

Auditing Search Power: A Perspective on Ethical Justification and Governance for Independent Search-Engine Audits

Yumo Zheng

Westminster School, 995 Hopmeadow Street, Simsbury, CT 06070, United States

ABSTRACT

This Perspective article argues that independent third-party audits of search engines are an ethical necessity since these sites wield public epistemic power without being inspectable by both researchers, users and regulators. While search engines perform the function of searching information and presenting the result, their main roles consist in filtering, ranking and personalizing contents for users. Nevertheless, the common problem with the users is that they have little knowledge about how these sites work and the system of self-regulation gives search power players a chance to control the information and the discourse of their power. In this connection, a hybrid audit governance framework, which involves the accreditation of independent auditors by a body of audit standards, graduated access corresponding to public interest in the audit process and other factors, such as privacy protections, secure audit environment, selective disclosures and complaint and remedy channels is seen as a more appropriate mechanism of accountability. Moreover, the analysis considers a number of conflicting issues with the search engines, such as trade secrecy, user privacy, search manipulation with the help of search engine optimization, problems with over regulation and potential symbolic compliance through weak audits. Thus, the search engines do not need to make their activities transparent to the public, but still they can be made auditable.

Keywords: search engines; algorithmic auditing; accountability; trade secrets; privacy; platform governance

INTRODUCTION

Even though search engines can be described as relatively basic methods of finding relevant websites, in reality, they perform actions like rankings, filtering, clustering, personalizing, summarizing, and visualizing results. In this context, their design affects what results

will be shown to where, who will be considered as a more credible source, what information will be excluded, and what content the user will never see. In this aspect, search engines play the part of institutions; however, they are not official institutions but companies that work as institutional actors with regard to providing information to the general public.

The resulting situation creates an accountability problem for search engines. Namely, being gatekeepers of public knowledge, search engines use ranking algorithms that are proprietary, changeable, and incomprehensible to most lay users. Thus, while users can see things like a ranked results page, autocomplete suggestions,

Corresponding author: Yumo Zheng, E-mail: marcozheng23@gmail.com.

Copyright: © 2026 Yumo Zheng. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Accepted August 21, 2026

<https://doi.org/10.70251/HYJR2348.4413151325>

knowledge panels, snippets, and news cards, they rarely know why some results appeared or disappeared on their screen, whether personalization was at work, why some content was elevated or demoted in the rankings, or what would happen to a similar query entered by a completely different person. As Laidlaw argues, given the increasingly crucial role of information, those who control the flow of information become participants in public discourse and democracy. Hence, the question of public accountability arises (1).

The aim of this Opinion/Perspective article is to make an ethical case for independent third-party audits of search engines, since these services exert epistemic power in an environment of information inequality and both ordinary user agency and self-regulation are insufficient to limit this power. The point here is not that search engines should be forced into neutrality understood as presenting the single and only “correct” order approved by governments. This understanding of search engines is flawed, as the very concept of ranking assumes selection and prioritizing. Instead, this article argues that search engines should be auditable, meaning that properly authorized outsiders should be able to check whether they fulfill their mission in a non-discriminatory, non-manipulative, non-arbitrary, and non-misleading manner. Throughout this article, “independent third-party audit” refers to the audit activity itself; “hybrid audit governance framework” refers to the institutional arrangement that authorizes and regulates those audits; and “graduated access” refers to the risk-based escalation of auditor access.

The proposed answer to this problem is not absolute transparency. Search engines have good reasons to keep some details secret, including protecting intellectual property, avoiding gaming and spamming, and ensuring user privacy. At the same time, this article contends that those concerns justify safeguarded auditability, not total opacity. This perspective proposes a hybrid audit governance framework: independent auditors, graduated access, protected environments, privacy-friendly access to data, selective disclosures, and a complaint procedure.

SEARCH ENGINES AS PUBLIC-INTEREST INFRASTRUCTURES

This is where the original premises of the argument are set out: search engines require independent supervision for reasons that go beyond being powerful companies and have something to do with the way they provide important public services through infrastructure.

This assertion is limited and also very important. It is not saying that search engines should be regulated exactly as the public utilities but neither does it say anything about the state controlling the results of rankings. Instead, it says that regardless of ownership, search engines provide services that are socially relevant for democracy and public knowledge.

Laidlaw frames search engines as information managers: institutions which classify and arrange information using criteria of their own. Hence, what the user comes across in his online experience is influenced by what information managers think. The more important the information becomes, the more that it needs to be viewed as such and the more its managers need to be viewed as people with their own set of responsibilities. The core of Laidlaw’s investigation is the question if search engines should be perceived as means of democratic communication with duties to the public good (1).

