrative trust proxy that accelerates onboarding, reduces verification friction, and stabilizes infrastructural legitimacy prior to epistemic evaluation itself.

The resulting asymmetries therefore emerge less through explicit ideological exclusion than through cumulative differences in administrative fluidity. Researchers possessing institutionally legible trust markers, such as university email domains, indexed publication histories, or established scholarly traces, inherit reduced infrastructural uncertainty within moderation systems. Independent researchers, by contrast, may remain epistemically legitimate while encountering greater verification burden, onboarding friction, or procedural instability due to reduced infrastructural legibility.

The resulting asymmetry is therefore not one of absolute exclusion. Independent researchers frequently retain access to lower-friction or less selective infrastructures such as OSF, Zenodo, or personal dissemination channels. However, access to higher-visibility or more institutionally validated scientific environments may remain comparatively more difficult due to increased verification requirements, infrastructural trust thresholds, and moderation uncertainty. Under these conditions, independent researchers are not necessarily excluded from scientific participation itself, but may encounter greater difficulty escaping zones of lower institutional validation and reduced epistemic visibility.

2 Access as Administrative Progression

Access within digital scientific infrastructures is not reducible to a binary distinction between acceptance and rejection. Instead, access can be conceptualized as a multi-stage process composed of successive administrative conditions:

$$\text{Access} = \text{Entry} \times \text{Progression} \times \text{Completion} \times \text{Persistence}$$

Similar infrastructural asymmetries have been described in studies of platform governance and digital access systems, where administrative fluidity becomes unevenly distributed across users possessing different institutional trust markers (Greene, 2021).

Under this framework, scientific participation depends not only on initial registration or formal permission to use a platform, but also on the ability to continuously progress through verification

systems, moderation procedures, infrastructural requirements, and long-term account stability.

Institutional affiliation functions as a compression mechanism across each stage of this process. Institutional email domains reduce administrative uncertainty during entry, accelerate progression through verification systems, facilitate completion of submission procedures, and increase persistence by stabilizing trust within moderation infrastructures. Conversely, personal email domains frequently introduce cumulative friction through manual review, delayed access, repeated verification requests, elevated anti-spam suspicion, or instability of platform trust.

Importantly, these frictions often operate prior to scientific evaluation itself. Access may therefore collapse without explicit rejection when one or more administrative stages become sufficiently unstable or costly. In this sense, modern scientific infrastructures increasingly regulate participation through differential administrative fluidity rather than overt exclusion.

Hierarchical Legitimacy Across Scientific Infrastructures

In practice, scientific dissemination infrastructures are not epistemically equivalent. Certain platforms, repositories, affiliations, and publication channels function as high-legitimacy environments whose outputs are more readily integrated into academic visibility systems, citation networks, institutional evaluation, and future access pathways. Others remain implicitly categorized as peripheral, informal, or lower-trust dissemination zones despite allowing technically valid scientific distribution.

Under these conditions, independent researchers may retain the ability to disseminate work through permissive infrastructures while simultaneously encountering difficulty accessing environments carrying stronger institutional legitimacy signals. The resulting asymmetry is important because the hierarchy between platforms is not merely descriptive but cumulative: visibility, trust, discoverability, moderation fluidity, and future access increasingly depend on prior presence within already legitimized infrastructures.

Consequently, even potentially strong or original independent work may remain structurally confined to lower-validation dissemination layers, not necessarily because of direct epistemic rejection, but because infrastructural legitimacy itself becomes recursively distributed through pre-existing institutional recognition.

3 Pre-Content Filtering

A central feature of modern scientific infrastructures is that filtering mechanisms increasingly operate before scientific content itself is evaluated. Rather than initially assessing protocols, manuscripts, or methodological quality, platforms frequently rely on administrative trust proxies during early access stages. This process can be described as *pre-content filtering*.

The most revealing aspect of these systems is often the neutrality of their administrative

language. Terms such as “verification purposes”, “false-positive”, “institutional email”, or “help you out” frame the restriction as a routine procedural safeguard rather than an exclusionary act, see Figure 1. Yet in some cases, the filtering process is fully automated at the account level, with no manual review, no evaluation of scientific content, and no assessment of methodological quality or expertise. Importantly, these mechanisms appear within preregistration and open science infrastructures that are explicitly designed to expand transparency and accessibility in scientific research.

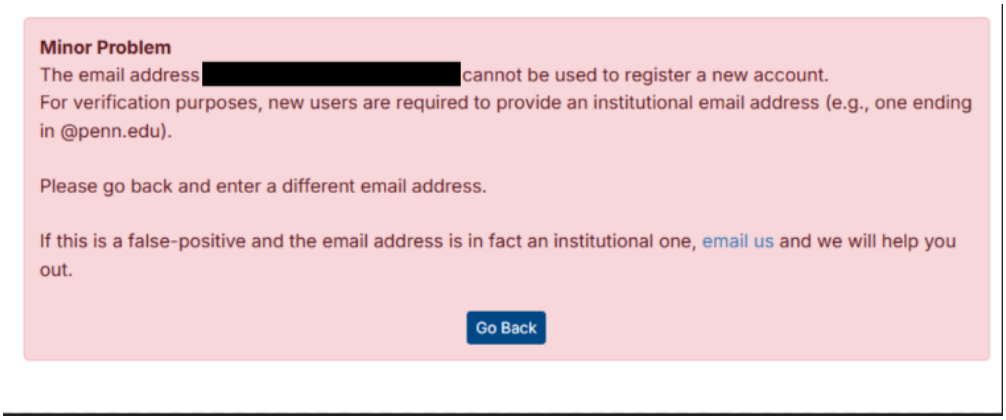


Figure 1: AsPredicted: "Minor Problem"

Under these conditions, the institutional email address effectively becomes a gatekeeping mechanism operating before scientific participation itself begins. The protocol is not visible, the idea has not been read, and the scientific contribution has not been evaluated. Filtering occurs entirely through administrative trust estimation.

