Article

new media & society
1–28

DOI: 10.1177/14614448231152546
journals.sagepub.com/home/nms
SAGE

Radical infrastructure: Building beyond the failures of past imaginaries for networked communication

Britt S Paris
Rutgers, The State University of New Jersey, USA

Corinne Cath
Open Technology Fund, USA

Sarah Myers West
New York University, USA

Abstract

Ongoing political, environmental, and economic crises require infrastructures that can respond to crises in ways that do not replicate and reinforce inequality. To this end, we use a case study method of analysis that compares the authors' previous work on Internet infrastructure at the levels of development, governance, and use to explore how these imaginaries promote or impede people-centered change in the development and maintenance of Internet infrastructure. This theoretical work puts the three existing cases in conversation to better understand how Internet infrastructure alternatives presented as radical, new, or non-hierarchical present shortcomings and opportunities, so that it might be more possible to imagine better, more truly radical, people-centered alternatives. From this comparison, we close our discussion with three heuristics for radical infrastructure: the need for pushing for alternative ensembles of support, busting the myth of technosolutionism, re-politicizing Internet infrastructure, and encouraging technical communities to build around cooperativity, not connectivity.

Corresponding author:
Britt S Paris, Rutgers, The State University of New Jersey, New Brunswick, NJ 08901, USA.
Email: britt.paris@rutgers.edu

Keywords
Cryptography, ethics of care, Future Internet Architecture, IETF, Internet infrastructure, Internet Protocol, science and technology studies, sociotechnical imaginaries, technosolutionism

Introduction

Internet infrastructure is built slowly, over time, protocol by protocol, in response to many different technical, social, political, environmental, and economic imperatives (Braman, 2011, 2017; Clark, 2018; Daniels, 2009; Nelson, 2002; Paris, 2020, 2021). The political, economic, and material instantiation and requirements of Internet infrastructure make it vulnerable to the effects of political polarization, economic strife, and decaying government apparatuses (Tarnoff, 2022). As interested parties prepare for, and respond to ongoing stressors and emergent crises, they must consider how these are imbricated with Internet infrastructure including, but not limited to, the impact of energy-hungry data centers on the environment (Hogan, 2015; Hou, 2022; Strubell et al., 2019; Vonderau, 2019). The surge in surveillance and data capture following the hasty and often uncritical adoption of online tools and applications during crises, for example, in the Covid-19 pandemic (Paris et al., 2021; Reynolds et al., 2022; Vitak and Zimmer, 2020), and the surge of extreme right-wing groups and their use of alternative platforms for organizing when they are kicked off of mainstream ones (Cath-Speth and Van Geuns, 2020; Jasser et al., 2021; Kor-Sins, 2021). These continually unfurling and increasingly emergent phenomena make it a particularly salient time to revisit and refresh methods to critically examine information infrastructures and, we argue, resist, reimagine, and rebuild them–sometimes from the ground up.

Given Latour's (1990) concept that "technology is a society made durable" (p. 103), it is not so surprising that market incentives that undergird US policy writ large, and tech policy in particular, also drive Internet infrastructure development, deployment, and use to the ends of maintaining structural inequality and economic exploitation (Harvey, 2003; Nelson, 2002; Noble, 2013 [1984], 2016, 2018; Schiller, 1995). But as science and technology studies (STS) and infrastructure studies have long claimed, infrastructures—sociotechnical processes in which people engage in social practices with technical artifacts that enable resources to be shared in networked systems (Bowker et al., 2010; Star and Ruhleder, 1994) are famously, often invisible until they break down (Star and Ruhleder, 1994). When they are working as intended, they are easy to ignore.[1] Or at least, that seems so on the surface. Information infrastructures, like the Internet, are more than just the technical material wires, cables, fiber, and routers that facilitate connection, but include organizations, policies, and human cooperation, and as such, are bound with multiple economic, environmental, social, political, and technical activities and imperatives (Bowker et al., 2010; Jackson et al., 2007), which compels researchers to surface the power relations made invisible in these sociotechnical systems (Jackson et al., 2007; Jackson, 2013; Larkin, 2013).

We are examining power structures and asymmetries in Internet infrastructure with an eye toward reconfiguring these sociotechnical practices, making feminist standpoint

epistemology and feminist STS (Barad, 2003; Collins, 1990; Haraway, 1991; Harding, 2004), from which these theoretical lenses and methods emerge, especially well-suited for this study. We draw from and contribute to work around people-centered social movements and science and technologies' concepts of infrastructures, imaginaries, ethics of care, and reconfiguration through the theoretical and methodological lens of feminist standpoint epistemology. In keeping with the methodological impetus of feminist standpoint epistemology (Collins, 2000 [1990]; Haraway, 1991; Harding, 2004), we draw together our collective experiences from being deeply embedded in each of these sites—work that we delve into in more depth elsewhere (Cath-Speth and Van Geuns, 2020, Cath, 2021a, 2021b; Paris, 2018, 2020, 2021; West, 2019, 2022). When placed in conversation with one another through a comparative case method, the differences and similarities among these cases, as well as the failures and opportunities they present, suggest novel starting points for the creation and further development of radical infrastructure.

Through this lens, we present and comparatively analyze relevant practices and theories drawn from three studies previously performed by the authors that serve as situated snapshots of three distinct sites or practices within Internet infrastructure development, each with its own promises of opportunity and realities of failure to achieve a radical, people-centered outcome:

1. At the site of developing technical protocols, with the Future Internet Architecture projects that reconceptualize how data are tracked and transmitted through Internet networks (Paris, 2018, 2020, 2021). The projects in this case promise a new and more flexible Internet infrastructure and were uniquely guided by a council of policy experts, philosophers, social scientists, and STS scholars. However, much of the work produced followed tech-centered, libertarian imaginaries around what the Internet could and should be.
2. At the site of governance, with Internet standards developed through the Internet Engineering Task Force (IETF) (Cath, 2021a, 2021b). The open governance culture of the IETF contains a radical promise for building and managing Internet infrastructure, rooted in bottom-up decision making and collaborative, open tech development. Yet, the anti-political orientation that undergirds its current technical practices hampers such radical possibilities, stressing the need to repoliticize Internet standards' setting.
3. At the site of applications, with cryptography communities (West, 2022). The projects in this case highlight how material possibilities may be animated or constrained at the application layer by the imaginaries of the communities of developers involved in building them: as such, who makes up the technical community matters profoundly for the worlds technological infrastructures make possible.

In our comparative presentation of these cases, the authors build on our previous work by putting each of these studies, their summarized findings, and the theories derived from them, in conversation with one another to develop further theories and understand practices and possibilities that span different levels of Internet infrastructure development, governance, and use.

While there exist many projects that are instructive for how to resist harms after the tech has already been deployed (Costanza-Chock, 2020; Cruz and Harindranath, 2020; Mertia, 2020; Rosa and Hauge, 2022; Scholz, 2016; Srnicek, 2016), we are looking at cases that function at a deeper, protocological layer. By examining sites of Internet infrastructure design, governance, and use, we provide a snapshot of promises and pitfalls around systems-based change. As we put these three sites of Internet infrastructure in conversation with one another, we develop a clearer picture of how sites of technological development that were presented as unique and more liberatory ways to develop, govern, and use Internet infrastructure are constrained and enabled by the imaginaries that alternatively impede or promote positive, people-centered change.

Below we provide a review of literature that explains how we use concepts such as imaginaries and reconfiguration from STS, and care ethics from feminist theory and apply these concepts to Internet infrastructure. The literature review leads to our research questions centering on how imaginaries present in the cases shape the values and practices that impede or promote change and is followed by our research design and findings. We discuss these findings with regard to the research questions. We end with three conceptual heuristics drawn from the shortcomings and opportunities that come from comparing the cases: the need for pushing for alternative ensembles of support, busting the myth of technosolutionism, re-politicizing Internet infrastructure, and encouraging technical communities to build around cooperativity, not connectivity.

Imagining and re-imagining networked communication infrastructures

Safiya Noble (2016) has called for deeper investigation and critique of information infrastructures that focuses on how power dynamics, the political economy, and cultural discourses shape information system development and use. This call aligns with the design justice principles outlined by Sasha Costanza-Chock (2020) to recognize that technology and information systems are developed by powerful people to maintain their power.

Following these provocations, two threads within STS literature animate our analysis of the co-constitutive nature of sociotechnical imaginaries and practices of Internet infrastructure development, deployment, and use that reify or subvert them. The first is how imaginaries are built into material sociotechnical practices, and second, how we might look toward an ethic of care in the practice of re-constituting Internet infrastructure from protocols to use practices.

Sociotechnical imaginaries around Internet infrastructure

Michel Callon (1980) and Sheila Jasanoff and Sang-Hyun Kim (2013, 2015), among others (Adams et al., 2009; Hecht, 2010; Levidow and Papaioannou, 2013; Mager and Katzenbach, 2021), have demonstrated sociotechnical imaginaries are co-constitutive with decision- and policy-making concerning technological projects. Imaginaries are a useful concept to think through the politics embedded within current Internet infrastructures, as they reflect and anticipate the desired futures of their creators (Adams et al., 2009; Mager and Katzenbach, 2021)—and their underlying value systems, meant to be

locked in place through the advancement of technology (Jasanoff and Kim, 2015: 5). Surfacing these imaginaries and untangling their various components is a key exercise toward reimagining—and building—alternative infrastructures centered in care and cooperativity.