In addition to impacting the way in which people find restaurants and compare prices of goods and services, search engines affect the way in which people discover politicians, scientific discoveries, controversy, minority groups, history, and crisis. This is a view that Bracha and Pasquale hold similar views regarding. Search engines function as control points in the context of networked environment, and they are not suggesting that the ranking that occurs through them is always wrong; rather, what they are saying is that the fact that search engines act as control points means that they become manipulable, distorted, or unjustly exclusionary (2).

The question is important due to the epistemic dependency provided by search engines. Without them, people wouldn’t be able to get access to the massive amount of available information. Sorting and classifying performed by the search engines make the information available while making some sources more prominent than others. As noted by Bracha and Pasquale, placing the data further than the second page makes it unavailable for people since their attention is focused on the top pages (2). This point gets supported by the explanation of algorithmic power by Diakopoulos, who says that ranking and filtering allow one information source to become more valuable than others (3).

Several empirical audit studies have shown that this concern extends to practical reality. Robertson, Lazer, and Wilson made audits for political-related Google searches, finding that there was significant variation in both SERPs and personalization depending on query type, user type, and date (4). It is particularly important

in this study since ordinary users do not conduct a comparison of logged-in search results with results obtained in incognito mode, do not gather the results for a long time, and do not experiment with how the query is phrased. The point is not that the search can differ between various users but how this difference can impact politically relevant exposure and remain unnoticed by the user.

Another key finding is obtained by Urman, Makhortykh, and Ulloa. In their work, they managed to show that without any intentional manipulation, in other words in default, non-personalized mode, various search engines can lead to differences in exposure to the information and create random information inequality (5). It matters because it shows that problems of accountability are not only connected to manipulative intentions and bias of personalization algorithms but are generated simply by opaque design and randomness.

Several other empirical researches confirm the claim about the multilayeredness and the extension of the phenomenon to fields outside the political sphere. In particular, Lin *et al.* showed that historically marginalized groups like women, black communities and LGBTQ+ face significantly higher negative biases regarding search engine autocomplete prediction (6). Dash, Rezapour, and Shah showed how image search could reproduce stereotypes connected to occupation and investigated a strategy for addressing this issue through re-ranking (7). Paramita *et al.* did not explore news search bias specifically. Instead, they used the methodology of participatory design to create an interface for increasing user consciousness about search bias of search engines (8).

One of the arguments against the thesis is provided by Goldman who argues that there is no way for the search engines to not be biased since they have to fulfill the function of the editor when ranking the content. The function of sorting, filtering, blocking the content is necessary to make them work effectively. This statement partly has merits: search engines are not able to be neutral in the sense that they are non-judgmental (9). Manne & Wright develop this idea by questioning the principle of “search neutrality”: according to them, its proponents presuppose some sort of market failure and damage for consumers without proving it at all. They assert that the notion of relevance is subjective; that the competition between search engines is carried out through provision of better results; and that regulation can harm innovations and consumer well-being (10).

Taken together, this section establishes the public-

interest basis for scrutiny: search engines regulate information on a large scale, affect politics, public debate, and representation, and are difficult for users to observe effectively. The neutrality counterarguments discussed above do not eliminate the need for scrutiny; instead, they narrow the claim from state-directed neutrality to auditability.

The argument of this section can be summarized as follows: search engines are considered infrastructures in the interest of the public because of their ability to regulate information on a large scale, their decision making has an effect on politics, public debate, and representation, users cannot regulate or witness such decision-making effectively, and the implementation of neutrality regulation is theoretically and practically ineffective. Therefore, it is argued that the current paper does not advocate for state regulation of search but rather auditability.

WHAT COUNTS AS AN AUDIT?

Now having made the case for why search engines are indeed an appropriate subject of scrutiny as per public interest considerations, the question now remains what kind of scrutiny can actually be accomplished within this framework. While in certain situations transparency may have been suggested as a universal cure to all problems, transparency is at times both impossible and undesirable, especially in the case of a system as complicated and powerful as the one in discussion. It is not possible at all times to grant access to source codes or even to training data.

As highlighted in Bandy’s detailed survey, “Algorithm Audits may be understood as empirical assessments of public algorithms that are undertaken in order to identify undesirable behavior.” Four types of machine behavior have been identified by the audit literature—these are discrimination, distortion, exploitation, and misjudgment. Out of all these forms of behavior, it is the search algorithms that stand out as a major form of focus (11). These have two main implications—that “algorithm audits are not just conceptual but practical.” Additionally, “algorithm audits go beyond discrimination.”