Figure 2 presents the response received from AsPredicted following a request for clarification regarding the platform’s policy toward non-institutional email addresses and publication-based exceptions.

AsPredicted moderation response regarding non-institutional email addresses and publication-based exceptions

> Hi Florian,
>
> We are currently exploring third party identity validation options and plan to implement this summer, but for the moment we do not accept non-institutional email addresses. We make exceptions when people have published papers using their non-institutional email addresses. If this doesn’t apply to you, you may use the OSF in the meantime as they have no identity control whatsoever.

Figure 2: AsPredicted response linking account access to institutional email verification or prior publication traceability.

AsPredicted is notably a preregistration platform, that is, a scientific infrastructure explicitly

designed to increase transparency and broaden access to scientific practice prior to publication itself. Access is instead conditioned on infrastructural trust signals such as institutional email domains and prior publication traceability, illustrating a form of pre-content filtering in which administrative legitimacy precedes epistemic evaluation.

Several platforms explicitly associate institutional email domains with reduced uncertainty and lower verification cost prior to any scientific interaction. On AsPredicted, users attempting registration with personal email providers such as Gmail may encounter direct restrictions before account creation or protocol submission. Similarly, ResearchBox presents institutional affiliation as a condition for streamlined onboarding and accelerated access, while personal email users are subjected to additional verification steps before entering the platform environment. arXiv likewise requests justification for the use of non-institutional email accounts and warns that free email providers may result in delays due to verification requirements, as shown in Figure 3.

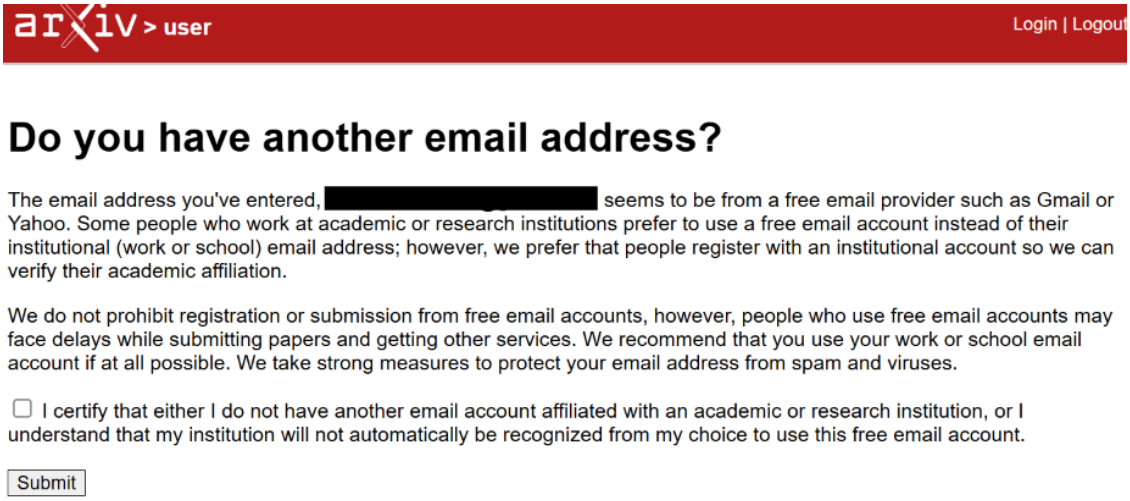


Figure 3: arXiv: "We prefer that people register with an institutional account"

The arXiv case is particularly informative because it presents the mechanism in a relatively transparent form. The platform explicitly associates institutional email addresses with verification and trust, acknowledges that free email providers may introduce additional delays, and simultaneously avoids framing the process as explicit exclusion. The resulting asymmetry therefore appears not as formal prohibition, but as differential infrastructural friction linked to institutional verifiability.

Importantly, these mechanisms are not framed as evaluations of scientific quality. Instead, they are presented as ordinary procedures linked to moderation scalability, anti-spam protection, identity verification, or infrastructural trust management. The result, however, is that institutional affiliation begins influencing scientific access before any content is reviewed. Infrastructural legitimacy therefore precedes epistemic evaluation.

4 Institutional Email as Epistemic Infrastructure

Institutional email addresses increasingly function as operational components of scientific trust infrastructures rather than simple communication tools. Across multiple digital research platforms, institutional domains are repeatedly associated with accelerated access, reduced verification burden, and lower moderation uncertainty. In this context, the institutional email becomes a compressed signal through which platforms infer legitimacy, accountability, and reduced infrastructural risk. In some cases, cademic pricing tiers and reduced friction are linked to institutional email verification, while personal email domains trigger alternative verification pathways and pricing structures.

