Science as Culture

ISSN: 0950-5431 (Print) 1470-1189 (Online) Journal homepage: www.tandfonline.com/journals/csac20

Governing by dismantling: tech oligarchy and the stifling of public data infrastructure

Louis Ravn, Bokar N'Diaye, Katie Mackinnon, Nanna Bonde Thylstrup & Dmitry Muravyov

To cite this article: Louis Ravn, Bokar N'Diaye, Katie Mackinnon, Nanna Bonde Thylstrup & Dmitry Muravyov (20 May 2026): Governing by dismantling: tech oligarchy and the stifling of public data infrastructure, Science as Culture, DOI: 10.1080/09505431.2026.2666073

To link to this article: https://doi.org/10.1080/09505431.2026.2666073

Published online: 20 May 2026.

SCIENCE AS CULTURE
https://doi.org/10.1080/09505431.2026.2666073

Routledge
Taylor & Francis Group

FORUM ARTICLE

Governing by dismantling: tech oligarchy and the stifling of public data infrastructure

Louis Ravn [a], Bokar N'Diaye [a], Katie Mackinnon [b], Nanna Bonde Thylstrup [b] and Dmitry Muravyov [c]

[a]Institute for Logic, Language and Computation, University of Amsterdam, Amsterdam, Netherlands; [b]Department of Arts and Cultural Studies, University of Copenhagen, København S, Denmark; [c]TU Delft, Department of Values, Technology & Innovation, The Ethics and Philosophy of Technology Section, Delft, the Netherlands

ARTICLE HISTORY Received 25 July 2025; Accepted 24 April 2026
KEYWORDS Tech oligarchy; data stifling; DOGE; public data infrastructure

Introduction

The ongoing consolidation of state and techno-economic power worldwide calls for the development of a new critical vocabulary. At this juncture, the concept of tech oligarchy has been proposed by scholars like Cohen (2025), highlighting how select individuals – notably tech CEOs – are positioned to reshape state institutions according to their own interests. Most emblematically, the tech oligarchy in the US has materialized in the form of the non-governmental advisory commission styled as the 'Department of Government Efficiency' (henceforth DOGE) and its orchestration of wide-ranging, technologically-mediated reconfigurations of federal agencies (Flavelle *et al.*, 2025; Pulley, 2025). As reported, DOGE has focused on reshaping essential public data infrastructures and systems, whether with respect to knowledge (Schneider, 2025), societal memory (Garber, 2025), or social services provision (Kelly, 2025).

These reconfigurations illustrate a deeply contradictory relationship between the tech oligarchy and public data infrastructure. By *public data infrastructure* we broadly refer, here and throughout this piece, to basic digital data systems that support the provision of essential public services or enable public access to data. On one hand, DOGE has gained access to the databases of various agencies, prominently including those of the Social Security Administration (Berzon *et al.*, 2025) and the Department of Health and Human Services (Giles *et al.*, 2025). Once access has been obtained, control over these data systems is then often leveraged to merge previously distinct databases (Kelly

CONTACT Louis Ravn l.ravn@uva.nl FNWI, ILLC, Universiteit van Amsterdam, P.O. Box 94242, Amsterdam 1090 GE, Netherlands

and Elliott, 2025a) – a pursuit of 'interoperability' (Archer *et al.*, 2025) aimed at intensifying the surveillance of already marginalized people (Monahan, 2025). These examples illustrate the insight that access to and control over digital data is an essential aspect of data-based statecraft (Fourcade and Gordon, 2020).

On the other hand, however, DOGE also engages in the strategic dismantling of public data infrastructure: it has gutted the digital services agency 18F (Pulley, 2025), haphazardly parted from the long-established COBOL programming language (Kelly, 2025), and terminated the production of specific datasets (Schneider, 2025; The Economist, 2025; Thylstrup and MacKinnon, 2025). These examples suggest that the tech oligarchy's data governance practices cannot be conceptually reduced to the consolidation of public data infrastructures. Instead, analyses of tech oligarchic data governance must also account for the strategic dismantling of particular public data infrastructures.

In this Forum Article, thus, we examine how the tech oligarchy governs public data infrastructures by accessing, merging, and dismantling them. Centering the deliberate nature of these infrastructural reconfigurations allows us to more finely question the incentives and rationales of said actors, whether conducive to wealth accumulation (Cohen, 2025), or alignment with the government's political goals (Berzon *et al.*, 2025). Doing so also establishes tech oligarchic actors' responsibility for the severe effects of these rearrangements of public data infrastructure, including the degradation of scientific knowledge (Schneider, 2025), the erosion of data privacy (Levy, 2025; see also Trahan, 2025), and the risks incurred by vulnerable people dependent on state services to fulfill essential needs (Kelly, 2025). Thus, the objective of this article is to foreground how the tech oligarchy's reconfiguration of public data infrastructures surfaces a strategic tendency toward infrastructural degradation.

To ground our analysis, we draw from the STS concepts of ontological politics (Mol, 2002) and stifling (Valkenburg, 2026) as well as the framework of agnotology (Proctor and Schiebinger, 2008, 2025). While Mol's (2002) analysis of ontological politics highlights the technoscientific practices which enact realities into being, Valkenburg (2026, p. 3) extends this by attending to practices that move things '*away* from existence and stability rather than toward them.' Concretely, he highlights that the non-existence of things, knowledge, and people are likewise the result of technoscientific enactments – practices he calls 'stifling.' Building on this notion, we argue that tech oligarchic power materializes through *data stifling:* i.e. deliberate interventions into public data infrastructures that degrade knowledge, memory, and people's lives. The concept of data stifling serves to underscore that these public infrastructural reconfigurations constitute an exercise in ontological politics: they materially constrain modes of existence. We further situate data stifling within the literature on agnotology, where scholars argue that ignorance is not an absence but a socially and materially produced condition, made and stabilized through institutions, practices, and infrastructures (Proctor and Schiebinger, 2008, 2025;

Thylstrup, 2025). From this agnotological perspective, data stifling becomes analytically legible not merely as data loss or administrative change, but as a set of infrastructural interventions that actively reshape what can be known, remembered, and acted upon.