Current imaginaries are heavily influenced by market and state ideologies that are reflected in technology policy (Hecht, 2010; Jasanoff and Kim, 2015; Levidow and Papaioannou, 2013). The imaginaries undergirding the nascent structures that would become ARPAnet, and then the Internet, were fundamentally shaped by the threat of a Cold War crisis.[2] The US military facilitated research and development of consolidated data packets, networking, and packet switching (Clark, 2018; Waldrop, 2002). As the Department of Defense's (DoD) Advanced Research Projects Agency (ARPA) partnered with universities to generate this research and create ARPAnet, these projects also incorporated early corporate computing behemoths, such as IBM and BBN as they created a system for routing traffic with Transmission Control Protocol (TCP) and Internet Protocol (IP) where policymakers and users would have to engage in "tussles" to institute their often competing interests (Braman, 2011, 2017; Clark et al., 2005).

As ARPAnet evolved into the Internet we know today, engineers and policy experts managed various stakeholders' "tussles" (Clark et al., 2005) under the assumption that the growing Internet infrastructure itself was, and would continue to be, a "neutral" mediator of these struggles. These emerging technologies were narrated as neutral and thus able to circumvent the problems of identity and inequality that were centered in social movements in the latter part of the 20th century—civil rights in the 1960s, women's reproductive rights in the 1970s, and disenchantment with American Cold War imperialism (Daniels, 2009; Nelson, 2002). As time wore on, these ad hoc partnerships set the stage for advances in Internet and computing technology guided by market ideology presented to corporate entities and the wider public as necessary and sufficient for a utopian future. We see the outcome of these imaginaries today in Internet infrastructure that is built and used to surveil users, particularly to disenfranchise already minoritized groups of people (Browne, 2015; Eubanks, 2015; Gandy, 1993) and to promote racist stereotypes (Noble, 2018), while further cultivating power and wealth for those who are already powerful (Harvey, 2003; Noble, 2013 [1984]; Schiller, 1995; Zuboff, 2019).

Concomitant with these techno-libertarian imaginaries, other more radical ideas around technically mediated information sharing and communication existed in Indigenous groups, for example, in the Kumeyaay, Luiseno, Cupeno, and Cahuilla near San Diego, CA (Srinivasan, 2017; Srinivasan et al., 2010), and aboriginal Australia (Srinivasan, 2017; Verran, 2002), that privileged interrelation between people and the environment, and in Black communities that focused on connection outside of the dominant, hegemonic, white upper-middle class culture (Brock, 2018; McGlotten, 2016; McIlwain, 2019; Nelson, 2011). By and large, these focused on community-based techno-scientific practices and communication around those practices, developed by those within communities for people like them to use and benefit from. In some cases, these practices developed to honor culturally specific knowledge production, in others, it was to resist cooptation by the dominant culture. In others still, these radical tactics emerged as an answer to oppressive strategies imposed by dominant groups to maintain their power. In many cases, multiple or all of the aforementioned motivations shaped

practices. We might understand these examples as fulfilling what Patricia Hill Collins (2000 [1990]) meant when she said that those who are marginalized by the dominant culture are best positioned to enact better systems because of their intimate knowledge of the problems, difficulties, and implications that result from these systems that exist in and extend what she calls the "matrix of oppression." However, these liberatory technological imaginaries remained on the periphery as dominant imaginaries set the terms for how the Internet would be developed and governed to mirror and reify the status quo of inequality well into the future.

Care ethics to reconfigure the Internet infrastructure

While imaginaries of the past replicate themselves in the rollout and use of Internet infrastructure at present, it doesn't mean these must necessarily continue to shape our future. Feminist STS operationalizes the possibility for change in these large technical systems through the concept of configuration, which focuses on the co-constitutive nature of society and technology and highlights that human agency and social coordination is fundamental to the development, deployment, and use of technical systems. Human social relations and values can change, or re-configure, technical enactment over time (Barad, 2003; Cetina, 1997; Haraway, 1991; Suchman, 2000). The concept of configuration is often suggested in feminist STS literature in conjunction with the ethics of care (Adams et al., 2009; Bellacasa, 2017; Martin et al., 2015; Murphy, 2006; Star, 1990), in which acknowledging and remediating contextual unequal power relations are at the forefront of decision-making.

Care ethics provide a uniquely suitable framework to surface and recast such relations, in contrast to virtue ethics, for example, which locates ethics in engaging the correct actions for the correct reasons (Annas, 2000, 2007). Care ethics, in contrast, focuses on caring relations between people and their environment (Bellacasa, 2017), including that part of it wrought from strings of zeros transmitted across wires and through the air into routers and connected devices. Care ethics provides us with a suitable framework for theorizing infrastructure as relationships (Larkin, 2013) that can be reimagined and rebuilt following people-centered values. We lean on care ethics to guide us, as we conceptualize technical systems that endeavor to re-configure these unequal and harmful power relations inherent in technical production, deployment, and use to foster sociotechnical change that values care—as captured in self-determination and justice—rather than market incentives, control, and efficiency.

There exist policy debates that suggest bringing care ethics to Internet infrastructure. At present, the most vocal camps argue for stronger US and EU regulation to break the outsized influence of the corporate platforms and Internet Service Providers that control Internet infrastructure at the end nodes, to enforce "net neutrality" and antitrust (Fight for the Future, 2021; Trendacosta, 2019). Others, including European policymakers and civil society, are considering how to "preserve the public core of the Internet"(Broeders, 2016; Global Commission on the Stability of Cyberspace GCHS, 2017) by establishing shared policy norms for protecting Internet infrastructure or by developing human rights guidelines for infrastructure engineers (Cath and Floridi, 2017; Ten Oever, 2020). Still other voices advocate for nationalizing the Internet as a public utility (Crawford, 2018; Malmgren, 2017) and/or suggest reforming it to allow for smaller scale configurations of

development, deployment, and use (Kienbaum, 2020; MacLellan, 2021; Tarnoff, 2022; Thompson, 2018).

Even as people-centered policy solutions based in the ethic of care exist, efforts within Silicon Valley to remediate harmful systems have been slow going. Often positioned by corporate entities as "responsible" or "ethical" tech, these initiatives often serve to recuperate, rather than resist or redefine, the power structures that ultimately serve a tech company's bottom line (Ames, 2019; Costanza-Chock, 2020; Eubanks, 2018; Noble, 2018; Waldman, 2021) and are increasingly met with public distrust. Other technical governance bodies such as the IETF experience change as even more slow and contentions, as illustrated by the IETF's reticence to implement inclusive naming conventions even as major tech firms made this move easily (Cath, 2021b; Conger, 2021; Inclusive Naming Initiative, 2021).

The evidence suggests that an activism rooted in care ethics is most likely to bring effective change to how infrastructure functions and for whom. People-centered social movement scholars Jane McAlevey (2016) and Piven and Cloward (1978) emphasize that nearly all effective and powerful movements in history take this approach, and leadership by ordinary people in radical movements is clearly evident recent tech industry organizing. Workers across lines of race, gender, and class within and adjacent to Silicon Valley are organizing in solidarity in many different ways, from gig workers and community organizers mobilizing to oppose worker exploitation on platforms like Uber and Instacart (Gig Workers Collective, 2022; Los Deliveristas Unidos, 2022; Uber & Lyft Drivers Union, 2022) to Latinx community organizers Mijente exposing Palantir's, Amazon's, and LexisNexis' close ties with, production, and support of harmful technologies used by US immigrations and customs control (ICE) (Mijente, 2018), leading to white collar tech workers to refuse their labor around on these technologies (Haskins, 2022). Other groups like EqualityLabs headed by Thenmozhi Soundarajan organize to end caste-based discrimination in the tech-sector (Soundarajan et al., 2019). Community organizers like the Stop LAPD Spying Coalition work to dismantle technologies used to uphold the carceral state (Benjamin, 2019a; Paris et al., 2022).

Several strategies and tactics stand out across these disparate examples: organizers in these campaigns use practices like power-structure analyses and power mapping to understand and visualize the spheres of influence of people or groups, what goals and which individuals hold networks and coalitions together, and how motivated and prepared coalitions are for collective action (McAlevey, 2016). Mutual aid work, guided by ethics of care, often supports this organizing and social mobilization around matters of concern, making sure people have their needs met for survival, which includes technology provision to food drop-offs and extends far beyond, while growing and cultivating community, solidarity, and larger networks of support (Spade, 2020).

At the user-facing application layer of Internet infrastructure, cooperative applications and platforms can and do draw from these (older) forms of labor organizing and localized public utilities cooperatives. Academics and activists explore how community and employee-owned ventures of all sorts can be built and function outside of corporate governance structures that are sensitive and accountable to the users of these applications (Scholz, 2016; Srnicek, 2016) as with social.coop, a cooperatively run instance of open source social platform Mastadon (Social.coop, 2022).

Others, like Safiya Noble (2018), have offered design and governance ideas toward public, non-commercial technologies at the application layer. Noble targets search, suggesting a different way of indexing and displaying information on the web that shows the informational domains, topics, and sources to better guide searchers. The question implicit in these platform-level interventions is who controls and profits from data flows, and how (ten Oever, 2021). Across the globe, many groups have taken up the mantle of radical Internet projects. For example, based in the United Kingdom, the May First Movement Technology member-run cooperative pushes for the collective localized control of technology. In Central (Cruz and Harindranath, 2020) and South America (Rosa and Hauge, 2022), and India (Mertia, 2020), users resist, strategically re-use, and recontextualize big tech company products.