On participant recruitment platforms such as Prolific, institutional affiliation directly affects economic and administrative access conditions. Academic pricing tiers are restricted to users capable of verifying institutional affiliation through organizational email domains, while personal email users may undergo manual review or lose access to discounted research infrastructure, as shown in Figure 4. Similarly, onboarding systems on research platforms frequently distinguish between users receiving "instant access" through institutional verification and those subjected to "extra steps" due to personal email domains. Infrastructural classification systems often lack a stable category for independent scientific activity situated outside recognized institutional or nonprofit frameworks.

Platform message

"We noticed that your account is currently configured under our nonprofit pricing. Could you please send us any documentation or additional information to verify your nonprofit organization status?"

"If you are not affiliated with an organization that has nonprofit status, we will need to move your account to our enterprise pricing, since this discounted rate is only available to nonprofit organizations or academic researchers."

"Once we have confirmed the correct pricing, we can consider restoring access to your account."

Figure 4: Example of status-based access reclassification. The account is not rejected on the basis of content, but access restoration is conditioned on documentary proof of nonprofit or academic status. In the absence of such documentation, the independent researcher is redirected toward enterprise pricing.

As shown in Figure 5, access asymmetries may emerge through pricing, verification, and status classification systems rather than explicit rejection of scientific content.

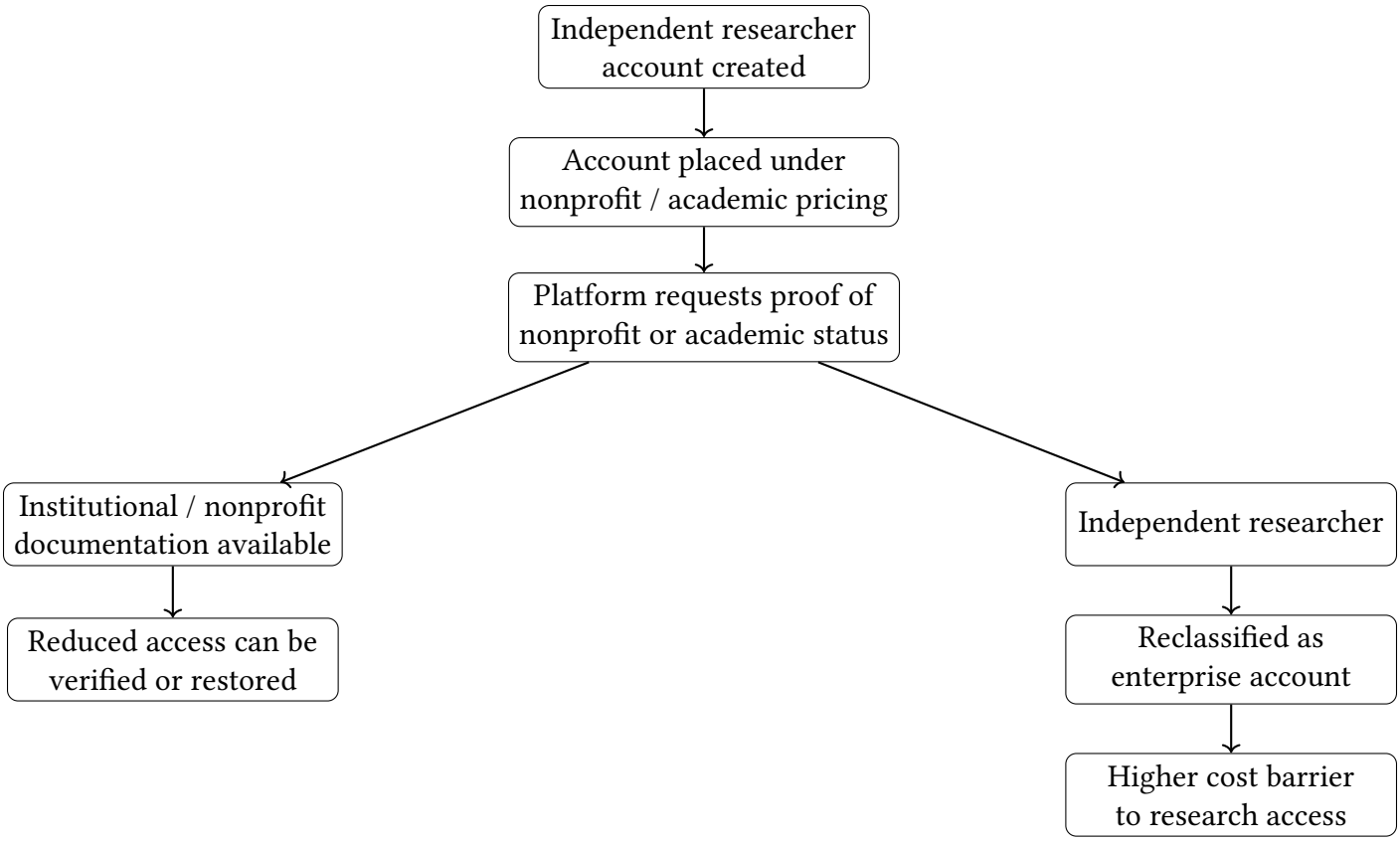


Figure 5: Access pathway in which independent researchers are shifted from academic or nonprofit treatment toward enterprise classification when they cannot provide institutional documentation. The exclusion does not occur through an explicit rejection of the research project, but through pricing, verification, and status categories.