Our contribution is thus twofold. Conceptually, we propose data stifling to underscore the tech oligarchy's deliberate interventions into public data infrastructures that degrade knowledge, memory, and people's lives. Empirically, we show how the case of DOGE manifests three distinct modalities of data stifling – namely, access, merging, dismantling – that each enact different stakes and targets, from individual privacy through welfare service provisions to collective institutional memory. Hence, we contribute to this Special Forum by positioning *data stifling* as both a central tactic of tech oligarchic governance and a broader mechanism within contemporary knowledge-ignorance politics.

This article proceeds in four steps. First, we provide a brief prehistory of the relationship between political power and public data infrastructural control in the US context. Building on this, we mobilize STS and history of science frameworks to formulate the concept of *data stifling*. Third, we analyze several examples showing how DOGE – as a materialization of tech oligarchic power – has strategically accessed, merged, and dismantled public data infrastructures. We close by discussing how tech oligarchic data stifling is already being resisted.

Political power and data infrastructural control in the US: a prehistory

Despite the seemingly abrupt removal of government web pages and data infrastructures, changes to information are expected to accompany transitions of power. Since 2004 – and the first large-scale effort to archive 75 million web pages from 1,370 civilian and military domains by the independent federal agency National Archives and Records Administration (NARA) (Jacobs and Jacobs, 2025) – frictions tied to the transformation of governmental websites between administrations are a staple in the US context. In 2008, NARA decided to discontinue this systematic archiving effort, which came at the end of George W. Bush's first term in office. Their justifications included significant resource constraints and a strict interpretation of federal records laws (Jacobs and Jacobs, 2025), as well as the subsequent constitution, and the creation of the End of Term Web Archive (EOT Archive) – a voluntary collaboration between archival institutions, major universities, and the Internet Archive (Seneca *et al.*, 2012).

Although the EOT Archive's activities have been ongoing since 2008, the 2016 election of Donald Trump raised new concerns. His administration's open hostility towards certain topics (e.g. diversity, climate change, etc.) engendered worries about the risk of important scientific data related to climate change being removed during the transition. In response, a number of data

archiving initiatives were formed, such as the Guerilla Archiving Event and several Data Refuge projects (Vera *et al.*, 2018). Similar grassroots efforts emerged with Trump's 2025 re-election (Thylstrup and MacKinnon, 2025). However, a significant turn with the 2025 Trump administration is the strategic mobilization of governmental power to stifle public archival institutions, public data storage facilities, and public data commons (Ovenden, 2025). For instance, using software that tracks .gov domains for changes, grassroots archivists have documented new US government websites containing lists of 'wasteful projects,' seemingly assembled by DOGE (see Figure 1; Reuter, 2025). More broadly, these efforts far outstrip the anticipated content churn between administrations, exemplifying instead an orientation toward infrastructural interventions that condition what remains legible and governable.

Data infrastructures are 'fluid and heterotemporal' (Velkova, 2023, p. 435), and therefore constantly moving and adjusting in their processes of assembly and disassembly (Latour and Yaneva, 2008). Because they are moreover sociomaterial, the damage caused by infrastructural dismantling is not limited to servers, codebases, or datasets; it also affects the routines, competencies, and trust relations that sustain information ecosystems. While systematic ethnographic evidence of emotional and organizational effects of DOGE's practices will take time to document, early whistleblower accounts and internal communications indicate severe disruption to government institutional capacity and continuity as well as expressions of what we might call institutional trauma (Cook, 2025; Dietkus, 2025). Public data infrastructures intricately shape societies' sense of what can be known and acted upon by governments; hence, dismantling that infrastructure undermines the capacity of governments to act. The following section ground this observation conceptually.

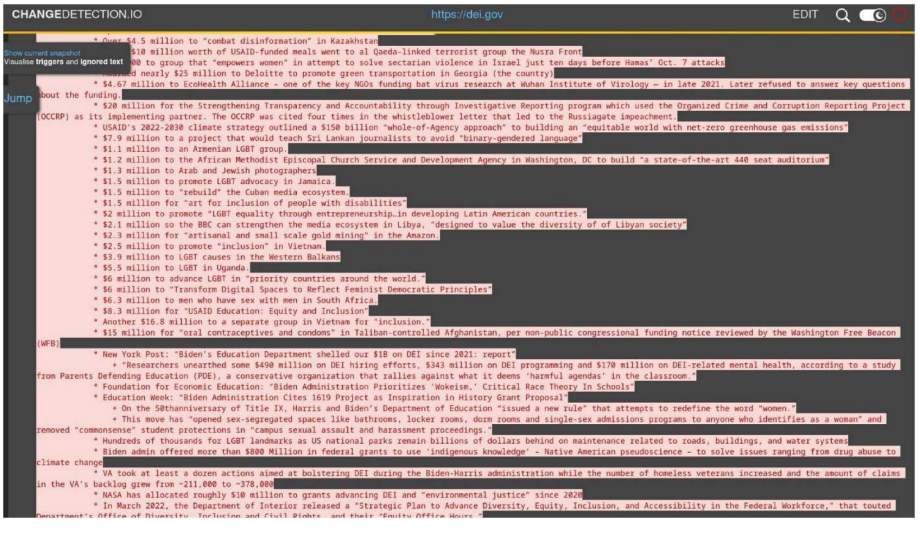

Figure 1. List of 'wasteful projects' ostensibly assembled by DOGE (Reuter, 2025).