At a deeper layer of Internet infrastructure, there are many radical examples of infrastructural interventions that may guide the practices of organizing for and instituting care-driven, people-centered reconfiguration of Internet infrastructure. Rory Solomon (2020) describes the governance and everyday maintenance and use practices at US sites using mesh networks, for example, the Detroit Community Technology Project (DCTP) builds mesh networks in underserved urban areas of Detroit, along with other types of organizing against technological overreach in policing, and advocating for housing and health justice (Detroit Community Technology Project, 2021). These mesh networks allow community members to access the Internet by circumventing Internet service providers who, because it is not profitable, are loath to provide adequate services to communities that are far-flung and/or disenfranchised (Ali, 2021; Burrell, 2018; Solomon, 2020).

For similar reasons, Internet cooperatives exist across the United States, Europe, and Latin America. Rural and indigenous Internet cooperatives present viable, alternative ensembles of support for people-centered Internet infrastructure in areas and in communities where the major providers are loath to build (Ali, 2021; Duarte, 2017; Institute for Local Self-Reliance, 2022; Trostle, 2021). In the case of these US-based rural and indigenous cooperatives, the government or the communities themselves invest in the material infrastructure to develop cooperatives that leverage local training and support to build, maintain, and govern broadband resources. Community users determine the payment model, if there is one, and when there is profit, users in the cooperative split it.

These alternative examples, imaginaries, and possibilities for developing radical Internet infrastructures drawing from care ethics, taken together, suggest a need for a more intentional reading of power. One that derives from care in the communities responsible for building, maintaining, and using Internet infrastructure to enable a more liberatory and practicable imaginary of Internet infrastructure that goes beyond and beneath the material layer. To this end, we lay out the research design below; the rest of the article will describe, compare, and critique these three sites of Internet infrastructure to suggest a set of practices that hold care at the core.

Research questions and methodology case study method and analysis

This article centers on two research questions to demonstrate how we might imagine and build radical infrastructure. The first, along with its subquestion, examines how

imaginaries are built into material sociotechnical practices around the Internet and how these imaginaries enable or resist change. The second, and its subquestion, explores how we might honor the ethic of care in practice of re-constituting Internet infrastructure both in its development and use. The significance of these questions lies in their contributions to a growing area of concern and expertise in the areas of Internet governance and infrastructure studies. Namely, to produce research in service of re-configuring sociotechnical systems to be more hospitable to the needs and interests of users and encourage the research community to engage in various aspects of the process of creating infrastructures that promote and cultivate equity and justice.

- What are the imaginaries around Internet infrastructure development and governance in the cases offered?
    - How do the imaginaries in these cases promote or impede change to the practice by which infrastructures are built and maintained?
- What can we learn from these cases about promoting meaningful change in Internet infrastructure?
    - What are specific (concepts/tactics) that would be useful?

Case study method, interpretative analysis process, and positionality

Below we describe three cases, from studies previously performed by the authors themselves, to explore these research questions. We use an interpretative case study method to put our previously collected and analyzed data and our previous collective experiences conducting the studies that comprise the three cases, in conversation with one another to compare cases, and reveal distinctions and similarities between the theoretical contributions of the case units (Gomm et al., 2009; Walsham, 1995). In doing this, we build upon our previous work by further synthesizing our cases that analyze different levels of Internet infrastructure to speak to one another and to the larger sociotechnical context in which they exist.

We present and analyze the cases using theoretical perspectives described above that are related to feminist standpoint epistemology, which seeks to examine interrelated phenomena as they unfold in the experience of lived life in the context of structural power relations (Collins, 2000 [1990]; Haraway, 1991; Harding, 2004). Case studies interpreted though feminist standpoint epistemology are useful for illuminating processes as they change over time, providing richness that can be a powerful means to knowledge, especially knowledge related to technical and social structural change (Harding, 2004; Paris et al., 2022; Pierre et al., 2021).

While positivist perspectives criticize researcher subjectivity in interpretation, as it ostensibly opens the door to bias and the intrusion of unreliability, feminist standpoint epistemology holds that knowledge is relational and researcher subjectivity can never be divorced from the interpretation of data (Collins, 2000 [1990]; Haraway, 1991; Harding, 2004). On the contrary, researcher subjectivity is critical to interpreting documents, discourse, and personal observations reported through narratives through the lens of structural power in lived life. As such, feminist standpoint epistemology often encourages novel normative prescriptions based in interpretative analysis that is shaped by researcher

subjectivity (Collins, 2000 [1990]; Harding, 2004). As feminist standpoint epistemology considers researcher positionality and subjectivity as a methodological concern, we note that the authors are all white women and were PhD students in the US and England engaging in critical, feminist perspectives on technology and deeply embedded in each of these sites at the time this research was performed. The authors have since continued to cultivate their perspectives in these areas and moved on to work in academia and civil society organizations.

The authors used the interpretative case study methodology in a two-step analytical process to answer the two main research questions and their subquestions.

Step 1. First is to describe and compare relevant practices, concepts, and imaginaries around Internet infrastructure that occur at different but related sites of Internet infrastructure, each of which had been drawn to some degree out in our previous work (Cath, 2021a, 2021b; Paris, 2018, 2020, 2021; West, 2019, 2022). To do this, we revisited our case data and subsequent publications, and fleshed out the imaginaries that were specific to the level of Internet infrastructure they represent, and collectively questioned and discussed how the imaginaries present at these levels impeded or promoted infrastructural change, using critical discourse analysis and feminist stand point epistemology to ask questions about (1) who gets to make decisions about infrastructure (in this study) and how; and who benefits from this decision-making structure and how, as well as (2) how promises of change are enacted or not in reality and day-to-day function, and why.

Step 2. In the process of the first analytical step, thematic threads emerged that were useful in contextualizing the shortcomings and opportunities we found in the imaginaries and the grounded practices in these cases that helped us articulate what concepts and tactics might be useful in reimagining or reconfiguring Internet infrastructure in response to the second research question and subquestion.

In that interpretative process, we developed theory iteratively in a reflexive conversation that allows us to see previously collected and analyzed data and experiences with our study sites in ways that lead to richer and more nuanced understanding of the cases at hand and the phenomena indicted in the research questions surrounding the bigger picture of Internet infrastructure.

Putting our previous work, in the form of already collected and analyzed data, published in cases, in conversation entails comparing case studies on a theoretical level without extracting portions of data that were collected previously, which can be found by accessing the articles cited with the studies that encapsulate the three case studies of Internet infrastructure cited in the next subsection overviewing the previously conducted and published studies comprising the cases.

Case overview

The cases below draw from data collected and analyzed separately by the authors in studies performed from 2016 to 2020 (Cath, 2021a, 2021b; Paris, 2018, 2020, 2021; West, 2022). The three studies informing the cases below used ethnomethods, primarily: iterative, semi-structured, and informal interviews, and participant observation at meetings

surrounding the three sites, to engage and understand how project principals understood and described their work at various levels of developing Internet infrastructure (Suchman, 2000), as well as technical document analysis (Braman, 2017), and critical discourse analysis (Van Dijk, 2005; Wodak and Meyer, 2009) as detailed below:

1. The first author collected and analyzed data at the site of technical development of a component of Internet infrastructure with new Internet protocol development projects to replace transmission control protocol and Internet protocol (TCP/IP) which determine how data are packaged, routed, and transferred through Internet networks with Future Internet Architecture (FIA) project meetings as NSF funding for FIA projects ended (Paris, 2018, 2020, 2021). The previously collected data included in the case study draw from 50 hours of interviews and participant observation at five events surrounding the FIAs, as well as from 6 years of listserv messages that are used to communicate and collaborate around the development of the FIA projects, and critical analysis of over 200 documents, including technical documents, website descriptions, video demos, and news stories around these projects.
2. The second author collected and analyzed data at the site of standards bodies with the Internet Engineering Task Force (IETF), which govern and control both development and deployment of Internet infrastructure components (Cath, 2021a, 2021b). The data for this case study draw on 3 years of ethnographic fieldwork (2017–2020), archival work, and over 65 semi-structured interviews. The archival work includes analysis of 6 years of working group documents, including listserv messages, of multiple IETF working groups, as well as over 500 documents, including government budgets, technical standards, and even poems[3] dedicated to Internet standards.
3. The third author collected and analyzed data at the site of use, understanding how cryptography community advocates co-opt components at the application layer of Internet infrastructure to counter surveillance (West, 2022). The data for this case study draw on 3 years of networked ethnographic fieldwork (Burrell, 2009) at conducted international conferences and workshops focused on the development of cryptographic systems, semi-structured interviews conducted at these field sites and complemented by archival research that examined the work of crypto developers stretching back to the mid-1960s.

Rationale for case selection

These cases were chosen for conversation with one another, because put together, these cases show a trajectory from the development of Internet infrastructure at the levels of Internet routing and transmission protocols to end nodes, or user-facing applications, as governance bodies shape both of these levels of infrastructure. At the level of technical protocol development, engineers' imaginaries around the futures they are building for, the types of affordances that will be necessary, and how they will encourage user buy-in all shape what is built, who is consulted in and guides that process of development (Dourish and Bell, 2014). At the next level, governance bodies make decisions about

control and deployment of various protocols and standards that make up Internet infrastructure (Braman, 2017; Clark, 2018) that determine both how the system is built by engineers and used by users. Those engaging with Internet infrastructure at the application layer or those at the end nodes of these information and communication systems must grapple with the decisions that are made at the more abstracted infrastructural levels. These users feel the palpable political imperatives of the systems that are designed and governed by these engineers and engineering policy bodies. Concerns and practices at the end nodes of the system are highlighted in the case around the cryptographic community advocates.