Diakopoulos defines a concept that is related here in terms of what he calls “reverse engineering”. As there are many algorithms that work like black boxes, the usual approach researchers follow in analyzing these algorithms includes observing their input-output behavior (3). Using different queries, different geographic locations, different times of search, different browsers,

and user accounts will allow to detect certain patterns that will shed light on how the system works. Exactly this logic is at the core of search engine auditing.

However, audits cannot be seen as a universally applicable approach. Casper *et al.* have created a valuable framework of classification of access modalities used in AI audits including black-box, grey-box, white-box, and outside-the-box access. Black-box access allows auditors to make queries and receive outputs from the systems being tested; grey-box provides auditors with limited exposure to the mechanisms inside; white-box means access to the components of the system; outside-the-box provides with access to the context, such as methodology, code, documentation, data, and internal evaluations besides access to the system. The major claim made by Casper *et al.* is that black-box access is not enough for a thorough AI audit as the space of possibilities remains narrow (12).

Indeed, the aforementioned finding takes on heightened importance in view of the fact that most of the existing searches of the search engines themselves make use of black-box or close to black-box access. This type of searches involve monitoring changes of result pages in relation to query changes, autocomplete options, personalization, sources and other parameters. Although the described studies are indeed very informative, there exist several limitations of the described types of searches. Examples of the relevant articles can be cited as Robertson *et al.* political SERP personalization audit; Urman *et al.* virtual agents for comparative political searches; and Lin *et al.* autocomplete biases using simulations and API (4–6).

This type of audits shares the black box approach to addressing the problem at hand. In other words, while they are able to showcase that bias or any other effect exists, most of the time they fail to explain the process. These kinds of audits will be able to show us results but they will not be able to provide a complete account of the process. Black box audits are able to show that certain political sources are displayed more often or certain autocomplete suggestions are based on demographic groups or users who are logged in receive more personalized information, but it is unable by itself to tell whether these phenomena are a result of training datasets, rankings, personalizations, location of the user or something else.

Within the hybrid audit governance framework proposed later, black-box auditing should remain a monitoring tool rather than the only form of scrutiny; deeper diagnostic review may require additional access.

WHY INDEPENDENT THIRD-PARTY AUDITS ARE ETHICALLY JUSTIFIED

Given the public-interest role and opacity established above, the ethical justification for independent third-party audits turns on whether user consent and user exit provide sufficient accountability. This perspective argues that they do not, because the average user lacks the necessary understanding of how rankings are calculated, how personalization works, what kinds of information get excluded, or whether certain classes of sources are disproportionately favored.

Consent becomes problematic because users lack relevant knowledge. A user can give the minimal kind of consent to use a search engine, but at the same time, that user cannot make an informed decision about the hidden processes the engine performs while showing certain results. This inability to understand whether results are personalized, whether relevant sources are being systematically excluded, or whether autocomplete suggests discriminatory queries leads to incomplete evaluation of search results. As Bracha and Pasquale point out, this creates black-box opacity in which missing results become “unknown unknowns,” since users cannot even perceive what they lack (2).

The exit option is also limited. It would be naive to assume that people will leave a search engine if they dislike its results, since they might not notice any distortion in the first place. Moreover, because the search market is concentrated, users are unlikely to escape search-engine domination simply by choosing another provider. Finally, even when options are available, the decision to move to another provider would be difficult given users’ lack of knowledge about the strengths and weaknesses of each option (2, 10).

Brandsma and Schillemans provide a useful conceptual framework for understanding this problem through accountability theory. In their view, accountability is a key mechanism of democratic control because it checks discretionary power. Their accountability cube conceptualizes accountability through three elements: information, discussion, and consequences. Information means that an actor provides an explanation of its activities. Discussion means that an accountability forum can challenge, interpret, or evaluate that explanation. Consequences involve sanctions, remedies, corrections, or responses to substandard behavior (13).

This cube helps differentiate several kinds of accountability failure. There are situations where actors lack sufficient information. There are also situations where

information exists but there is no forum for discussing it. Finally, there are situations where discussion occurs but no action follows. Search-engine accountability currently risks all three failures. Users receive limited and often non-comprehensible information; many researchers lack access to search mechanisms; and sometimes the identification of negative impacts is followed by inaction.