Forgetting, ignorance, and epistemic injustice enacted through data infrastructures

STS and history of science offer valuable conceptual vocabularies for analyzing how realities and knowledges are produced, enacted, and actively contested. In the following, we draw from the related STS concepts of ontological politics and stifling (Mol, 2002; Valkenburg, 2026) as well as the framework of agnotology (Proctor and Schiebinger, 2008; Galison, 2025; Thylstrup, 2025).

The concept of ontological politics was developed by STS scholar Annemarie Mol (1999, 2002), whose analyses highlighted that technoscientific practices enact the realities of what they describe or represent. Her central insight was that the realities – the ontologies – of scientific objects and knowledges do not precede the practices through which they are enacted. To use an example from Mol's (2002, p. 6) analysis, the ontology of a particular disease emerges from how that disease is 'brought into being, sustained, or allowed to wither away in common, day-to-day, sociomaterial practices.' For our analytical purposes, an important implication is that the constitution of scientific objects, knowledge, and memory depends on their enactment into being.

Valkenburg (2026) extends the analysis of ontological politics by arguing that STS scholars should not only attend to how ontologies – as modes of existence – are enacted. Rather, he argues that the non-existence of objects, knowledges, and people must likewise be understood as enacted. Concretely, he draws attention to practices that move things away from stability, legibility, and endurance rather than toward them. He dubs these practices '*stifling*,' reflecting 'the production of invisibility, irrelevance, silence, unthinkability, and other forms of non-existence' (ibid., p. 6). As such, the concept of stifling extends scholarship on ontological politics by directing analytical attention to those practices that hamper the existence of specific objects, knowledges, and people. Put differently, stifling emerges as a particular form of ontological politics that is oriented towards enacting the invisibility, irrelevance, or even non-existence of specific knowledges, forms of memory, and people. Thus, the related concepts of ontological politics and stifling have analytical utility for our analysis because they sensitize us to how collective forms of knowledge, memory, and social actors are actively rendered fragile, irrelevant, invisible, or non-existent through the tech oligarchy's reconfiguration of public data infrastructures.

The framework of agnotology sharpens this perspective by insisting that ignorance is not reducible to error, uncertainty, or missing information, but must be analyzed as an outcome of social, political, and material processes (Proctor and Schiebinger, 2008, 2025). Crucially, contemporary digital ignorance studies extend this insight beyond discursive manipulations to include infrastructures, institutions, and technical systems as central sites of ignorance production (Thylstrup, 2025). From this viewpoint, ignorance is engineered,

maintained, and stabilized through digital sociomaterial arrangements, and digital data infrastructures render these dynamics particularly visible. If epistemic orders depend on classification systems, archives, protocols, and storage regimes (Bowker and Star, 1999; Bowker, 2005), then interventions into such infrastructures inevitably carry epistemic consequences. Ignorance can be produced not only through denial or misinformation, but through permissions, interfaces, APIs, archival policies, and the maintenance – or withdrawal – of data production pipelines. What becomes at stake is not solely what is known, but what can be known at all. The agnotological sensitivity to how ignorance is actively and sociotechnically produced is useful for our purposes because it guides our attention to how particular forms of strategic ignorance result from the ways in which the tech oligarchy governs public data infrastructures.

Building on these traditions, we conceptualize *data stifling* to direct attention to the tech oligarchy's strategic reconfigurations of public data infrastructures that curb the conditions under which knowledge, memory, and social actors remain durable, accountable, and actionable. As such, data stifling extends agnotology by naming a distinct modality of ignorance production operating through public data infrastructures. Rather than treating data loss or infrastructural change as secondary effects, data stifling foregrounds them as mechanisms through which epistemic and ontological orders are actively reorganized. Seen this way, data stifling becomes analytically legible as a form of ontological politics and ignorance production: a means through which the durability of knowledge, the stability of records, and the legibility of social actors are unevenly redistributed.

The practices and politics of *data stifling*

In the following, we showcase how data stifling figures as a central component of the tech oligarchy's techno-political repertoire, using examples related to DOGE. We analyze three different modes in which data stifling plays out: first, by accessing sensitive data systems; second, by merging disparate databases; and third, by dismantling existing public data infrastructure.

Accessing data systems: privacy politics

> Waste, fraud, and abuse have been deeply entrenched in our broken system for far too long. […]. It takes direct access to the system to identify and fix it. (Harrison Fields, February 2025)

A core component of emerging data stifling practices is enforcing and gaining access to federal databases. While state power has long depended on the scope of its access to data (Fourcade and Gordon, 2020), DOGE introduces a novelty:

a tech oligarchic actor, positioning itself as a proxy for the state, enforcing access to systems previously off-limits.

Most prominently, this has included accessing databases at the Social Security Administration (SSA) (Berzon *et al.*, 2025), the Department of Health and Human Services (HHS) (Giles *et al.*, 2025), the Department of Labor (DOL) (Feiger and Elliott, 2025), and the National Labor Relations Board (NLRB) (McLaughlin, 2025). Significantly, access is commonly demanded not on a 'read-only' basis, but as including extensive permissions, for example 'unrestricted permission to read, copy and alter data' at the NLRB (McLaughlin, 2025) or the capacity to 'navigate the entire file system, change user permissions, and delete or modify critical files' at the Treasury Department (Elliott *et al.*, 2025b). Despite struggles over DOGE's capacity to access federal data systems, it has usually prevailed – also aided by Supreme Court rulings (Liptak and VanSickle, 2025).