These three cases as they are laid out below promote discussion around imaginaries as they manifest in these particular sites of Internet infrastructure: (1) technical development at the protocol layer; (2) governance and policy as enacted in Internet governance bodies; and (3) use at the application layer. These imaginaries and the practices surrounding them point to the shortcomings and opportunities present in these cases and suggest how interested parties might re-configure Internet infrastructure. We follow up on this in the discussion, proposing a set of conceptual heuristics that can be a starting point for the creation and further development of radical infrastructure.

Case studies

Stale imaginaries: technical Internet protocol development in the Future Internet Architecture projects

The FIA projects' goal was to build new protocols to replace Transmission Control Protocol (TCP) and Internet Protocol (IP) that currently transfer and route information across a rapidly changing and ever-more complex Internet, while engaging in ethics and values in design directives (Paris, 2018, 2020). The imaginaries guiding these projects were nearly carbon copies of the libertarian utopias of the 1960s and 1970s, and revealed themselves as engineers and project directors engaged in technical practice, envisioned use cases, and made partnership decisions (Paris, 2018, 2020). Instead of the crisis of communism or of counter-cultural movements, the crisis that spurred NSF funding was framed as technical in nature. The shortcomings of the current Internet cited by FIA researchers and engineers—that people want to use it for content streaming, and that crises of all kinds require efficient surveillance and response infrastructure—promise economic opportunity and are used to justify the FIA projects' work. Efficiency, Internet of Things (IoT) compatibility, mobility, and data provenance were claimed as the primary technical considerations in each project, boasting smooth and frictionless data streams as users move through the world (Shilton, 2015; 2017; Paris, 2018). While each of these technical considerations carry great opportunity for reinvention of the sociotechnical sphere and practices around the Internet to be more people-centered, each of these technical considerations carries possibilities both for augmenting lucrative data flows and tracking and commodifying these data streams (Paris, 2018, 2020, 2021). This is no accident. These technical practices and imagined use contexts are shaped by the interests of those they need to buy-in from to support the technology—governmental and industry actors who operate on market-based directives and benefit from the maintenance of

structural inequities. The imaginaries articulated by the FIAs succeeded in justifying buy-in from corporate and military entities as in 2016 they partnered with the US Department of Defense, and infrastructure giants Huawei and Cisco, to name a few (Paris, 2020).

In addition to the protocol development projects' stale imaginaries also were heavily inflected with technical chauvinism despite attempts to the contrary. What was different about this project to revamp the Internet was that it engaged with the NSF-funded Values in Design (VID) Council, the group of social and political science experts and ethicists taxed with instructional engagements with FIA engineers and project leaders to encourage the development of the final infrastructural components to deeply consider social and political concerns. While again, at the time of instantiation, the engagement with the VID council suggested opportunity to create a people-centered Internet, the VID council found that the FIA projects engaged perfunctorily and superficially due to cross disciplinary siloing and engineers' attitudes that they knew best about how to build social and political possibility into their protocols (Nissenbaum et al., 2013; Paris, 2018, 2020). In conversations, through marketing materials, and through published papers and reports FIA respondents demonstrated disinterest in and even neglect of how these technologies are and will be used in ethically, socially, and politically fraught scenarios, as well as how their protocols, or their governance of these protocols, might shape these scenarios (Paris, 2018, 2020). Those who had things to say simply claimed political and technical neutrality guided their work. This chauvinism around technical expertise shaped not only the ways the protocols were built, but who was consulted and how, as well as whose concerns are not considered or taken seriously in the development stage of these protocol projects. This examination of Internet infrastructure projects that were supposed to be guided by ethical, social, and political directives show that while these interventions may hold promise, this type of work will fail to deliver on such promises if they do not question the imaginaries that maintain the status quo of surveillance and commodification, nor do they dissuade technicians from courting buy-in from state and corporate partnerships, so that even when engineers and engineering policymakers claim to want to build infrastructure to better meet the needs of society their practices are insufficient to measure up to their claims.

Apolitical imaginaries: governance of Internet standards in the Internet Engineering Task Force (IETF)

Beyond, and often before, processually entangled with the work of Internet infrastructure development, opaque organizations exercise significant power over the Internet's infrastructure. One such organization is the Internet Engineering Task Force (IETF). Founded in 1986, the IETF is one of the oldest private and industry-led Internet standard-setting bodies and it evolved directly out of the Internet's predecessor. The IETF was created to continue to develop the Internet standards that enable the exchange of information on this vast communication network by connecting different infrastructural products and services to one another, collaboratively and in a bottom-up fashion The need for such standards arose organically to ensure that heterogeneous networks could interact. IETF's governance is characterized by the absence of top-down management, a rough and

rugged culture (Cath, 2021a, 2021b) and technology development based on voluntary coordination between technical actors. Well-known global, and often secretive, Internet hardware and software companies, including Apple, Cisco, Cloudflare, Facebook, Google, and Huawei, participate in the IETF's open governance model. This model, and the participation of these industry behemoths in the IETF, speaks to the radical potential of this standards body as a blueprint for people-centric bottom-up Internet governance. This study demonstrates the possibilities and limits of the IETF's governance model; to drive the creation of radical Internet infrastructure(s), IETF participants must repoliticize their work. IETF participants often express their work in terms of the IETF's unofficial mantra, "We do not do politics." Many IETF-ers describe themselves, and thus imagine themselves, as "just engineers" who work on networking, routing, and other technical aspects of Internet standardization. However, this seeming rejection of the role of politics in standardization and responsibility for the impact of standards on society is shallow. In discussions about politics broadly construed, many IETF participants display a distinctly "anti-political orientation" (Malazita and Resetar, 2019: 300) toward technology, in which they purposefully present their work as devoid of politics. In doing so, they rhetorically absolve themselves from responsibility for their technology's societal consequences, rather than genuinely believing they are blameless. This denial of politics can best be described as "engineered innocence" (Cath, 2021a)—a deliberately and socially constructed position of blamelessness for the real-world consequences of decisions made within the context of technology development, in this case, of standards-setting.

Disentangling the engineers' superficial apolitical stance from their deeper underlying beliefs about the nature of technology makes it possible to repoliticize their work and revise it toward the development of radical infrastructures. Making the "tacit knowledge" (MacKenzie and Spinardi, 1995: 44) that underpins engineered innocence explicit, namely that certain technologies have negative rights and justice ramifications that are best left unspoken, complicates the ability of engineers to develop harmful technologies—as they lose their shield of engineered innocence. Undoing the protective utility of this shared approach to technology development is a first step toward repositioning the organization's infrastructural work in feminist STS orientations focused on a "politics of care" (Bellacasa, 2017; Martin et al., 2015; Murphy, 2006; Star, 1990) and reorienting their work to more radical possibilities. Doing so is important as "engineered innocence" is often invoked by technologists to downplay the power they have to safeguard it and rebuke calls for increased politicizing their work.

Enclave publics: cryptography advocates counter surveillance at the application layer

The imaginaries constituted within technical communities around the political possibilities of technological infrastructures can offer potent alternatives to existing Internet infrastructure. Cryptography is one such example where many different ideas around the political potential of technical infrastructures developed (West, 2019, 2022). Much of our existing commercially driven Internet infrastructure—and the platforms that run on top of it—relies on a business model in which data are commoditized and traded for the purpose of targeting advertising. This model has alternately been described as data

capitalism (West, 2019) and surveillance capitalism (Zuboff, 2019), terms that elucidate, on the one hand, the political economy underpinning much of our Internet infrastructure, and on the other, the harms caused by it. Scholars like Simone Browne (2015) and Ruha Benjamin (2019a, 2019b) further illustrate how surveillance is deeply rooted in anti-Black racism and tied into larger infrastructures of racial capitalism and the carceral state.

Crypto advocates have been particularly active in seeking to contest the conditions of surveillance capitalism through the production of encrypted software, as well as through community dialogues designed to make this software more widely usable by the communities who are disproportionately harmed by the surveillance state, such as communities of color, queer communities, religious minorities, and human rights defenders (Kamara, 2020). Here the production of radical infrastructure is enmeshed in an ethic of care (Kazansky, 2021). Surveillance is conceptualized as a networked, rather than individuated, phenomenon (Marwick and boyd, 2014). This means that taking steps to protect ones' communications is not only for self-protection, but for the protection of all those one communicates with. For example, collectives of crypto advocates and digital security trainers create anticipatory infrastructures (Kazansky, 2021), designed to anticipate and mitigate potential harms to the community in an environment of deep uncertainty. For other developers, a goal is to implement encryption at a deep, infrastructural layer in software protocols where, as one developer described it, it wouldn't set the ceiling but would raise the floor. While encrypted messaging has been the primary locus of many extant discussions around countering surveillance, advocates in the network of field sites observed envisioned a broader set of sociotechnical infrastructures that would encrypt and protect a wide array of social, economic, and political life: creating more secure platforms for the transmission of invoices for work, for example, or security-minded dating apps designed to protect users from stalking and abuse.