In some cases, infrastructural trust escalation extends beyond simple onboarding friction into conditional account restoration workflows. On participant recruitment platforms such as Prolific, accounts flagged by automated security systems may subsequently undergo legitimacy clarification procedures involving institutional affiliation, nonprofit status verification, research-purpose disclosure, and internal review escalation prior to possible reinstatement. Importantly, these processes remain framed through supportive administrative language ("we're here to help", "relevant team", "thank you for your patience") rather than explicit exclusionary terminology. The resulting structure therefore combines automated trust suspicion with conditional infrastructural legitimacy reconstruction, as shown in Figure 6.

Prolific support message: security-mediated legitimacy inquiry

Hello Florian,

Thank you for contacting us.

I am sorry to hear that you have encountered this issue. I have reviewed the situation and can see that your account has been flagged by our security systems.

Before we can restore access to your account, we would like to learn more about the research you are conducting on Prolific.

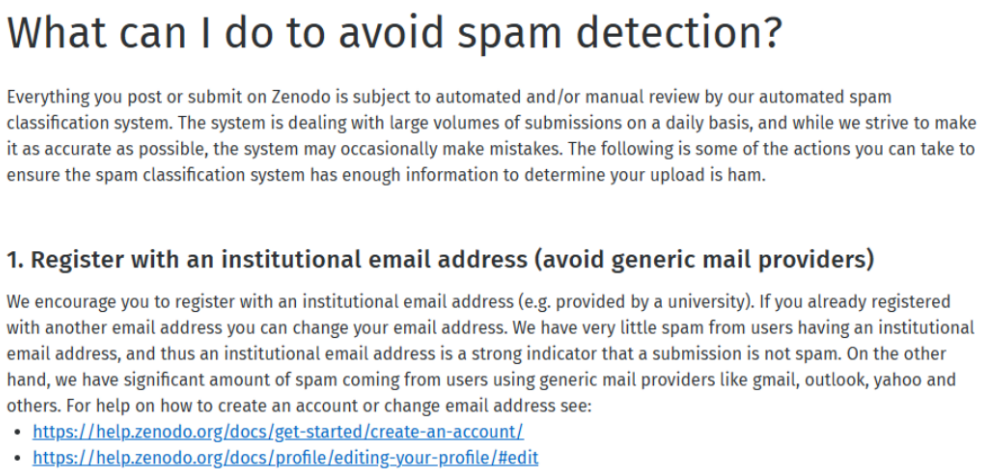
To help us, please share the following information:

- *Which institution are you affiliated with, if any?*
- *What type of studies do you wish to conduct?*
- *What is the objective of your research?*

We look forward to your reply.

Figure 6: Prolific account restoration request following a security flag. The message illustrates a security-mediated legitimacy inquiry in which account access becomes conditional on clarification of institutional affiliation, study type, and research purpose before participation can resume.

These asymmetries are often justified through operationally legitimate concerns such as participant compensation, data quality, moderation cost, or infrastructure sustainability, as shown in Figure 7. The resulting access differences therefore do not necessarily emerge through explicit exclusionary intent. Instead, institutionally affiliated researchers inherit reduced financial and administrative friction, while independent researchers may encounter increased infrastructural cost when attempting to conduct empirical research.



What can I do to avoid spam detection?

Everything you post or submit on Zenodo is subject to automated and/or manual review by our automated spam classification system. The system is dealing with large volumes of submissions on a daily basis, and while we strive to make it as accurate as possible, the system may occasionally make mistakes. The following is some of the actions you can take to ensure the spam classification system has enough information to determine your upload is ham.

1. Register with an institutional email address (avoid generic mail providers)

We encourage you to register with an institutional email address (e.g. provided by a university). If you already registered with another email address you can change your email address. We have very little spam from users having an institutional email address, and thus an institutional email address is a strong indicator that a submission is not spam. On the other hand, we have significant amount of spam coming from users using generic mail providers like gmail, outlook, yahoo and others. For help on how to create an account or change email address see:

- https://help.zenodo.org/docs/get-started/create-an-account/
- https://help.zenodo.org/docs/profile/editing-your-profile/#edit

Figure 7: Zenodo institutional email recommendation for anti-spam verification.

What makes these systems particularly resilient is that they are normatively shielded by

legitimate operational concerns such as spam prevention, fraud reduction, moderation scalability, and infrastructural security. As a result, criticism of these mechanisms can easily be reframed as opposition to quality control itself, thereby limiting discussion at the level of principle even when implementation effects remain asymmetrical. At the same time, the filtering architecture preserves strong plausible deniability. Platforms do not explicitly state that independent researchers are excluded; rather, they present their systems as ordinary anti-spam or verification procedures. Because the underlying filtering criteria often remain partially opaque, the boundary between illegitimate submissions and legitimate but weakly institutionalized research becomes increasingly difficult to contest externally.