Gaining such access and control over these data systems relates to data stifling in two ways. On an immediate level, it constitutes serious privacy infringements, implying direct risks for people whose sensitive data has become accessible in this way – whether related to employee complaints (McLaughlin, 2025), migrant children (Robins-Early, 2025), or visa applicants (Giles *et al.*, 2025). Specifically, illicit access operates as stifling by making people newly legible to scrutiny while simultaneously weakening their capacity to contest how they are categorized, assessed, or acted upon. Similarly concerning is that DOGE accesses sensitive federal data systems without requiring its operatives to undergo the otherwise mandatory cybersecurity training, engendering profound cybersecurity concerns as a result (McLaughlin, 2025). The acceleration of access without governance further results in temporal stifling: by framing state operations as needing constant 'course-correction' rather than stable rule-based legality, where remediation becomes politically impossible, DOGE normalizes a hasty re-engineering of the state that renders oversight obsolete (Roberge *et al.*, 2026). It thereby gives its patrons the prerogative to punitively undermine their chosen targets, from the ventures of political opponents (Bellodi and Lee, 2025) to the civil rights of vulnerable populations.

Merging data sets: interoperability politics

> The way the government is defrauded is that the computer systems don't talk to each other. (Elon Musk, April 2025)

Having enforced access to various sensitive databases, a second central aspect of data stifling encompasses the *merging* of previously distinct data sets and infrastructures in the name of interoperability. While interoperability has long been a feature of tech companies' discourses, as in the case of Meta (Bechmann, 2013; Thylstrup, 2018), the more recent spread of Palantir's systems in the security

sector is instructive here. Describing itself as 'interoperable to the core,' Palantir's systems are typically employed to facilitate the fusion of previously distinct data systems in security contexts (Archer *et al.*, 2025). These logics materialize in DOGE's merging of data systems.

Kickstarted by an executive order to eliminate data silos (Levy, 2025), DOGE has stitched together datasets from, for example, the Social Security Administration, the Department of Homeland Security, and the Internal Revenue Services (IRS) (Kelly and Elliott, 2025a). The aim behind fusing and centralizing these datasets into a 'master database' (Kelly and Elliott, 2025a) has been to enhance the surveillance of targeted immigrants, aimed at supporting the Trump administration's broader immigration crackdown. What is stifled here is both privacy and the protective function of separation: that is, the institutional boundaries that previously limited cross-domain inference, which become increasingly porous, enabling new forms of composite suspicion and administrative action. The organization by DOGE of large hackathons aimed at producing a single 'mega API' allowing disparate software systems to cross-communicate (Kelly, 2025), leaves little doubt as to the interests of tech oligarchs in handling and centralizing such sensitive datasets.

Both dataset merging and API developments operate through a questionable imaginary of interoperability as inherently good, achieved by breaking down silos. While alluring, this prospect overlooks key nuances of the politics of interoperability (Archer *et al.*, 2025; Bellanova *et al.*, 2025): for example, it benefits some at the expense of others and it usually depends on collaborations with problematic firms like Palantir. Significantly, interoperability here serves as a precondition for surveilling and persecuting immigrants, whose deportation is a priority for Trump. Tech oligarchic practice is thus shaped not only by economic imperatives (e.g. enrolling Palantir), but by the performance of shared conservative values (e.g. anti-migrant ideology). By rendering targeted groups traceable, these infrastructural reconfigurations exemplify how tech oligarchs problematically shape living conditions through data systems.

Dismantling data infrastructure: knowledge and memory politics

> So we have to really delete entire agencies, many of them. (Elon Musk, February 2025)
> Agencies shall utilize enforcement discretion to de-prioritize enforcement actions that stretch statutory authority or exceed the constitutional powers of the Federal Government. (White House Executive Order, February 2025)

A third mode of data stifling is constituted by the partial or complete *dismantling* of existing public data infrastructures. Conceptually, dismantling is a form of intentional infrastructural undoing characterized by an abruptness that is absent from related modalities of infrastructural takedown, such as abandonment (Brodie and Velkova, 2021), or ruination (Stoler, 2008). Instead, dismantling can be seen as more closely related to politically charged forms of

infrastructural destruction (Burke, 2010) and erasure (Fredrikzon and Haffenden, 2023), evidenced in both the modus operandi and optics of DOGE.

First, DOGE has sought to replace COBOL, a programming language known for its enduring stability and foundational role in the Social Security Administration's infrastructure (Renderos, 2025). Choosing rapid migration to a new system within a few months not only put millions of people at risk of not receiving their benefits (Kelly, 2025), but also served to justify the displacement of COBOL-trained government workers in favor of new, DOGE-compliant hires. This entailed the appointment of six 'promising young coders,' each under 25 and with unconventional credentials, tasked with orchestrating sweeping budget and personnel cuts within at least nine federal departments and agencies (Elliott *et al.*, 2025a). One of them, 23-year old Luke Farritor, was reportedly still learning COBOL on the job, simultaneously querying his public X followers for large language models (LLMs) capable of automating basic document format conversion (Revolving Door Project, 2025). While DOGE enthusiasts celebrate such hires as meritocratic innovation (Makridis, 2025), this tactic is thus better understood as an example of data stifling through which situated institutional knowledge is erased, infrastructural authority reordered, and the capture of public data infrastructure accelerated.

Second, another example is the gutting of 18F, a digital services agency founded in 2014 to support the adoption of best practices and technology products in federal agencies (Pulley, 2025). As Pulley (2025) showed, 18F had actually been shown to improve the delivery of important government services, which illustrates that efficiency is not DOGE's goal (cf. Cohen, 2025). In other cases, it is the production of specific datasets that has been ended; for example, datasets made by the US Census Bureau (Schneider, 2025). Such acts erode the availability of essential information to researchers.