In this context, it is important to analyze the disclosure-related failures discussed by Greiling and Spraul. They describe problems of reluctance to disclose information and information overload. Their approach is useful because accountability can be compromised both when an actor withholds information and when it shares so much information, or such technical information, that nobody can understand it (14). As applied to search engines, the message is clear: while “trust us” is insufficient, providing large amounts of technical information without explanation is also useless. The ethical requirement is not disclosure itself, but usable disclosure that involves interpretation, contestation, and consequences.

Independent third-party audits can help achieve these goals better than many other forms of analysis. Internal audit is useful, but it does not address the problem of independence. Transparency reports are likely to disclose selected aspects beneficial to the organization, while user complaints provide only symptoms, not the root cause of the problem. Independence matters because search providers have incentives to avoid disclosing weaknesses, define criteria of success in self-interested terms, or interpret failures as isolated events. As Casper *et al.* note, proprietary systems often perform internal evaluations with selective disclosure and outsiders with only limited black-box access (12).

Consequently, this article offers the following philosophical rationale: when a private actor wields infrastructural power over public knowledge, and when affected persons lack meaningful observability, comprehensibility, and exit opportunity, accountability requires independent forums capable of producing information, processing it, and creating consequences. Search engines possess all these qualities and therefore should be subject to independent third-party audits.

THE THREE MAJOR CONSTRAINTS: TRADE SECRETS, PRIVACY, AND GAMING

The preceding section justifies the case for independent third-party audits of search engines. But justifying independent third-party audits and designing

the hybrid audit governance framework are two different tasks. The objections to the proposed framework are significant. Search engines function within competitive environments; they use proprietary technologies; and they process sensitive user information. Therefore, any credible governance framework must specify how these obstacles can be addressed.

Trade Secrets

Perhaps the first and most common objection relates to potential leaks of proprietary information. Search engines spend considerable amounts of money developing ranking, spam detection, query parsing, user interface, and quality-evaluation technologies. If this information is shared widely, competitors may exploit the technology while manipulators may reverse-engineer it. Manne and Wright’s criticism of regulating search neutrality highlights these considerations and argues that regulating search bias may undermine innovation, consumer welfare, and ordinary product design (10).

The same line of reasoning applies to Goldman’s objection: since search engines perform editorial functions, disclosure and re-ordering of results may undermine the processes that make search useful (9). This argument goes beyond pure business consideration because, if disclosure makes search more vulnerable to spam or less relevant, the public and users also suffer.

Nonetheless, the case of trade secret is not an indicator that the secrecy is all inclusive. In this regard, Levine’s discussion of trade secrecy provides useful guidance. Levine observes that trade secrecy has been viewed as a doctrine of business; but with the developments in the digital era, trade secrecy can be regarded as a doctrine of public infrastructure, involving such things as voting machinery, the internet, and communications. Whereby a private operation has assumed significant importance in the public space, there is the need to balance commercial secrecy with democratic requirements of public accountability (15).

Pasquale provides a similar argument in his work ‘The Black Box Society’. According to him, organizations with immense powers have been able to gather a lot of information about people while their rating or decision systems are closed. As a result, the difference lies in the fact that people are transparent for institutions while institutions are opaque for people (16). This is seen in search engines as they may have access to the private data of the people such as political views, health issues and other things.

Bracha and Pasquale offer a more nuanced approach

to this question. First, they acknowledge that too much transparency will result in low search quality and even manipulation. Still, they believe that a certain level of transparency or oversight is necessary, and there might be cases when an institution worthy of trust is allowed to analyze a process behind the scenes (2).

Therefore, they suggest that courts and administrative agencies may strike the balance between secrecy and transparency with methods like sealed documents, specific review and limited access (2).

Therefore, the argument presented in this context does not support openness of search algorithms. This paper argues that independent third-party auditors must be provided with an opportunity to review the search systems from the perspective of legality, fairness, and accountability. The technical issues associated with such an approach were highlighted by Casper *et al.*: improved audit ability may result from the use of protections, application programming interfaces, safe research facilities, access control, and confidentiality (12).

Privacy

The privacy problem is not the same as the problem of trade secrets. It is likely that the design of a useful audit scheme will require having access to user query-related information, customized settings, click behavior, educational resources, and implementation details. Hence, it will become possible for sensitive user information to be revealed. Such an audit process will violate the interest of the public because it will compromise private data that the public wants protected.

In this respect, the discussion of Rubinstein and Good about privacy-by-design is relevant to the issue of search engines and their governance problem. According to them, privacy cannot be limited to concepts. It should materialize in terms of the products' design and the governance of them as well. These include data minimization, data retention limitation, notice and choice, access, transparency, accountability, and oversight. Moreover, it is noted that regulators need to give clear guidelines to balance privacy and business needs and to achieve privacy goals (17).