Across these examples, reconceptualizing the work of developing privacy-protective communications infrastructures means developing an alternative imaginary for what social life on the Internet is and could be and taking steps to enact it at the application layer. With a community-grounded understanding of the harms caused by ubiquitous surveillance, cryptography advocates began to see cryptography as critical to creating space for free expression and for community formation, particularly among minoritized groups (Kaye, 2015).

This study theorizes this vision for an Internet as akin to what Catherine Squires (2002) in her work on the Black public sphere has called enclave publics, hidden from the view of the dominant public and the state. By developing the tools to make enclave publics possible, these crypto advocates render possible an imaginary for the Internet that puts privacy and community, rather than connectivity, at the center of networked infrastructure.

Offering these cases in conversation with one another allows a glimpse of how imaginaries are built at different layers of Internet infrastructure in these particular sites that build up from the technical layer of protocols to the user-facing application layer, and the governance and policy decisions that shape both of these layers, as well as how change is enacted or resisted through practices at each site. Overall, the imaginaries present in the first two cases at the technical and governance layer appeal to the hegemony of the status quo, to which the third case offers a rich rebuttal to those practices as users contest

these through their own tactics. While the first site promised change, it offered little. The second site resists change. The last meaningfully enacts change. In the next section, we further discuss these imaginaries and relationships to change, as well as failures, shortcomings, and opportunities found through comparing these cases at different levels of Internet infrastructure. We then provide suggestions for conceptual heuristics to imagine how Internet infrastructure might be meaningfully reconfigured with regard to the ethics of care.

Discussion

The dual intents of this article are to (1) highlight imaginaries present in these sites of Internet infrastructure development and discuss their openness to change and resultant consequences, (2) provide an ameliorative approach to the problems surfaced in the exploration of the imaginaries and how they roll out in practice. As such, we end the discussion with a set of conceptual heuristics related to reconfiguring Internet infrastructure with regard to the ethics of care. We start this section by discussing our case studies and reviewing how they relate to imaginaries. By doing so, we clarify the shortcomings and opportunities of the imaginaries present in each of the cases to expand on these.

Our three case studies show how imaginaries can unfold in practice at different sites in the practice of building Internet infrastructure. The first case study illustrates an example of imaginaries that value libertarian market rationality. Within the FIA projects the primary problem to be solved is guise as that of technical insufficiency; however, the solutions promote surveillance and commodification of data. Under the guise of neutrality and technical chauvinism, the engineers argue that they know best and would not even take their engagement with ethics and values experts seriously. These observations suggest that while the FIA projects claim they are building something radically new, this accounts only for the novelty of the technical systems they create. The engineers imagine a future that ignores, or at least does not meaningfully reckon with the shortcomings of the past and present Internet that has heretofore valued surveillance and commodification (Paris, 2020). The FIA's engagement with the VID Council represents an opportunity, because it was a way to divert federal funding to reimagining Internet infrastructure. While perhaps the intervention carried shortcomings and did not appropriately focus engineers in the way the VID council had hoped, it represents a subtle reimagining of ensembles of support that could be used to encourage people-centered Internet infrastructure projects. Perhaps future iterations could instead engage a VID-like Council to focus the work of technicians with civil society organizations within their communities to solve various technical problems they have around Internet infrastructure, as is done with the Detroit Community Technology Project.

The second case study demonstrates how an anti-political imaginary drives technical work in the IETF. This approach allows engineers to strategically mute their role in architecting political outcomes, like power consolidation in the Internet, while maintaining the status quo of their quiet power in place. Both the first and second case show that deliberate choice by engineers and policymakers to make no decisions when it comes to questions of equity: whose interests are served and who falls by the wayside within the systems they build and govern. These "tussles" (Braman, 2017; Clark, 2018; Clark et al.,

2005) are meant to be offloaded to users, or are left as decisions to be made by the corporate entities that dominate both protocol and application design.

The IETF's founding governance principles, of bottom-up governance and collaborative open technology practices, provide important opportunities for building more progressive Internet infrastructures. These deeply ingrained practices are currently aimed toward the same market logics that thwarted the FIA projects work. But they need not be. The current anti-political orientation of the IETF engineers can be reverse engineered. There are ongoing efforts within the IETF, including by a group of researchers and activists convening human rights protocol considerations (HRPC) meetings, to repoliticize standardization. These efforts encourage engineers to reframe their work as political, rather than neutral, and create space to supplant the dominant anti-political imaginary with a more radical view of standardization as the design of power and control. Building out these conscious efforts of repolitizing Internet infrastructure and co-designing alternative imaginaries through direct engagement in technical discussions, is key to reshaping the mundane practices through which radical alternatives are made.

The third case of cryptographic communities shows what can happen when these tussles (Clark et al., 2005) are offloaded to users at the end nodes or application layer of Internet infrastructure. This case shows how both the technical design and governance of these systems that have been built to surveil and commodify user activity both shut people out and create and compound harm to those who are already minoritized. It also shows the potential to rebuild new infrastructures that contest dominant practices of surveillance, across many domains of social, economic and political life. Their work draws from alternate imaginaries that value care and cooperativity as they try to build and promote systems that provide space for human thriving.

Then, there is the issue of how these imaginaries encourage or defeat meaningful change. Applying the feminist STS concept of re-configuration (Barad, 2003; Haraway, 1991; Suchman, 2000) to sociotechnical infrastructure helps us see how actors in all three cases—engineers, governance experts, and users—assert their agency within the system to push for what they see as new solutions to their sociotechnical problems with Internet infrastructure.

A common suggestion coming from the academy, journalism, government, and even industry is that the problems wrought by the tech industry can be fixed by actors who "stand in" for the public without directly engaging ordinary people. The first case with the FIA projects who engaged with the VID council to try to build values into new Internet protocols function much like other models of institutional reform that can only enable incremental change, if any at all (McAlevey, 2016; Piven, 1978). The second case shows the "reform" tactics by which change is thwarted through "engineered innocence" and claims that 'we don't do politics' (Cath, 2021a). But, instead of continuing to build and deploy infrastructures from the top down, reinforcing an outdated libertarian ideal of the "survival of the fittest" (Cath, 2021b; Daniels, 2009; Nelson, 2002; Noble, 2018; Paris, 2020), the third case of use and contestation with the cryptographic communities suggests meaningful ways to enact technical design and governance solutions to counter the oppression present in current Internet infrastructure function.

There are many possible reasons why we might see the clearest examples of reconfiguration at the application layer. One of the most obvious is that the infrastructure is

designed to encourage such "tussles" (Clark et al., 2005). That we see user-driven change most prominently supports the thesis from social movement literature that the most powerful forms of change come from below, or from ordinary people (McAlevey, 2016; Piven, 1978) and suggests a need for massive mobilization as suggested and supported by heuristics below. The resistance from engineers and policy experts in the first and second cases suggests that these groups are already organized in achieving the goals of maintaining the status quo of surveillance, commodification that values economic profit and political power. These observations suggest the need to educate and re-organize those who do the technical and policy work that other Internets are possible and preferable by developing tactics to re-imagine epistemologies around the practice of building Internet infrastructure.

At the level of infrastructure, those interested in meaningful reconfiguration can draw from both radical imaginaries and the imaginaries presented in the cases above, as well as their shortcomings and opportunities, to envision how reconfiguration can be imagined and implemented in the practice of building, deploying, and using the overlapping sociotechnical systems that comprise the Internet. We argue that in this task, it is possible to incorporate an ethics of care that focuses on contextual, situated power differentials, related to development, deployment, and use of Internet infrastructural tools. Below we provide some conceptual heuristics which may be helpful in imagining and organizing around this task.

Conceptual heuristics for radical Internet infrastructure

The imperatives for intersectional technology studies (Noble, 2016) and design justice (Costanza-Chock, 2020) require we apply critical lenses through the processes of technology development, and deployment to begin imagining and building a better sociotechnical future. As a way ahead, we offer tactics for organizing ourselves as activists, academics, and technologists to recognize, use, and in some cases diffuse our power to shape structures of control in favor of working in solidarity with those who are traditionally left out of these processes to foster self-determination and liberation, in service of building a more just sociotechnical future.

As such, our intervention is focused primarily on the broader topic of leveraging relationships and building power to change epistemologies and practice around Internet infrastructure. The big three epistemological assumptions that create the ontological practice of Internet infrastructure development and deployment illuminated in the cases are that engineers and Internet policymakers:

1. Justify their control by adhering to status quo ensembles of support.
2. Push technosolutionism.
3. Focus on connectivity as a mode of generating profit instead of generating community ties among users or the public good.

Engineers, capital, and professional advocates have a vested interest in maintaining these topics and are very organized in this respect, whether or not they are thinking of their praxis for maintaining power in this way. However, seeing these patterns suggests

several opportunities for broader enactment of a people-centered Internet that bracket out advocacy-led regulation and that can, and likely must, happen in several different spheres. Such a practice can draw from activist organizing tactics. Activist groups interested in sociotechnical change already engage in power mapping around particular topics as they coordinate. A power map of the entities involved in Internet infrastructure comes clearer into view from the cases above but is beyond the scope of this article. Structure tests to determine agentic capacity have been carried out around demonstrations like the 2019 Google Walkout and in the unionization of tech workers across the United States. These tactics for taking power and using it for self-determination in tech spheres can be useful in the following radical imaginaries for Internet infrastructure suggested through analyzing the cases.