Last, and related to questions of social memory, DOGE claimed to have orchestrated the migration of 14,000 magnetic records of the General Services Administration to what they describe as 'permanent modern digital records' (Cole, 2025). Not only does this overlook that magnetic digital tapes in many comparable cases are the most cost-efficient storage technology (Sparkes, 2025), it also omits the particular long-term vulnerabilities of newer forms of data storage, such as hardware failure in cloud systems (Stokel-Walker, 2025). These examples constitute strategic erosions of public data infrastructure, whether by gutting digital service agencies, breaking away from infrastructural programming languages, or terminating the production of datasets.

Collectively, these practices of dismantling public data infrastructure illustrate the politics of data stifling, related to the strategic undermining of digital knowledge, memory, and infrastructure (i.e. agnotology). These practices erode access to knowledge, resulting in the production of ignorance (Proctor and Schiebinger, 2008; Thylstrup, 2025). Beyond hampering knowledge production, dismantling also introduces and normalizes gaps within

public information infrastructures, gaps that later become difficult to detect, contest, or repair. Data stifling therefore indicates a tech oligarchic interest in strategic ignorance and forgetting, whether economically or politically motivated; practices of forgetting that are partially afforded by the inherent modifiability and impermanence characterizing data infrastructures (Velkova, 2025).

Further, the dismantling of public data infrastructure produces new infrastructural instabilities, as when the provision of social services becomes endangered through haphazard programming language migrations. Long-embedded systems, such as COBOL, become visible not by accidental breakdown (cf. Bowker and Star, 1999), but by strategic dismantling. Most importantly, as we have sought to stress throughout this paper, data stifling *as* dismantling of public data infrastructure ultimately constitutes a form of ontological politics: the accessibility of knowledge is eroded, societal memory made more fragile, and people's livelihoods consequently made precarious.

Conclusion

In this Forum Article, we argued that tech oligarchic power materializes through *data stifling:* that is, strategic reconfigurations of public data infrastructures that curb the conditions under which collective knowledge, memory, and social actors remain durable, accountable, and actionable. Our analysis of DOGE highlighted three salient, distinct modalities of data stifling: (a) the enforcement of *access* to federal data systems, (b) the *merging* of previously distinct datasets and databases, and (c) the *dismantling* of data infrastructures. Calling these infrastructural interventions data stifling highlights that they constitute an exercise in ontological politics insofar as they reshape material realities: illicit access endangers privacy, merging accelerates surveillance of already marginalized groups, and dismantling erodes essential knowledge and social memory.

From an agnotological perspective, these are not merely losses but infrastructural techniques for producing durable uncertainty (Proctor and Schiebinger, 2008, 2025). Hence, once data production pipelines are terminated or scrambled, some questions either cannot be answered with data, or, conversely, become answerable only through costly, partial, or privately mediated substitutes. These substitute data infrastructures – some of which we detail below – aspire to maintain the public accessibility to essential data over time, yet often rely on unstable forms of volunteer labor by activists, researchers, archivists, and librarians (Lucas, 2025). The broader point is that in contemporary digital societies, as we have argued throughout this article, public data infrastructures constitutively shape conditions of livelihoods, modes of governance, systems of knowledge, and stores of memory. Drawing from the frameworks of ontological politics, stifling, and agnotology helped us underscore this: the strategic reconfigurations of public data infrastructures by tech oligarchs are tantamount to not only enacting particular realities – as an analysis of ontological

politics would reveal – but also unmaking specific modes of existence, knowledge, and memory.

We hope to contribute to the critical study of tech oligarchy by raising awareness of the paradoxical relationship between tech oligarchic power and public data infrastructures. Even though the extraction, accumulation, and retention of data remains central to data-driven statecraft (Fourcade and Gordon, 2020), our analysis stresses the need to contend with the dismantling, loss, erasure, and outright destruction of public data infrastructures as an urgent and qualitatively distinct problem. Data stifling names this infrastructural dismantling as a specific tactic of tech oligarchic data governance: a mode of power exercised through strategic subtraction, i.e. terminating datasets, breaking maintenance chains, and reorganizing access, so that absence and instability become politically productive. While data infrastructures have always been subject to change (Bowker, 2005; MacKinnon, 2022; Velkova, 2025), conditions of tech oligarchy enable a select range of individuals to abruptly modify public data infrastructure in accordance with their own interests.

Yet, data stifling does not present us with a fait accompli. The various dismantlings of public data infrastructures in the US are actively being resisted by university researchers, librarians, the Internet Archive, and the Reddit Data Hoarders, among others (Lucas, 2025; Maemura and Wagner, 2025). These actors systematically archive various forms of federal data at risk of inaccessibility, modification, or loss. Thus, just as data stifling becomes engrained in the politics of the US tech oligarchy (Kelly and Elliott, 2025b), so too does the resistance to erasures of data infrastructure – exemplified by initiatives such as the Data Rescue Project (DRP, 2025), the Environmental Data Governance Initiative (EDGI, 2025), or CDC Restored (CDC Restored, 2025). These initiatives are invaluable, yet they nevertheless cannot remain the principal answer to the erasure and fragilization of digital memory in the US and elsewhere (Ovenden, 2025). While better grasping the practices and politics of tech oligarchy is an important critical endeavor, the deeper implication of understanding data stifling as a result of tech oligarchic conditions is that these very conditions ought to be resisted.

Author contributions

CRediT: **Louis Ravn:** Conceptualization, Writing – original draft, Writing – review & editing; **Bokar N'Diaye:** Conceptualization, Writing – original draft, Writing – review & editing; **Katie Mackinnon:** Conceptualization, Writing – original draft, Writing – review & editing; **Nanna Bonde Thylstrup:** Conceptualization, Writing – original draft, Writing – review & editing; **Dmitry Muravyov:** Conceptualization, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The writing of this article was generously supported by the European Research Council under the grants "Deep Culture – Living with Difference in the Age of Deep Learning" (Grant no. 101141330) as well as "Data Loss: The Politics of Disappearance, Destruction and Dispossession in Digital Societies" (Grant no. 101078386).