Spam, paper mills, and fraudulent submissions are increasing across scientific and professional infrastructures, making large-scale trust filtering operationally attractive. Institutional email therefore functions as an imperfect but empirically useful proxy, with some platforms explicitly reporting substantially lower abuse rates among institutionally affiliated users. At the same time, because independent researchers definitionally lack such institutional identifiers, any infrastructure relying heavily on institutional email verification will almost inevitably generate significant exclusionary asymmetries against independent participation, even in the absence of explicit anti-independent policy.

The institutional email therefore functions as a form of epistemic infrastructure. It operates not merely as a contact mechanism, but as a scalable trust technology that reduces moderation cost and administrative uncertainty before any scientific evaluation occurs.

The exclusionary mechanism is distributed rather than localized. No single decision explicitly prohibits participation, yet the cumulative structure progressively increases friction, cost, ambiguity, and conditionality for independent researchers. Rather than directly evaluating epistemic content, platforms increasingly rely on pre-screening heuristics designed to reduce uncertainty and moderation burden at scale, a broader tendency observed in contemporary algorithmic governance systems (Amoore, 2020).

5 Friction-Based Access

Access within modern scientific infrastructures increasingly operates through cumulative administrative friction rather than binary acceptance or rejection. In many cases, independent researchers are not formally prohibited from participation. Instead, access becomes progressively slowed, destabilized, or administratively intensified through additional verification layers operating prior to scientific evaluation.

Several platforms explicitly describe these mechanisms in terms of delay or procedural escalation rather than exclusion. arXiv warns that users registering with free email providers "may face delays" due to additional verification requirements. Prolific subjects personal email

users to “manual review” processes before account approval, while other platforms impose “extra verification steps” for users lacking institutional identifiers.

Importantly, these mechanisms do not necessarily prevent participation in absolute terms. Rather, they increase the temporal, cognitive, and administrative cost of progression through scientific infrastructures. Access therefore becomes asymmetric not through explicit prohibition, but through differential fluidity. Institutionally affiliated users encounter reduced friction, accelerated onboarding, and stabilized trust pathways, whereas independent users experience greater uncertainty and administrative burden.

This distinction is structurally important because cumulative friction can substantially reduce practical access even in the absence of formal exclusion. Modern scientific systems therefore increasingly regulate participation through variable infrastructural resistance rather than overt rejection.

6 Normalized Quiet Exclusion

The filtering mechanisms described above rarely appear as explicit acts of exclusion. Instead, they are typically embedded within ordinary interface design, verification workflows, onboarding systems, and routine administrative recommendations. This process can be described as *normalized quiet exclusion*: a form of status-based filtering presented as operationally neutral and procedurally ordinary.

Several platforms integrate institutional preference directly into user interfaces through seemingly banal design elements such as placeholders, onboarding prompts, or verification recommendations. Expressions such as “Open Research Made Easy” may coexist with immediate requests for institutional email addresses, while personal email providers are subtly positioned as exceptions requiring additional scrutiny, see Figure 8. In these environments, institutional affiliation is presented not as a controversial criterion, but as the normal infrastructural baseline of legitimate scientific participation.

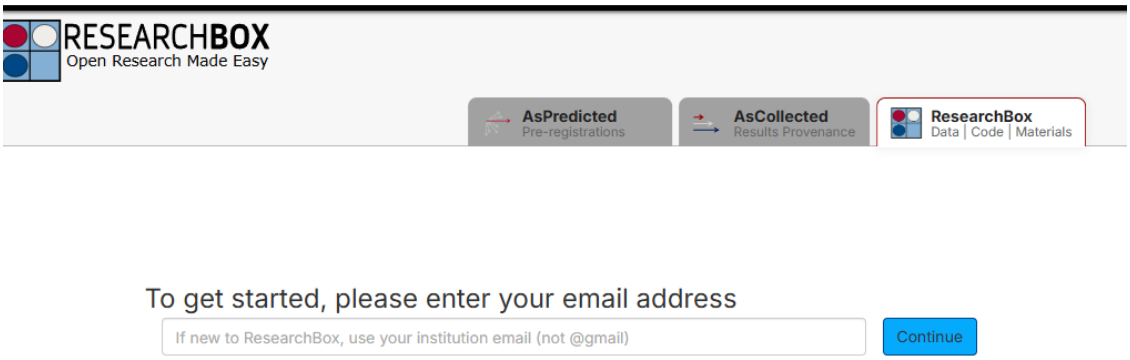


Figure 8: "If new to ResearchBox, use your institution email (Not @gmail)

Importantly, the visual and linguistic neutrality of these systems reduces the visibility of exclusionary dynamics. There is often no explicit rejection, ideological statement, or identifiable banning event. Instead, status-based filtering is absorbed into routine platform operation and framed through administratively reasonable concepts such as verification, anti-spam protection, moderation efficiency, or trust management.

As a result, exclusion increasingly operates through normalized infrastructural expectations rather than overt prohibition. Institutionally affiliated users experience scientific systems as fluid and immediately accessible, while independent researchers encounter cumulative procedural friction that appears natural, technical, and non-discretionary, as shown in Figure 9.