Pushing for new ensembles of support for Internet infrastructure. The juxtaposition of the FIA and IETF cases with the cryptographic communities case raises a fundamental question: How can a just and equitable Internet be built from what exists when the Internet was developed by the military and corporations to surveil and extract data from users? The FIA and IETF cases show the difficulties for both engineers of new Internet infrastructures and governance bodies to think outside of the military-corporate model, even when building new systems. Their inability or unwillingness to build systems that depart from standard models for ensembles of support in these projects suggests possible interventions. In contrast, departing from the standard model of surveillance or data capitalism is precisely the objective of the ensembles of support within the cryptographic communities, which explicitly come together around a shared aim to build out technological infrastructures for different ways of being in community online.

Following Internet cooperatives and cooperative utilities' ensembles of support and governance mechanisms are instructive here (Institute for Local Self-Reliance, 2022; Trostle, 2021). In these instances, money for establishing new infrastructures, new systems, and new services often comes from the government. Users in localized settings guide development, deployment, and financial issues related to these practices through open governance. Campaigns to draw public attention to possibilities and feasibility of these solutions are the first step. Subsequent steps would push for government investment in public, not-for-profit Internet infrastructure with no strings attached as they have done with cooperative utilities.

Busting the myth of technosolutionism. In the FIA case, developers claiming to build new Internet infrastructures were working off the same imaginaries of a bodiless, apolitical Internet, justifying their work as a commonsense solution to sociotechnical upheaval, exactly as those building the Internet in the 20th century had done (Paris, 2018, 2020). The IETF case study demonstrated that engineers are aware of their power but strategically deny it to maintain the status quo of their unchecked influence (Cath, 2021b). In both cases, they maintain and strengthen the myth that social change can be fomented through technology. This myth pervades in public and political discourse, leading both the public and politicians to turn toward technology to address social concerns, inequities, and the provision of public services (Ames, 2019; Eubanks, 2018). Yet, the cryptographic communities, while they do enact technical changes, do so through different

people-centered modes of governance; they recognize that the problems they are working to solve or reform are inherently political and can therefore not be resolved through technology alone. Their work seems to recognize that holistic change requires input from all sides and compels hard choices about how to allocate public funds, the bounds of care, and who is included in those.

Instead Internet infrastructure should be considered relationally, as the technical backbone facilitating networks made of people with needs. Recalling the concepts around "tussles in cyberspace" (Clark, 2018; Clark et al., 2005) and how these provided partial or temporary solutions for negotiation at the application layer, there must be more concentrated and long-standing engagement with this task. Efforts to address social issues, as well as developing and deploying these technical networks, can draw from care ethics and mutual aid's commitments to upholding human dignity, care, and justice (Spade, 2020). This might be realized by reorienting the development of these systems not toward the ends of profit, but toward the needs of actual people, and could take many different forms. At a minimum, it would require engineers and policymakers to meaningfully listen to people as experts on their technical needs, and work in solidarity with them, recognizing the political nature of their work.

Encourage technical communities to build around cooperativity not *connectivity.* The FIA projects' overt focus on mobility, IoT compatibility, and sometimes covert focus on surveillance and commodification supports the assertion that connectivity and, particularly, the drive to connect more networks to the Internet is a key motivator among technical communities in Internet governance (ten Oever, 2021). This focus on connectivity as an ontological good eludes difficult questions regarding who is served by more connectivity and what other principles should drive Internet infrastructure.

The cryptographic communities suggest a way to think about how self-determined, ground-up, cooperative, collaborative information and communication infrastructures do what they can to reconfigure data flows to dismantle corporate power. The IETF's governance model demonstrates that these practices exist and thrive in technical communities but require a re-orientation toward explicit progressive alternatives. Along with practices found in Internet and public utility cooperatives' ensembles of support, Safiya Noble's (2018) search algorithm and Trebor Scholz' (2016) cooperative practices move the Internet to a place before and beyond corporate monopolies by suggesting thoughtful bottom-up governance. While these recommendations from Noble and Scholz are not infrastructure at the level of protocols, they are infrastructural in the sense that they are the social practices surrounding what to do with the data flows within sociotechnical systems.

Conclusion

This work provides a snapshot of examples at different levels of Internet infrastructure development and use, and standards governance that shape the relationship between the first two levels. In so doing, this article builds on the three authors' previous critical studies of different levels of Internet infrastructure and takes them a step further by putting them in conversation with one another to better understand the promises and pitfalls that

beset these sites and develop a theoretical synthesis to point out possibilities. Beyond the generalizability limitations of an interpretative comparative case study, the cases and sites of infrastructure they indicate are not the only examples of these sites, nor perhaps even the most representative examples of these levels of infrastructure that exist. Even as we have found one set of imaginaries around these levels of infrastructure that seem to suggest certain things about the political and economic concerns that undergird and shape these, further study that investigates other examples in similar classes or in other categories of Internet infrastructure outside the classes these examples represent may uncover further nuances, provide context, or contest what we have found here. Furthermore, studying ownership of the deeper levels of Internet infrastructure like data centers, Internet fiber, and undersea cables, and how to reconfigure privatized ownership to be people-centered public ownership is beyond the scope of this article, but would be warranted in conjunction with the work this article puts forward.

It remains that the public-private Internet infrastructure that exists at present is largely homogenized, highly commodified, and surveillance-focused, imbricated in and exacerbated by economic inequality, political division, and climate change (Hogan, 2018; Jasser et al., 2021; Malazita and Resetar, 2019; Strubell et al., 2019; Tarnoff, 2022; Vonderau, 2019). But this does not mean that these problems must necessarily shape the future. That alternative future, however, requires further attention to the infrastructural layers of the Internet below the most visible of social media and other commercial consumer applications.

As those in power benefited from the design of our existing Internet infrastructures, many across the globe have seen and felt the burgeoning weight of institutional crises, infrastructure breaches and collapse for a long time (Jackson, 2013; Nelson, 2002, 2011;Noble, 2016). If those interested in Internet reconfiguration projects follow the lessons learned from the cases above and focus on making infrastructures workable for the most vulnerable, they will work for everyone (Collins, 2000 [1990]). This work will require attending to the relationality of these systems, users, policy, and designers, asking critical questions along the way about who is served by information and communication infrastructures, and how. Making infrastructure work also requires further development of new mechanisms of Internet development, deployment, and governance.

Pushing this work toward reality requires organizing both technologists, policy experts, and the public of users around "radical" people-centered imaginaries that make sense given today's sociotechnical landscape. As was, and is, the case with public utility cooperatives, rural and indigenous Internet cooperatives, and inscribing refusal as a critical response to technology development and deployment in ways that are similar to extant organizing within the tech industry, such as in the Tech Worker Coalition. As people organize and refuse, they can pressure design and governance bodies to acknowledge their political positions to push a widespread radical reimagination and a new set of goals for what Internet infrastructures could be. They can draw on such projects as Riseup, Movement Technology, and Mayfirst, and imaginaries outside of the dominant technopolitical sphere that feature self-determination and *liberatory*—not libertarian—goals of equality, inclusivity, care, and contextual decision-making for technological projects.

There are many possible roads to take, and each will be accompanied by conflict, hard decisions, and powerful interests attempting to discredit and dismantle liberatory projects at every turn. If the past is an indicator, the future path is likely to be beset with difficulties (Nelson, 2002, 2011; Tarnoff, 2022; Waldman, 2021). Yet, the cost of clinging onto legacy infrastructures, and their past imaginaries, for the sake of stability and continuation of the status quo comes at too high a price. Moving beyond the flaws of past imaginaries is necessary in order to imagine, articulate, and subsequently build radical infrastructures.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Britt Paris' research was supported by the School of Education and Information Dean's Graduate Fellowship; Summer Graduate Research Fellowships; and an Assistantship at the Kleinrock Center for Internet Studies, all during her PhD in Information Studies at the University of California, Los Angeles (2014–2018).

Corinne Cath's research was supported by the Ford Foundation (grant number 136179, 2020) and the Alan Turing Institute for AI and Data Science (PhD studentship 2016–2020).

Sarah Myers West's research was supported through a Wallis Annenberg Graduate Fellowship at the Annenberg School for Communication and Journalism.

ORCID iDs

Britt S Paris https://orcid.org/0000-0003-1527-7953

Sarah Myers West https://orcid.org/0000-0002-3947-6896

Notes

1. More precisely, infrastructures are invisible to those who are not adversely impacted by them: for example, a pedestrian may not give much thought to a sidewalk being repaired unless it affects their mobility, in which case it's a significant factor in day-to-day life.
2. The advent of computation follows a similar trajectory and is intertwined with the processes we describe in this article, but that history is beyond the scope of this article.
3. RFC 1121. *Act One - The Poems.* Jon Postel, Leonard Kleinrock, Vint Cerf, and Barry Boehm. https://tools.ietf.org/html/rfc1121. September 1989.

References

Adams V, Murphy M and Clarke AE (2009) Anticipation: technoscience, life, affect, temporality. *Subjectivity* 28(1): 246–265.

Ali C (2021) *Farm Fresh Broadband: The Politics of Rural Connectivity*. Cambridge, MA: MIT Press.

Ames MG (2019) *The Charisma Machine: The Life, Death, and Legacy of One Laptop Per Child*. Cambridge, MA: The MIT Press.

Annas J (2000) *Platonic Ethics, Old and New*. Ithaca, NY: Cornell University Press.

Annas J (2007) Virtue ethics. In: Copp D (ed.) *Oxford Handbook of Ethical Theory*. Oxford: Oxford University Press, pp. 1–24.