Hence, audit systems must take into account privacy preservation as one of its fundamental principles. This will involve limiting access to data based on what is absolutely essential; using techniques such as aggregating, redacting, or sampling of private information; keeping private data safe through secure environments, and not disclosing any users' identity in audit results. Simply put, privacy must be sorted out

before users are granted access.

Apart from that, there is the ethical aspect involved: while the need for auditing of search engines cannot be overlooked due to the effect it has on the users, the users must not bear the consequences of it. It is important to create an audit system which would shield users from being exposed by both the platform itself and the auditor.

Gaming and System Integrity

Another objection concerns gaming and vulnerability. Search engines operate in a hostile environment, with search engine optimization (SEO) manipulation, spam, link farms, click fraud, misinformation campaigns, and content farms working against the system. If the audit procedure leads to disclosure of too much information about ranking systems and anti-spam thresholds, these techniques may simply be adjusted accordingly. A search engine cannot be considered static.

Another such argument can be seen from Goldman who argues that it is important for editorial controls because it would help ensure that a system is not taken advantage of by spamming, clicking, fraudulent, and off-topic content (9). Similarly, Bracha and Pasquale agree that transparency can encourage gaming activities and reduce the effectiveness of search engines, and according to Manne and Wright, it is hard to tell whether results sorting or manipulation occurs due to the relevance aspect being subjective and dynamic (2, 10).

These criticisms do not require abandoning auditability. This perspective instead distinguishes audit access from public disclosure: the question becomes what information must be made available, to whom, and on what grounds. Independent third-party auditors may receive protected access while only a limited set of findings is released publicly.

COMPARING GOVERNANCE MODELS

In light of the above-discussed ethical aspects and limitations, this part will analyze governance frameworks that cover both search accountability and audits. In contrast to pursuing the most open governance framework, the aim here is to determine the governance model which suits the need for both accountability and secrecy.

Pure Self-Regulation

The simplest form of the governance structure assumes that the search engine carries out its own audit of itself and its practices, prepares reports at regular

intervals, and decides on how much control from outside can be allowed. The strengths of this structure can be quite obvious: the search engines know the system better, and are able to conduct self-audits without providing any undesired data.

From an ethical point of view, however, the problem of conflicts of interests still persists. Accountability is comprised of information disclosure, evaluation and consequences thereof; and in the case of self-regulation, all these functions are fulfilled by one party – the same one that is being judged. The company chooses what information should be provided, on what grounds it should be evaluated, and what consequences it might have after. If the society has to rely on the company's statements, there might be a need for withholding some information.

Suggestions made by Manheim *et al.* are constructive in the context of AI audit standards boards. Some of these include transparency not being sufficient in itself in the risk mitigation process, internal audits being indulged in the practice of safety-washing, independent third-party audits requiring standards to have credibility, industry-specific standards sometimes lacking in credibility, and the possibility of regulatory frameworks becoming outdated because of their inflexibility. This would imply that industry-centric approaches might prove insufficient (18).

Direct State Regulation

In yet another scheme, there is direct involvement of the state in regulating search activities. Under this scheme, the state will be involved in laying out the disclosure standards, inspection standards, and also rank policies in some areas like elections, health, or information related to disasters. There are merits in this scheme considering that the search engines influence public dialogue and there must be public authority where there is public interest.

The problem still exists, though. According to Bracha and Pasquale, “there exist dangers of over-regulation, regulation capture, paternalistic treatment of content, and incompetent regulators’ handling of complex systems in the case of direct regulation” (2). The same idea is expressed by Manne and Wright; in their view, costs of direct regulation of search engines would be higher than the benefits, and a Federal Search Commission would be necessary to supervise an unclear area of search engines’ functioning (10).

Conceptually, another problem emerges: if search engines affect discourse, direct governmental

management of ranking poses a danger. It would be a mistake for a government to become the body responsible for deciding what political, scientific, or cultural results should be emphasized and ranked highly. Therefore, although government involvement may be essential in authorizing and supporting independent third-party audits, direct management of rankings should be avoided.

Complaints-Based Co-Regulation

The third model considered here is a complaints-based approach that falls under co-regulation. Laidlaw argues that accountability should include an independent complaints mechanism that allows website owners and users to complain about abrupt changes in ranking, deceptive search results, and violations of dignity principles. Such a system would support relevance, transparency, and user dignity through an appropriate channel (1).