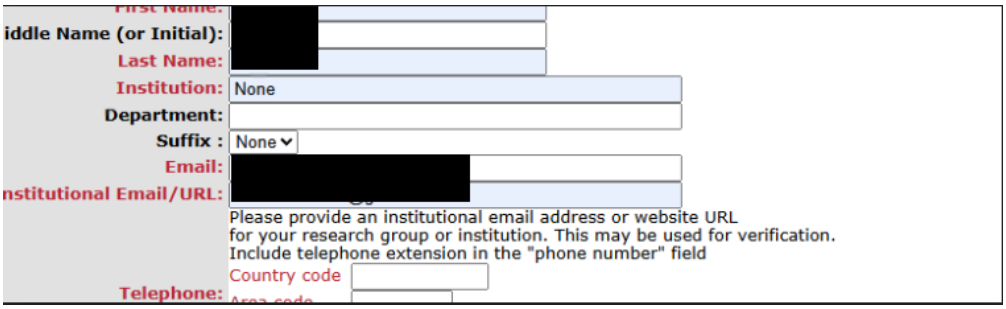


Figure 9: BioRxiv

The BioRxiv case, as shown in Figure 7, further illustrates how these mechanisms may emerge through ordinary bureaucratic optimization rather than explicit exclusionary intent. The platform initially seeks institutional anchoring, traceability, and verifiable identity before scientific participation occurs. This logic is particularly understandable within high-risk biomedical preprint environments characterized by large submission volumes, reputational sensitivity, and strong anti-spam or anti-fraud requirements. Yet the resulting structure still places administrative trust prior to epistemic evaluation.

7 Infrastructural Legitimacy vs Epistemic Legitimacy

A central distinction emerging from these cases is the difference between *epistemic legitimacy* and *infrastructural legitimacy*. Epistemic legitimacy refers to the scientific quality of a protocol, manuscript, dataset, or theoretical contribution. Infrastructural legitimacy, by contrast, refers to the degree to which a researcher possesses administrative markers compatible with large-scale trust, verification, and moderation systems.

Importantly, these categories are not fully independent. Institutional affiliation correlates, albeit imperfectly, with methodological training, peer feedback exposure, prior publication integration, and accountability structures. As a result, institutional markers often function as empirically useful trust proxies within large-scale scientific infrastructures. Digital platforms increasingly rely on such infrastructural legitimacy during early access stages because direct epistemic evaluation is costly, slow, and difficult to scale. Institutional email domains, indexed publications, academic affiliations, and established platform traces therefore operate as compressed trust signals capable of rapidly reducing uncertainty prior to scientific review.

Under this architecture, institutional affiliation does not merely indicate professional membership within academia. It becomes operationally integrated into scientific infrastructures as a mechanism for lowering moderation cost, simplifying identity verification, reducing fraud exposure, and stabilizing trust. Conversely, independent researchers may remain epistemically legitimate while lacking the infrastructural markers required for low-friction participation.

This distinction helps explain why many contemporary access asymmetries do not appear as direct judgments about scientific quality. In many cases, filtering occurs before any substantive evaluation of ideas takes place. The system does not necessarily reject epistemic content itself, but instead regulates participation through compatibility with administrative trust architectures. The issue is therefore not that infrastructural legitimacy is entirely disconnected from epistemic quality, but that probabilistic institutional correlations become operationalized into scalable pre-content filtering systems.

A recent correspondence from Preprints.org illustrates this distinction especially clearly. In explaining why a manuscript was not posted, the platform stated that the decision did not reflect the scientific quality of the work, but referred instead to screening criteria such as the limited number of references, the age of cited sources, the need for recent literature, and, crucially, author verification procedures. The message further explained that, due to increased concerns regarding paper mills and potentially fraudulent submissions, the platform had adopted a more cautious screening approach involving checks of previously published papers and requests for an institutional email address, an email previously associated with published work, or an ORCID identifier.

Importantly, the author already possessed an ORCID identifier at the time of submission,

displayed directly beneath the manuscript title in a highly visible and structurally central position during screening. The identifier was therefore neither hidden nor difficult to locate, but immediately observable within the submission interface itself. The moderation response consequently suggests that infrastructural legitimacy is not reducible to the mere existence of a persistent researcher identifier. Rather, legitimacy may additionally depend on publication traceability, institutional affiliation, and prior integration within recognized scholarly infrastructures, see Figure 10.

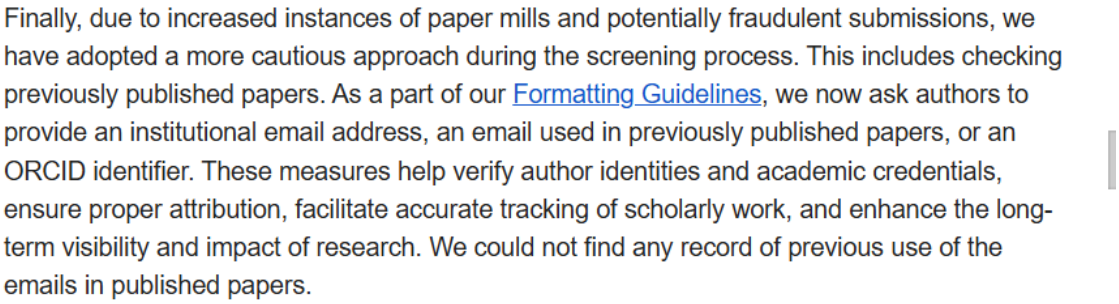

Finally, due to increased instances of paper mills and potentially fraudulent submissions, we have adopted a more cautious approach during the screening process. This includes checking previously published papers. As a part of our Formatting Guidelines, we now ask authors to provide an institutional email address, an email used in previously published papers, or an ORCID identifier. These measures help verify author identities and academic credentials, ensure proper attribution, facilitate accurate tracking of scholarly work, and enhance the long-term visibility and impact of research. We could not find any record of previous use of the emails in published papers.