Barad K (2003) Posthumanist performativity: toward an understanding of how matter comes to matter. *Signs* 28(3): 801–831.

Bellacasa MP (2017) *Matters of Care: Speculative Ethics in More Than Human Worlds*. Minneapolis, MN: University of Minnesota Press.
Benjamin R (ed.) (2019a) *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham, NC: Duke University Press.
Benjamin R (2019b) *Race after Technology: Abolitionist Tools for the New Jim Code*. 1st ed. Cambridge: Polity Press.
Bowker GC, Baker K, Millerand F, et al. (2010) Toward information infrastructure studies: ways of knowing in a networked environment. In: Hunsinger J, Klastrup L and Allen M (eds) *International Handbook of Internet Research*. Dordrecht: Springer Netherlands, pp. 97–117.
Braman S (2011) The framing years: policy fundamentals in the Internet design process, 1969–1979. *The Information Society* 27(5): 295–310.
Braman S (2017) Internet histories: the view from the design process. *Internet Histories* 1(1–2): 70–78.
Brock A (2018) Critical technocultural discourse analysis. *New Media & Society* 20(3): 1012–1030.
Broeders D (2016) *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.
Browne S (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.
Burrell J (2009) The field site as a network: a strategy for locating ethnographic research. *Field Methods* 21(2): 181–199.
Burrell J (2018) View of thinking relationally about digital inequality in rural regions of the U.S. *First Monday* 23(6). Available at: https://doi.org/10.5210/fm.v23i6.8376
Callon M (1980) The state and technical innovation: a case study of the electrical vehicle in France. *Research Policy* 9(4): 358–376.
Cath C (2021a) *Changing Minds and Machines: A Case Study of Human Rights Advocacy in the Internet Engineering Task Force (IETF)*. Oxford: Oxford University Press.
Cath C (2021b) The technology we choose to create: human rights advocacy in the Internet Engineering Task Force. *Telecommunications Policy* 45(6): 102144.
Cath C and Floridi L (2017) The design of the Internet's architecture by the Internet Engineering Task Force (IETF) and Human Rights. *Science and Engineering Ethics* 23(2): 449–468.
Cath-Speth C and Van Geuns S (2020) How hate speech reveals the invisible politics of internet infrastructure. *Brookings*. Available at: https://www.brookings.edu/techstream/how-hate-speech-reveals-the-invisible-politics-of-internet-infrastructure/
Cetina KK (1997) Sociality with objects social relations in Postsocial Knowledge Societies. *Theory, Culture & Society* 14(4): 1–30.
Clark DD (2018) *Designing an Internet*. Cambridge, MA: MIT Press.
Clark DD, Wroclawski J, Sollins KR, et al. (2005) Tussle in cyberspace: defining tomorrow's Internet. *IEEE/ACM Transactions on Networking* 13(3): 462–475.
Collins PH (2000 [1990]) *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. Boston: Unwin Hyman.
Conger K (2021) "Master," "slave" and the fight over offensive terms in computing. *The New York Times*. Available at: https://www.nytimes.com/2021/04/13/technology/racist-computer-engineering-terms-ietf.html
Costanza-Chock S (2020) *Design Justice: Community-Led Practices to Build the Worlds We Need*. Cambridge, MA: MIT Press.
Crawford S (2018) Why you won't be getting 5G connectivity any time soon. *Wired*. Available at: https://www.wired.com/story/america-needs-more-fiber/

Cruz EG and Harindranath R (2020) WhatsApp as "technology of life": reframing research agendas. *First Monday*. Available at: https://doi.org/10.5210/fm.v25i12.10405

Daniels J (2009) *Cyber Racism: White Supremacy Online and the New Attack on Civil Rights*. Lanham, MD: Rowman & Littlefield Publishers.

Detroit Community Technology Project (2021) Technology rooted in community needs. Available at: https://detroitcommunitytech.org/

Dourish P and Bell G (2014) "Resistance is futile": reading science fiction alongside ubiquitous computing. *Personal and Ubiquitous Computing* 18(4): 769–778.

Duarte ME (2017) *Network Sovereignty: Building the Internet across Indian Country*. Seattle, WA: University of Washington Press.

Eubanks V (2015) The policy machine. *Slate*. Available at: http://www.slate.com/articles/technology/future_tense/2015/04/the_dangers_of_letting_algorithms_enforce_policy.html

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Fight for the Future (2021) Fight for the future, defending our basic rights and freedoms. *Fight for the Future*. Available at: https://www.fightforthefuture.org

Gandy OH (1993) African Americans and Privacy: understanding the Black perspective in the Emerging Policy Debate. *Journal of Black Studies* 24(2): 178–195.

Gig Workers Collective (2022) Gig Workers Collective. Available at: https://www.gigworkerscollective.org/home

Global Commission on the Stability of Cyberspace GCHS (2017) Call to protect the public core of the Internet. *GCSC*. Available at: https://cyberstability.org/research/call-to-protect/

Gomm R, Hammersley M and Foster P (2009) *Case Study Method*. Thousand Oaks, CA: SAGE.

Haraway D (1991) A cyborg manifesto: science, technology and socialist-feminism in the late 20th century. In: Haraway D (ed) *Simians, Cyborgs, and Women: The Reinvention of Nature*. London and New York: Routledge, pp. 149–181.

Harding S (2004) *The Feminist Standpoint Theory Reader: Intellectual and Political Controversies*. London and New York: Routledge; Boca Raton, FL: CRC Press. Available at: https://www.routledge.com/The-Feminist-Standpoint-Theory-Reader-Intellectual-and-Political-Controversies/Harding/p/book/9780415945011

Harvey D (2003) The fetish of technology: causes and consequences. *Macalester International* 13: 1–29.

Haskins C (2022) Google and Amazon ignore employee protests and plow ahead with deals involving the US Military, ICE, and CBP. *Business Insider*. Available at: https://www.businessinsider.com/google-amazon-quietly-contract-dod-ice-cbp-employee-protests-2022-9

Hecht G (2010) The power of nuclear things. *Technology and Culture* 51(1): 1–30.

Hogan M (2015) Data flows and water woes: the Utah Data Center. *Big Data & Society* 2(2): 2053951715592429.

Hogan M (2018) Big data ecologies. *Ephemera* 18(3): 631.

Hou C (2022) Presenting new research climate justice x digital rights. *Branch*. Available at: https://branch.climateaction.tech/issues/issue-4/climate-justice-digital-rights/

Inclusive Naming Initiative (2021) Inclusive Naming Initiative. Available at: https://inclusivenaming.org/word-lists/

Institute for Local Self-Reliance (2022) Cooperatives build community networks. *Community Broadband Networks*. Available at: https://muninetworks.org/content/rural-cooperatives-page

Jackson SJ, Edwards PN, Bowker GC, et al. (2007) Understanding infrastructure: history, heuristics and cyberinfrastructure policy. *First Monday*. Available at: https://doi.org/10.5210/fm.v12i6.1904

Jackson SM (2013) Rethinking repair. In: Gillespie Y, Boczkowski PJ and Foote K (eds) *Media Technologies: Essays on Communication, Materiality and Society*. Cambridge, MA: MIT Press, pp. 221–239.

Jasanoff S and Kim SH (2013) Sociotechnical imaginaries and National Energy Policies. *Science as Culture* 22(2): 189–196.

Jasanoff S and Kim SH (2015) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Chicago, IL: University of Chicago Press.

Jasser G, McSwiney J, Pertwee E, et al. (2021) "Welcome to #GabFam": far-right virtual community on Gab. *New Media & Society*. Epub ahead of print 28 June. DOI:10.1177/14614448211024546.

Kamara S (2020) Crypto for the people, invited talk at Crypto 2020. Available at: https://www.youtube.com/watch?v=Ygq9ci0GFhA

Kaye D (2015) United Nations report to the Human Rights Council on encryption, anonymity, and the human rights framework. *United Nations Human Rights Council*. Available at: https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx

Kazansky B (2021) "It depends on your threat model": the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951720985557

Kienbaum K (2020) Cooperatives essential to bringing high-quality fiber Internet access to rural America. *Institute for Local Self-Reliance*. Available at: https://ilsr.org/cooperatives-essential-to-bringing-high-quality-fiber-internet-access-to-rural-america/

Kor-Sins R (2021) The alt-right digital migration: a heterogeneous engineering approach to social media platform branding. *New Media & Society*. Epub ahead of print 20 August. DOI: 10.1177/14614448211038810.

Larkin B (2013) The politics and poetics of infrastructure. *Annual Review of Anthropology* 42(1): 327–343.

Latour B (1990) Technology is Society Made Durable. *The Sociological Review 38*(1_suppl): 103–131. https://doi.org/10.1111/j.1467-954X.1990.tb03350.

Levidow L and Papaioannou T (2013) State imaginaries of the public good: shaping UK innovation priorities for bioenergy. *Environmental Science & Policy* 30: 36–49.

Los Deliveristas Unidos (2022) Los Deliveristas Unidos. Available at: https://losdeliveristasunidos.org/

McAlevey JF (2016) *No Shortcuts: Organizing for Power in the New Gilded Age*. Oxford: Oxford University Press.

McGlotten S (2016) Black data. In: Johnson EP (ed) *No Tea, No Shade: New Writings in Black Queer Studies*. Durham, NC: Duke University Press, pp. 262–286.

McIlwain CD (2019) *Black Software: The Internet & Racial Justice, from the Afronet to Black Lives Matter*. Oxford: Oxford University Press.