This model highlights one significant deficiency of many audit models: their focus on system-level evaluation. Complaints provide an opportunity for affected individuals to speak to the problems they face. This process can also uncover hidden problems that ordinary metric-based methods fail to detect.

The weakness of the complaint model is clear: it is reactive and dependent on harmed users realizing that their rights or interests have been affected. Moreover, search-engine harm is hard to detect because users may not know what they were missing. This does not mean that complaints cannot become a useful addition to other audit mechanisms. They are needed, but they are not sufficient for complete search accountability.

Accredited Independent Third-Party Audits with Graduated Access

Among the models considered here, this perspective argues that a mixture of mechanisms centered on accredited independent third-party audits with graduated access may offer a stronger balance of accountability and confidentiality. This approach combines public authorization of independent oversight with protected access to proprietary information and selective disclosure, while addressing the disadvantages of the models discussed above.

This review highlights the problems within institutions associated with the process of conducting independent third-party audits of search engines. According to Mattli and Büthe, the process of delegating governmental authority to private organizations may lead to a multiple-principals situation because different standard-setting

organizations tend to behave differently toward the stakeholders who affect their sustainability (19). This does not mean that privately managed standards tend to be always captured and weak, and government standards tend to be inflexible. Instead, this is an indication that the process of conducting an audit needs to be regulated by certain institutions.

The approach of Trebilcock and Iacobucci with regard to privatization and accountability is pertinent as well. These scholars assert that there is a difference between accountability inside an institution and the accountability of the institution as a whole. Even though private firms can be highly effective when it comes to pursuing their own ends, that does not mean that they are equipped with adequate means for dealing with public accountability problems (20). Search serves as a good illustration of this.

Thus, the proposed hybrid audit governance framework works as an intermediary institution between private entities and the state. The model neither turns the search engines into governmental institutions nor makes the former irrelevant. On the other hand, it allows for independent monitoring of information, which might have been unreachable earlier.

A PROPOSED HYBRID AUDIT GOVERNANCE FRAMEWORK

This perspective proposes a hybrid audit governance framework grounded in one core concept: the more public interest in the search process is involved, the stricter the access and accountability procedure should be. The examples where additional scrutiny applies include political elections, medical issues, crises, civil rights issues, public safety concerns, and concerns pertaining to minorities' interests, compared to normal commercial searches.

The suggested framework involves seven elements. In order to make the framework clear, its constituent parts are highlighted in parallel fashion as follows.

Independent Search-Engine Audit Standards Board

This perspective therefore proposes a dedicated board to take charge of setting audit standards, certifying the auditors, updating methodologies from time to time, and making sure that the audit process does not become just a formality. According to Manheim *et al.*, internal audits have the potential of being reduced to mere 'safety washing', that independent third-party audits demand legitimate standards; that standards developed in industry

do not hold much legitimacy, and that regulation systems remain obsolete. Therefore, they call for the formation of AI Audit Standards Board to maintain the relevancy of audit in a changing system (18). This is something that needs to be considered in the hybrid audit governance framework for search engines.

Accredited Independent Auditors

Independent third-party audits must be carried out by qualified auditors who lack any potential conflicts of interest. These auditors must possess technical proficiency and be under a duty of confidentiality. At the same time, they must act legally and ethically in conducting their process through integrity and accuracy. There are reasons why independence must be maintained. It is because audits will not carry any weight at all if they are completely in charge by those being audited. However, independence is not enough. There is a need for specialization.

Graduated Access Based on Risk and Audit Type

Independent third-party audits do not always need access to be uniform. Regularly conducted audits can adopt the black-box approach using virtual agents, web-scraping, controlled search, source distribution assessment, and autocomplete analysis. Nevertheless, when there is a situation that black-box audit points out critical and mysterious issues or when the issue under scrutiny falls into an important setting, it is essential to seek for more access. This distinction should follow the access classification introduced by Casper *et al.* (12), which distinguishes black-box, grey-box, white-box, and outside-the-box access. In the access ladder below, structured application programming interface (API) access is an intermediate operational mechanism proposed by this perspective; it is not a separate category in Casper *et al.*'s taxonomy.

A practical access ladder might look like this:

1. Public black-box audit: controlled observation of results, suggestions, rankings, components, and variation.
2. Author-proposed structured API access: controlled access to outputs, metadata, and testing interfaces.
3. Grey-box audit: limited access to internal documentation, feature categories, testing data, or aggregate logs.
4. White-box or outside-the-box audit: secure review of internal evaluations, policy decisions, model documentation, training or ranking data summaries, and deployment practices.