Figure 10: Preprints.org moderation response linking publication access to institutional traceability and prior scholarly integration.

The increasing reliance on prior publication traces, indexed scholarly histories, and previously validated academic identities may progressively transform infrastructural access into a recursive legitimacy system in which prior institutional recognition becomes a de facto prerequisite for obtaining future recognition, see Figure 11. Under such conditions, researchers lacking already-legitimized publication histories may encounter growing difficulty entering visibility networks precisely because the infrastructures governing access increasingly treat prior inclusion itself as evidence of future trustworthiness.

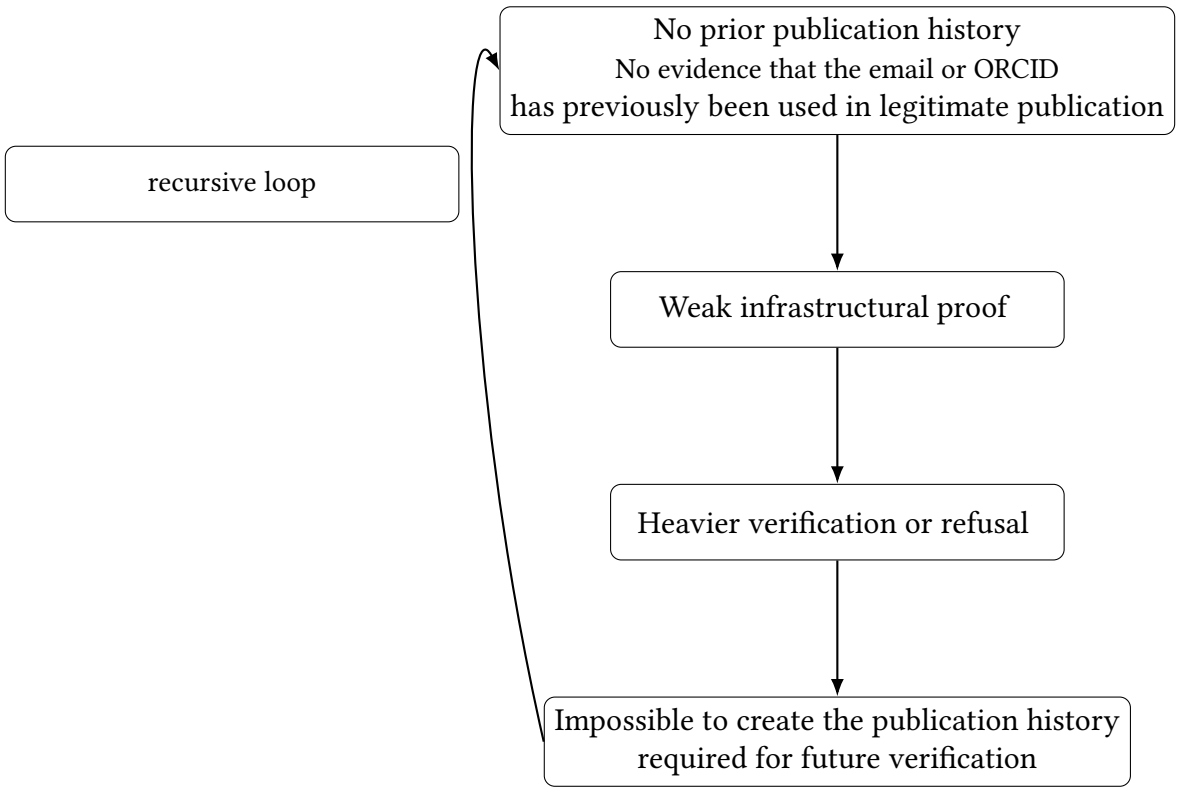


Figure 11: Recursive infrastructural legitimacy loop.

This case is analytically important because it separates epistemic judgment from infrastructural trust. The manuscript was not described as scientifically invalid. Rather, the difficulty concerned the absence of recognizable administrative markers linking the author to an already legible scholarly identity, especially the absence of prior published use of the submitted email address. In this sense, previous visibility within the publication system becomes a trust signal for future access to publication infrastructure.

The case therefore illustrates a circular feature of infrastructural legitimacy. Researchers who already possess institutional emails, indexed publication histories, and stable scholarly traces are easier to verify and therefore encounter lower moderation uncertainty. Independent researchers, by contrast, may remain epistemically legitimate while lacking the infrastructural markers that make them administratively legible. Access is thus not denied through a direct claim about scientific quality, but becomes conditional on compatibility with platform-level trust architectures designed for moderation, fraud prevention, and scalable identity verification. The resulting dynamic resembles a recursive form of cumulative advantage comparable to the Matthew effect in science (Merton, 1968), in which prior institutional visibility progressively increases future infrastructural legibility and reduces verification uncertainty.