Notes on contributors

Louis Ravn is a PhD Candidate on the Deep Culture project at the University of Amsterdam. In this context, his research focuses on the epistemics, politics, and materialities of data and deep learning techniques. His primary research interest lies in better understanding how contemporary deep learning is increasingly shaped by sociotechnical operations of synthesis, compression, and distillation. To that end, he draws from frameworks across science and technology studies (STS), critical AI studies, critical data studies, and social theory. Before joining Deep Culture, he was a Research Assistant at the University of Copenhagen. His research has been published in Big Data & Society, Internet Policy Review, Surveillance & Society, and Digital Society.

Bokar N'Diaye is a PhD Candidate in the ERC-funded Deep Culture project at the University of Amsterdam. Trained in the comparative anthropology of religions and digital humanities at the University of Geneva, his research examines the cultural adoption and disputed authorities of generative machine learning models, especially inasmuch as they depend on the tacit interests, informal communities, or preferred narratives of certain actors on the genAI scene. Within the Deep Culture project, he explores how human creativity is mediated through deep learning implementations, and how users navigate and rationalize the uncertainty tied to AI outputs and anomalies. He has presented at conferences in STS and digital humanities, including 4S, NeurIPS, and MASSHINE, and his work has appeared in Hertziana Studies in Art History and Artl@s Bulletin.

Katie MacKinnon is a Postdoctoral Fellow on Data Loss (DALOSS): the politics of disappearance, destruction, and dispossession in digital societies at the University of Copenhagen. She researches historical, political, and ethical implications of long-term data storage across datasets, models, archives, and in the production of internet histories and futures.

Nanna Bonde Thylstrup is an Associate Professor in Modern and Digital Culture at the University of Copenhagen and Principal Investigator of the ERC-funded project Data Loss: The Politics of Disappearance, Destruction, and Dispossession in Digital Societies (DALOSS). Her research explores the political and ethical dimensions of data, machine learning, and digital infrastructures, with a particular focus on how loss, deletion, and transformation shape contemporary knowledge systems. She is the author and editor of several books, including The Politics of Mass Digitization (MIT Press) and Uncertain Archives: Critical Keywords for the Age of Big Data (MIT Press), and her work has been published in journals such as Big Data & Society, Media, Culture & Society, and Digital Journalism. Her current work develops a conceptual framework for understanding data loss not as failure, but as a constitutive feature of digital systems, with implications for how knowledge is produced, governed, and contested.

Dmitry Muravyov is a PhD Candidate at TU Delft, working as part of the AI DeMoS Lab. His PhD project explores the issues surrounding algorithmic fallibility—a shared condition of living with technology's breakdowns, failures, and errors. Dmitry is interested in how practitioners in different fields understand these notions, the philosophical, technical, and

historical roots of these concepts, and how people, individually and collectively, can live with fallible technologies. His research engages the fields, such as philosophy of technology, STS, design research, and critical data & algorithm studies.

ORCID

Louis Ravn http://orcid.org/0009-0005-4303-6905
Bokar N'Diaye http://orcid.org/0000-0002-7682-794X
Katie Mackinnon http://orcid.org/0000-0003-0928-5172
Nanna Bonde Thylstrup http://orcid.org/0000-0001-6094-2970
Dmitry Muravyov http://orcid.org/0000-0002-8568-2199

References

Archer, M., Ravn, L. and Thylstrup, N. B. (2025) The political economy of platformed silos: Theorizing data storage reconfigurations in the age of interoperability capitalism, *Big Data & Society*, 12(2), pp. 1–6.

Bechmann, A. (2013) Internet profiling: The economy of data interoperability on Facebook and Google, *MedieKultur: Journal of Media and Communication Research*, 29(55), pp. 72–91.

Bellanova, R., Pollozek, S. and Passoth, J. H. (2025) The technopolitics of interoperability in security, migration, and border control, *Big Data & Society*. Available at: https://journals.sagepub.com/page/bds/techno-politicsofinteroperability.

Bellodi, L. and Lee, K. (2025) The executive unbound: Politicized bureaucracy and partisan procurement under DOGE. Available at: https://lucabellodi.com/material/DOGE_Bellodi_Lee.pdf (accessed 16 February 2026).

Berzon, A., Nehamas, N. and Bernard, T. S. (2025) The bureaucrat and the billionaire: Inside DOGE's chaotic takeover of social security, *The New York Times*, June 16. Available at: https://www.nytimes.com/2025/06/16/us/politics/doge-social-security.html (accessed 18 July 2025).

Bowker, G. (2005) *Memory Practices in the Sciences* (Cambridge, MA: MIT Press).

Bowker, G. and Star, S. L. (1999) *Sorting Things Out: Classification and Its Consequences* (Cambridge, MA: MIT Press).

Brodie, P. and Velkova, J. (2021) Cloud ruins: Ericsson's Vaudreuil-Dorion data centre and infrastructural abandonment, *Information, Communication & Society*, 24(6), pp. 869–885.

Burke, P. (2010) Loss and gain: The social history of knowledge, 1750–2000. Available at: https://www.theoryculturesociety.org/blog/peter-burke-on-the-social-history-of-knowledge-1750-2000 (accessed 21 January 2026).

CDC Restored (2025) Mission. Available at: https://aboutus.restoredcdc.org/mission (accessed 12 May 2025).

Cohen, J. E. (2025) Oligarchy, state, and cryptopia, *Fordham Law Review*, 94, pp. 1–45. doi:10.2139/ssrn.5171050.