Secure Audit Environments

Access to increased resources should never mean freedom to copy or expose sensitive data. The work of Casper *et al.* offers an approach on how to create safe environments where auditing can take place without endangering the level of safety (12). Such an approach includes structured APIs, a safe environment, technical assistance, and confidentiality procedures. The hybrid audit governance framework need to follow such precautions. An auditor can have access to sensitive information, provided it is done safely and publicly reported on it.

Privacy-Preserving Data Access

Independent third-party audits must be planned according to privacy by design concept. This concept entails that issues related to privacy should be included in the engineering process and requirement definition as discussed by Rubinstein and Good (17). In the case of independent third-party audits of search engines, privacy by design requires data minimization, data aggregation, data retention, data redaction, access logging, and strict control on user's data. The hybrid audit governance framework needs to ask the critical question about "how much of sensitive data will be minimum for answering the auditing question?" If aggregated data or synthetic data would suffice then any access to the actual data must be prevented.

Selective Public Reporting

While the public has a right to accountability, it does not have to be a right to know all the technical details of how things work. The reports that should be released to the public should indicate audit scope and process, types and limitations of access, key audit findings, outstanding risks, cooperation by the website platform, whether any remedies were necessary, and the need for further audits. This way, both accountability and confidentiality can be preserved.

Complaints and Remedies Process

An independent third-party audit should not be just a report on what has been seen without doing anything about it. The independent complaint procedure by Laidlaw has to become part of the hybrid audit governance framework (1). Complaints from all stakeholders who may include end-users, academics, civil society groups, journalists and publishers have to be allowed to bring up their complaints with the matter at hand. There should be a mandate from the auditing body

to investigate any legitimate complaint received from any quarter.

The theory of accountability therefore becomes applicable. An effective audit theory should involve processes that provide information, deliberation, and consequence. Information that does not undergo deliberation leaves citizens with mere facts but no interpretation. Deliberation that does not result into consequences turns accountability into merely discussion. The proposed hybrid audit governance framework needs all three (13).

OBJECTIONS AND LIMITATIONS

The first concern regarding the framework is the cost it may place on private firms. As argued in Section 1, this perspective ties these quasi-public obligations specifically to the public-interest role of search engines rather than to private ownership generally (1, 2, 20).

Second, audits can also turn into mere audit theatrics, posing real risks to organizations. Casper *et al.* point out that bad audits can create a false sense of assurance and allow for safety and ethics washing activities (12). Similarly, Manheim *et al.* argue that existing approaches can be dangerous where they are built on poor standards, fragmentation, or procedures affected by industry control (18). The answer to this criticism is that this paper does not promote independent third-party audits for their own sake, but independent third-party audits operating within the proposed hybrid audit governance framework.

Third, the fast rate of change could make an audit unnecessary. Such a claim has some merit to it. In a study, Ulloa *et al.* prove the need for proper infrastructure when auditing search engines and highlight that there is a constant development going on in websites, thus, maintenance will have to be conducted regularly. Moreover, virtual agents have potential use for future audits, but the methodology involved is complicated (21).

Fourth, governance institutions may be prone to the problem of capture. This hypothesis is supported by relevant studies in literature. According to Mattli & Büthe, effective private delegation of governance relies on the nature of principal-agent relations (19). Thus, the standard-setting agency must guarantee that nobody—whether it is search engines, regulatory agencies or any other groups—has control over the operation of this institution. In contrast, it should comprise professional experts in their field, members of civil societies, people dealing with privacy issues, etc.

Fifth, political speech is highly reactive to regulatory oversight. The above thesis therefore chooses not to leave it to governments to regulate search ranking. While we have avoided suggesting who exactly occupies the leading positions among the political actors whose voices we wish to amplify, we have created an evaluation process that measures the way search engine companies perform in politically significant situations. There lies a fundamental difference: Government regulation of speech is very different from the evaluation of whether a gatekeeper is acting properly.

CONCLUSION

Taken together, the preceding sections support this perspective's position that search-engine accountability should not take the form of complete transparency, direct governmental control, or an impossible requirement of neutrality. Goldman and Manne and Wright make a valid point about the responsibility of search engines to use judgment (9, 10); at the same time, the literature discussed here supports the need for independent scrutiny (1, 2, 11, 12).

The practical implication is that policymakers, search providers, standards organizations, researchers, and civil-society groups should begin developing and piloting standards for independent third-party audits of search engines. The next step should not be a vague call for transparency, but a concrete effort to test graduated access models, establish auditor accreditation mechanisms, design secure audit environments, and create public reporting and complaint procedures. Under the hybrid audit governance framework proposed here, search engines need not disclose all of their information to the public, but they should be subject to independent and meaningful third-party audits.