The resulting asymmetry is therefore structural rather than purely ideological. Institutionally affiliated researchers inherit pre-allocated infrastructural trust, while independent researchers

must repeatedly reconstruct legitimacy across fragmented verification environments.

8 Discussion

The mechanisms described in this paper do not necessarily emerge from explicit exclusionary intent. In many cases, institutional affiliation functions as an administratively efficient trust signal for reducing moderation cost, verification burden, and infrastructural uncertainty at scale (Gillespie, 2018; Power, 1997).

However, these systems may still produce important access asymmetries. Scientific participation increasingly depends not only on epistemic evaluation, but also on compatibility with infrastructural trust architectures operating prior to content review itself (Star, 1999). Importantly, these asymmetries do not necessarily require centralized coordination or explicit exclusionary policy. They may emerge progressively through local administrative optimizations in which platforms independently adopt low-cost trust proxies to reduce moderation burden, infrastructural uncertainty, and verification complexity at scale.

As a result, independent researchers may remain scientifically legitimate while encountering greater administrative friction through delays, verification escalation, onboarding instability, or reduced access fluidity.

The paper further proposed the concept of normalized quiet exclusion to describe how cumulative access asymmetries may emerge through ordinary administrative procedures rather than explicit rejection. Rather than relying on overt exclusionary events, these systems may progressively regulate participation through differential infrastructural fluidity, verification burden, and administrative trust allocation. Under this architecture, scientific participation increasingly depends not only on epistemic legitimacy, but also on compatibility with infrastructural trust systems operating prior to scientific evaluation itself.

The central issue is therefore not necessarily overt prohibition, but the growing role of pre-content trust estimation within modern scientific infrastructures.

The present paper primarily aims to diagnose and conceptualize an increasingly important infrastructural mechanism rather than provide a fully scalable replacement architecture. The operational problems addressed by contemporary scientific platforms, including spam, paper mills, identity fraud, moderation cost, and verification scalability, are real and structurally difficult to solve. Institutional trust proxies persist partly because they provide computationally inexpensive reductions of uncertainty under high-volume conditions.

Existing alternatives such as ORCID identifiers, prior-publication traceability, or manual verification already appear only partially sufficient, as illustrated by the Preprints.org case discussed earlier. Fully replacing infrastructural heuristics with direct epistemic evaluation at early access stages would likely remain economically and computationally infeasible at scale under current

conditions.

The central contribution of the present framework is therefore diagnostic rather than purely prescriptive. The concept of quiet exclusion attempts to render visible a distributed infrastructural dynamic that often remains normalized, operationally justified, and administratively opaque despite its potential consequences for independent scientific participation.

Future work may explore whether alternative trust architectures, including decentralized reputation systems, third-party identity attestation, cryptographic verification frameworks, or other scalable legitimacy mechanisms, could reduce dependence on institutional affiliation while preserving moderation feasibility.

9 Conclusion

This paper introduced the concept of pre-content filtering, in which administrative trust signals such as institutional email domains influence scientific access before content itself is evaluated. Across multiple digital research platforms, institutional affiliation functions as a mechanism for reducing verification burden, moderation uncertainty, and infrastructural cost.

The paper further proposed the concept of normalized quiet exclusion to describe how cumulative access asymmetries may emerge through ordinary administrative procedures rather than explicit rejection. Under this architecture, scientific participation increasingly depends not only on epistemic legitimacy, but also on compatibility with infrastructural trust systems operating prior to scientific evaluation itself.

The author's interest in this topic was partially motivated by personal experiences navigating scientific platforms as an independent researcher.

10 References

Amoore, L. (2020). Cloud Ethics: Algorithms and the Attributes of Ourselves and Others. Duke University Press.

Bowker, G. C., & Star, S. L. (2000). Sorting Things Out: Classification and Its Consequences. MIT Press.

Brayne, S. (2020). Predict and Surveil: Data, Discretion, and the Future of Policing. Oxford University Press.

Espeland, W. N., & Sauder, M. (2007). Rankings and Reactivity: How Public Measures Recreate Social Worlds. American Journal of Sociology, 113(1), 1-40.

Fourcade, M., & Healy, K. (2017). Seeing Like a Market. Socio-Economic Review, 15(1), 9-29.

Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.

Greene, D. (2021). The Promise of Access: Technology, Inequality, and the Political Economy of Hope. MIT Press.

Haak, L. L., Fenner, M., Paglione, L., Pentz, E., & Ratner, H. (2012). ORCID: A System to Uniquely Identify Researchers. Learned Publishing, 25(4), 259-264.

Merton, R. K. (1968). The Matthew Effect in Science. Science, 159(3810), 56-63.

Morin, F. (2026). The Quiet Exclusion of Independent Researchers. Unpublished manuscript.

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.

Power, M. (1997). The Audit Society: Rituals of Verification. Oxford University Press.

Roberts, S. T. (2019). Behind the Screen: Content Moderation in the Shadows of Social Media. Yale University Press.

Star, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377-391.

Striphas, T. (2015). Algorithmic Culture. European Journal of Cultural Studies, 18(4-5), 395-412.