Cole, S. (2025) Another masterful gambit: DOGE moves from secure, reliable tape archives to hackable digital records, *404 Media*, April 8. Available at: https://www.404media.co/doge-gsa-magnetic-tape-archives-digital-storage/ (accessed 18 July 2025).

Cook, J. (2025) DOGE federal workers traumatizing workers. That costs money too, *US News and World Report*, March 19. Available at: https://www.usnews.com/opinion/articles/2025-03-19/trump-federal-workers-layoffs-doge-trauma (accessed 12 February 2026).

Data Rescue Project (DRP) (2025) About data rescue project. Available at: https://www.datarescueproject.org/about-data-rescue-project/ (accessed 12 May 2025).

Dietkus, R. (2025) The intentional weaponization of Trauma, *LinkedIn*, February 20. Available at: https://www.linkedin.com/pulse/intentional-weaponization-trauma-rachael-dietkus-lcsw–24jtc/?trackingId=85mk3L%2BDS9yoxbUSRWFVew%3D%3D (accessed 12 February 2026).

The Economist (2025) DOGE comes for the data wonks, March 31. Available at: https://www.economist.com/united-states/2025/03/30/doge-comes-for-the-data-wonks (accessed 19 January 2026).

Elliott, V., Gilbert, D. and Newman, L. H. (2025a). The young, inexperienced engineers aiding Elon Musk's government takeover, *Wired*, February 2. Available at: https://www.wired.com/story/elon-musk-government-young-engineers/ (accessed 3 April 2026).

Elliott, V., Mehrotra, D., Feiger, L. and Marchman, T. (2025b). A 25-year-old with Elon Musk ties has direct access to the federal payment system, *Wired*, February 4. Available at: https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/ (accessed 18 July 2025).

Environmental Data & Governance Initiative (EDGI) (2025) About. Available at: https://envirodatagov.org/about/ (accessed 18 July 2025).

Feiger, L. and Elliott, V. (2025) DOGE has access to sensitive labor department data on immigrants and farm workers, *Wired*, April 10. Available at: https://www.wired.com/story/doge-access-immigration-data-department-of-labor/ (accessed 18 July 2025).

Flavelle, C., Nehamas, N. and Tate, J. (2025) Missteps, confusion and 'viral waste': The 14 Days that doomed USA.I.D, *The New York Times*, June 22. Available at: https://www.nytimes.com/2025/06/22/us/politics/usaid-cuts-doge.html (accessed 18 July 2025).

Fourcade, M. and Gordon, J. (2020) Learning like a state: Statecraft in the digital age, *Journal of Law and Political Economy*, 1, pp. 78–108.

Fredrikzon, J. and Haffenden, C. (2023) Towards erasure studies: Excavating the material conditions of memory and forgetting, *Memory, Mind & Media*, 2, pp. 1–24.

Galison, P. (2025) Law against knowledge: Anti-epistemology, in: R. N. Proctor and L. Schiebinger (Eds) *Ignorance Unmasked: Essays in the New Science of Agnotology*, pp. 85–99 (Ch. 6) (Redwood City, CA: Stanford University Press).

Garber, M. (2025) Control. Alt. Delete, *The Atlantic*, February 27. Available at: https://www.theatlantic.com/culture/archive/2025/02/trump-doge-deletion-propaganda/681775/ (accessed 18 July 2025).

Giles, M., Feiger, L., Schiffer, Z. and Haskins, C. (2025) Here's all the health and human services data DOGE has access to, *Wired*, April 22. Available at: https://www.wired.com/story/doge-data-access-hhs/ (accessed 18 July 2025).

Jacobs, J. A. and Jacobs, J. R. (2025) *Preserving Government Information: Past, Present, and Future* (San Diego: FreeGovInfo Press).

Kelly, M. (2025) DOGE plans to rebuild SSA code base in months, risking benefits and system collapse, *Wired*, March 20. Available at: https://www.wired.com/story/doge-rebuild-social-security-administration-cobol-benefits/ (accessed 18 July 2025).

Kelly, M. and Elliott, V. (2025a). DOGE is building a master database to surveil and track immigrants, *Wired*, April 10. Available at: https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/ (accessed 18 July 2025).

Kelly, M. and Elliott, V. (2025b). This is DOGE 2.0, *Wired*, July 10. Available at: https://www.wired.com/story/next-stage-doge-elon-musk/ (accessed 23 July 2025).

Latour, B. and Yaneva, A. (2008) "Give me a gun and I will make all buildings move": An ANT's view of architecture, *Architectural Design Theory*, 1, pp. 103–111.

Levy, S. (2025) President Trump's war on 'information silos' is bad news for your personal data, *Wired*, April 4. Available at: https://www.wired.com/story/plaintext-trump-executive-order-information-silos-privacy/ (accessed 18 July 2025).

Liptak, A. and VanSickle, B. (2025) Justices grant DOGE access to social security data and let the team shield records, *The New York Times*, June 6. Available at: https://www.nytimes.com/2025/06/06/us/politics/supreme-court-doge-social-security.html (accessed 18 July 2025).

Lucas, J. (2025) The data hoarders resisting Trump's purge, *The New Yorker*, March 15. Available at: https://www.newyorker.com/news/the-lede/the-data-hoarders-resisting-trumps-purge (accessed 12 May 2025).

MacKinnon, K. (2022) The death of GeoCities: Seeking destruction and platform eulogies in web archives, *Internet Histories: Digital Technology, Culture and Society*, 6(1–2), pp. 237–252.

Maemura, E. and Wagner, T. L. (2025) 'Everyone has their reasons for curating the data they have decided to keep': A thematic analysis of data hoarding as digital curation practice, *Information Research*, 30, pp. 789–797.

Makridis, C. (2025) Overcoming the federal talent gap: Evidence from special governmental employees and other pathways. Available at SSRN 5315023.