REFERENCES

1. Laidlaw EB. Private power, public interest: An examination of search engine accountability. *Int J Law Inf Technol*. 2009; 17 (1): 113-145. doi:10.1093/ijlit/ean018.
2. Bracha O, Pasquale F. Federal Search Commission? Access, fairness, and accountability in the law of search. *Cornell Law Rev*. 2008; 93 (6): 1149-1210.
3. Diakopoulos N. Algorithmic accountability: on the investigation of black boxes. New York: Tow Center for Digital Journalism, Columbia Journalism School; 2014. <https://doi.org/10.1080/21670811.2014.976411>
4. Robertson RE, Lazer D, Wilson C. Auditing the personalization and composition of politically-related search engine results pages. In: Proceedings of the 2018 World Wide Web Conference. New York: Association for Computing Machinery. 2018; p. 955-965. doi:10.1145/3178876.3186143.
5. Urman A, Makhortykh M, Ulloa R. The matter of chance: auditing web search results related to the 2020 U.S. presidential primary elections across six search engines. *Soc Sci Comput Rev*. 2022; 40 (5): 1323-1339. doi:10.1177/08944393211006863.
6. Lin C, Gao Y, Ta N, Li K, Fu H. Trapped in the search box: an examination of algorithmic bias in search engine autocomplete predictions. *Telemat Inform*. 2023; 85: 102068. doi:10.1016/j.tele.2023.102068.
7. Dash S, Rezapour A, Shah C. Fairness in image search: a study of occupational stereotyping in image retrieval and its debiasing. arXiv. 2023. doi:10.48550/arXiv.2305.03881.
8. Paramita ML, Kasinidou M, Kleanthous S, Hopfgartner F. Towards improving user awareness of search engine biases: a participatory design approach. *J Assoc Inf Sci Technol*. 2024; 75 (5): 581-599. doi:10.1002/asi.24826.
9. Goldman E. Search engine bias and the demise of search engine utopianism. *Yale J Law Technol*. 2006; 8: 188-200.
10. Manne GA, Wright JD. If search neutrality is the answer, what's the question? Arlington (VA): International Center for Law & Economics; 2011. <https://doi.org/10.2139/ssrn.1807951>
11. Bandy J. Problematic machine behavior: a systematic literature review of algorithm audits. *Proc ACM Hum Comput Interact*. 2021; 5 (CSCW1): Article 74. doi:10.1145/3449148.
12. Casper S, Ezell C, Siegmann C, Kolt N, Curtis TL, Bucknall B, et al. Black-box access is insufficient for rigorous AI audits. In: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency. New York: Association for Computing Machinery; 2024. doi:10.1145/3630106.3659037.
13. Brandsma GJ, Schillemans T. The accountability cube: measuring accountability. *J Public Adm Res Theory*. 2013; 23 (4): 953-975. doi:10.1093/jopart/mus034.
14. Greiling D, Spraul K. Accountability and the challenges of information disclosure. *Public Adm Q*. 2010; 34 (3): 338-377
15. Levine DS. Secrecy and unaccountability: trade secrets in our public infrastructure. *Fla Law Rev*. 2007; 59 (1): 135-186.
16. Pasquale F. The black box society: the secret algorithms that control money and information. Cambridge (MA): Harvard University Press; 2015.

- <https://doi.org/10.4159/harvard.9780674736061>
17. Rubinstein IS, Good N. Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technol Law J.* 2013; 28 (2): 1333-1413. <https://doi.org/10.2139/ssrn.2128146>
 18. Manheim D, Martin S, Bailey M, Samin M, Greutzmacher R. The necessity of AI audit standards boards. *AI Soc.* 2025; 40: 6609-6624. doi:10.1007/s00146-025-02320-y.
 19. Mattli W, Büthe T. Accountability in accounting? The politics of private rule-making in the public interest. *Governance.* 2005; 18 (3): 399-429. doi:10.1111/j.1468-0491.2005.00282.x.
 20. Trebilcock MJ, Iacobucci EM. Privatization and accountability. *Harv Law Rev.* 2003; 116 (5): 1422-1453. <https://doi.org/10.2307/1342731>
 21. Ulloa R, Makhortykh M, Urman A. Scaling up search engine audits: practical insights for algorithm auditing. *J Inf Sci.* 2024; 50 (2): 404-419. doi:10.1177/01655515221093029.