McLaughlin, J. (2025) A whistleblower's disclosure details how DOGE may have taken sensitive labor data, *NPR*, April 15. Available at: https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security (accessed 18 July 2025).

Mol, A. (1999) Ontological politics: A word and some questions, *The Sociological Review*, 47(1), pp. 74–89.

Mol, A. (2002) *The Body Multiple: Ontology in Medical Practice* (Durham, NC: Duke University Press).

Monahan, T. (2025) Surveillance in Trump's America, *Surveillance & Society*, 23(1), pp. 1–16.

Ovenden, R. (2025) There is no political power without power over the archive, *The Observer*, July 12. Available at: https://observer.co.uk/news/international/article/there-is-no-political-power-without-power-over-the-archive (accessed 18 July 2025).

Proctor, R. N. and Schiebinger, L. (2008) *Agnotology: The Making and Unmaking of Ignorance* (Stanford, CA: Stanford University Press).

Proctor, R. N. and Schiebinger, L. (Eds) (2025) *Ignorance Unmasked: Essays in the New Science of Agnotology* (Stanford, CA: Stanford University Press).

Pulley, A. (2025) DOGE 'deleted' fed agency that strived for increased government efficiency, *The Badger Project*, May 8. Available at: https://thebadgerproject.org/2025/05/08/doge-deleted-fed-agency-that-aimed-to-increase-government-efficiency/ (accessed 18 July 2025).

Renderos, S. (2025) DOGE's tech takeover threatens the safety and stability of our critical data, *MIT Technology Review*, April 14. Available at: https://www.technologyreview.com/2025/04/14/1114988/doges-tech-takeover-threatens-the-safety-and-stability-of-our-critical-data/ (accessed 18 July 2025).

Reuter, M. (2025) Leak allegedly reveals DOGE list of "wasteful projects", *Netzpolitik*, February 24. Available at: https://netzpolitik.org/2025/u-s-government-leak-allegedly-reveals-doge-list-of-wasteful-projects/ (accessed 13 February 2026).

Revolving Door Project (2025) DOGE agent: Luke Farritor. Available at: https://therevolvingdoorproject.org/doge-agent-luke-farritor/ (accessed 3 April 2026).

Roberge, J., Chartier-Edwards, N. and Galaretta, V. (2026) DOGE blitzkrieg: On Musk's artificial intelligence statecraft, *Science as Culture*, 34, pp. 1–14.

Robins-Early, N. (2025) Doge gained access to sensitive data of migrant children, including reports of abuse, *The Guardian*, April 3. Available at: https://www.theguardian.com/us-news/2025/apr/03/doge-data-migrant-children (accessed 18 July 2025).

Schneider, M. (2025) DOGE targets Census Bureau, worrying data users about health of US data infrastructure, *AP*, May 23. Available at: https://apnews.com/article/census-bureau-doge-federal-surveys-fe560e377be69e913660a6d90c1ee419 (accessed 18 July 2025).

Seneca, T., Grotke, A., Hartman, C. N. and Carpenter, K. (2012) It takes a village to save the web. 'The End of Term Web Archive', *Documents to the People*, 40, pp. 16–23.

Sparkes, M. (2025) DOGE ditching tape storage could put data at risk, say experts, *NewScientist*, April 7. Available at: https://www.newscientist.com/article/2475276-doge-ditching-tape-storage-could-put-data-at-risk-say-experts/ (accessed 16 January 2026).

Stokel-Walker, C. (2025) DOGE is ditching this analog file storage system. That could spell bad news for data integrity, *Fast Company*, April 4. Available at: https://www.fastcompany.com/91313270/doge-is-ditching-magnetic-tapes-but-at-what-cost-to-data-integrity (accessed 16 January 2026).

Stoler, A. L. (2008) Imperial debris: Reflections on ruins and ruination, *Cultural Anthropology*, 23(2), pp. 191–219.

Thylstrup, N. (2018) *The Politics of Mass Digitization* (Cambridge, MA: The MIT Press).

Thylstrup, N. B. (2025) On data loss and disappearance in digital societies, in: R. N. Proctor and L. Schiebinger (Eds) *Ignorance Unmasked: Essays in the New Science of Agnotology*, pp. 71–84 (Ch. 5) (Redwood City, CA: Stanford University Press).

Thylstrup, N. B. and MacKinnon, K. (2025) The politics of digital erasure: Governance and control in government information infrastructure, *Verfassungsblog: On Matters Constitutional*, March 24. Available at: https://verfassungsblog.de/the-politics-of-digital-erasure-us-data/ (accessed 12 May 2025).

Trahan, L. (2025) Trahan announces effort to reform privacy act of 1974, protect Americans' data from government abuse, March 18. Available at: https://trahan.house.gov/news/documentsingle.aspx?DocumentID=3491 (accessed 23 July 2025).

Valkenburg, G. (2026) An enquiry into modes of non-existence, *Science, Technology, & Human Values*, 51(3), pp. 664–688.

Velkova, J. (2023) Retrofitting and ruining: Bunkered data centers in and out of time, *New Media & Society*, 25(2), pp. 431–448.

Velkova, J. (2025) Data infrastructures and their temporalities, in: T. Venturini, A. Acker and J. Plantin (Eds) *Sage Handbook of Data and Society*, pp. 74–99 (Thousand Oaks, CA: Sage Publications).

Vera, L. A., Dillon, L., Wylie, S., Ohayon, J. L., Lemelin, A., Brown, P., Sellers, C., Walker, D., and Environmental Data and Governance Initiative (2018) Data resistance: A social movement organizational autoethnography of the environmental data and governance initiative, *Mobilization: An International Journal*, 23(4), pp. 511–529.