MacKenzie D and Spinardi G (1995) Tacit knowledge, weapons design, and the uninvention of nuclear weapons. *American Journal of Sociology* 101(1): 44–99.

MacLellan L (2021) For better or worse, web infrastructure is not a public good. *Quartz*. Available at: https://qz.com/work/1956070/internet-infrastructure-companies-should-be-public-utilities/

Mager A and Katzenbach C (2021) Future imaginaries in the making and governing of digital technology: multiple, contested, commodified. *New Media & Society* 23(2): 223–236.

Malazita JW and Resetar K (2019) Infrastructures of abstraction: how computer science education produces anti-political subjects. *Digital Creativity* 30(4): 300–312.

Malmgren E (2017) Nationalize the networks. *Dissent Magazine*. Available at: https://www.dissentmagazine.org/online_articles/net-neutrality-repeal-case-for-public-broadband

Martin A, Myers N and Viseu A (2015) The politics of care in technoscience. *Social Studies of Science* 45(5): 625–641.

Marwick AE and boyd d (2014) Networked privacy: how teenagers negotiate context in social media—Alice E Marwick, danah boyd, 2014. *New Media & Society* 16(7): 1051–1067.

Mertia S (2020) *Lives of Data: Essays on Computational Cultures from India*. Amsterdam: Institute of Network Cultures.

Mijente. (2018). *Who's Behind ICE? The Tech and Data Companies Fueling Deportations* (pp. 1–75). Mijente. https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

Murphy M (2006) *Sick Building Syndrome and the Problem of Uncertainty: Environmental Politics, Technoscience, and Women Workers*. 1st ed. Durham, NC: Duke University Press.

Nelson A (2002) Introduction: FUTURE TEXTS. *Social Text* 20(2(71)): 1–15.

Nelson A (2011) *Body and Soul: The Black Panther Party and the Fight against Medical Discrimination*. Minneapolis, MN: University of Minnesota Press.

Nissenbaum H, Stark L and Zeiwitz K (2013) Values in design council: an end of project report NSF Eager: values in design in the Future Internet Architecture. Available at: http://www.nyu.edu/projects/nissenbaum/vid/pdfs/VIDCouncilReportv2.pdf

Noble DF (2013 [1984]) *Forces of Production*. New York: Knopf Doubleday Publishing Group.

Noble SU (2016) A future for intersectional black feminist technology studies. *Scholar & Feminist Online* 13(3): 1–2. Available at: https://sfonline.barnard.edu/traversing-technologies/safiya-umoja-noble-a-future-for-intersectional-black-feminist-technology-studies/

Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

Paris B (2018) *Time constructs, the origins of a future Internet*. PhD Dissertation Los Angeles, University of California Los Angeles. Available at: https://escholarship.org/uc/item/133926p6

Paris B (2020) The Internet of Futures Past: values trajectories of networking protocol projects. *Science, Technology, & Human Values*. Epub ahead of print 24 November. DOI: 10.1177/0162243920974083.

Paris B, Currie M, Pasquetto I, et al. (2022) Data burdens: epistemologies of evidence in police reform and abolition movements. *Data Justice and the Right to the City*. Available at: https://www.research.ed.ac.uk/en/publications/data-burdens-epistemologies-of-evidence-in-police-reform-and-abol

Paris B, Reynolds R and McGowan C (2021) Sins of omission: critical informatics perspectives on privacy in e-learning systems in higher education. *Journal of the Association for Information Science and Technology*. Epub ahead of print 29 September. DOI: 10.1002/asi.24575.

Paris BS (2021) Time constructs: design ideology and a future internet. *Time & Society* 30(1): 126–149.

Pierre J, Crooks R, Currie M, et al. (2021) Getting ourselves together: data-centered participatory design research & epistemic burden. In: *Proceedings of the 2020 CHI conference on human factors in computing systems*, Yokohama, Japan, 8–13 May, pp. 1–11. New York: ACM.

Piven FF and Cloward R (1978) *Poor People's Movements: Why They Succeed, How They Fail* (unknown edition). New York: Vintage Books.

Reynolds R, Aromi J, McGowan C, et al. (2022) Digital divide, critical-, and crisis-informatics perspectives on K-12 emergency remote teaching during the pandemic. *Journal of the Association for Information Science and Technology*. Epub ahead of print 2 May. DOI: 10.1002/asi.24654.

Rosa FR and Hauge JA (2022) GAFA's information infrastructure distribution: interconnection dynamics in the Global North versus global south. *Policy & Internet* 14(2): 424–449.

Schiller H (1995) *Information Inequality*. 1st ed. London and New York: Routledge

Scholz T (2016) *Platform Cooperativism: Challenging the Corporate Sharing Economy*. Berlin: Rosa Luxemburg Siftung.

Shilton, K. (2015). Anticipatory Ethics for a Future Internet: Analyzing Values During the Design of an Internet Infrastructure. *Science and Engineering Ethics*, 21(1), 1–18. https://doi.org/10.1007/s11948-013-9510-z

Shilton, K. (2017). Engaging Values Despite Neutrality: Challenges and Approaches to Values Reflection during the Design of Internet Infrastructure - Katie Shilton, 2018. *Science, Technology, & Human Values*. http://journals.sagepub.com/doi/10.1177/0162243917714869

Social.coop (2022) Social.coop: a cooperative decentralized social network. *Grassroots Economic Organizing*. Available at: https://geo.coop/content/socialcoop-cooperative-decentralized-social-network

Solomon R (2020) *Meshiness: mesh networks and the politics of connectivity*. New York University Proquest Dissertation Publishing. Available at: https://www.proquest.com/openview/35dca67d10717f2130572fb824cb1b7b/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y

Soundarajan T, Kumar A, Nair P, et al. (2019) Facebook India report. *Equality Labs*. Available at: https://www.equalitylabs.org/facebookindiareport

Spade D (2020) *Mutual Aid: Building Solidarity during This Crisis*. New York: Verso Books.

Squires CR (2002) Rethinking the black public sphere: an alternative vocabulary for multiple public spheres. *Communication Theory* 12(4): 446–468.

Srinivasan R (2017) *Whose Global Village? Rethinking How Technology Shapes Our World*. New York: New York Unversity Press.

Srinivasan R, Becvar KM, Boast R, et al. (2010) Diverse knowledges and contact zones within the digital museum. *Science, Technology & Human Values* 35(5): 735–768.

Srnicek N (2016) *Platform Capitalism*. 1st ed. Cambridge: Polity Press.

Star SL (1990) Power, technology and the phenomenology of conventions: on being allergic to onions. *The Sociological Review* 38(Suppl. 1): 26–56.

Star SL and Ruhleder K (1994) Steps towards an ecology of infrastructure: complex problems in design and access for large-scale collaborative systems. In: *Proceedings of the 1994 ACM conference on computer supported cooperative work*, Chapel Hill, NC, 22–26 October, pp. 253–264. New York: ACM.

Strubell E, Ganesh A and McCallum A (2019) Energy and policy considerations for deep learning in NLP. In: *Proceedings of the 57th annual meeting of the association for computational linguistics*, Florence, July 2019, pp. 3645–3650. New York: ACM.

Suchman L (2000) Embodied practices of engineering work. *Mind, Culture, and Activity* 7(1–2): 4–18.

Tarnoff B (2022) *Internet for the People: The Fight for Our Digital Future*. New York: Verso Books.

Ten Oever N (2020) *Wired norms: inscription, resistance, and subversion in the governance of the Internet infrastructure*. PhD Dissertation, University of Amsterdam, Amsterdam.

ten Oever N (2021) "This is not how we imagined it": technological affordances, economic drivers, and the Internet architecture imaginary. *New Media & Society* 23(2): 344–362.

Thompson C (2018) Rural America could reboot the old DIY spirit of the Internet. *Wired*. Available at: https://www.wired.com/story/rural-america-diy-internet-spirit-reboot/

Trendacosta K (2019) Real net neutrality is more than a ban on blocking, throttling, and paid prioritization. *Electronic Frontier Foundation*. Available at: https://www.eff.org/deeplinks/2019/02/real-net-neutrality-more-ban-blocking-throttling-and-paid-prioritization.

Trostle H (2021) Building indigenous future zones: Four tribal broadband case studies. *Community Networks*. Available at: https://ilsr.org/wp-content/uploads/2021/02/Indigenous FutureZones-0221.pdf

Uber & Lyft Drivers Union (2022) Rideshare Drivers United. *Uber & Lyft Drivers Union*. Available at: https://www.drivers-united.org/

Van Dijk TA (2005) Critical discourse analysis. In: Schiffrin D, Tannen D and Hamilton HE (eds) *The Handbook of Discourse Analysis*. Hoboken, NJ: Blackwell Publishers Ltd, pp. 349–371.

Verran H (2002) A Postcolonial Moment in science studies: alternative firing regimes of environmental scientists and aboriginal land owners. *Social Studies of Science* 32(5–6): 729–762.

Vitak J and Zimmer MT (2020) How Covid-19 is changing workplace surveillance: American workers' experiences and privacy expectations when working from home. *Covid-19 and the Social Sciences—Social Science Research Council (SSRC)*. Available at: https://covid19research.ssrc.org/grantee/how-covid-19-is-changing-workplace-surveillance-american-workers-experiences-and-privacy-expectations-when-working-from-home/

Vonderau A (2019) Storing data, infrastructuring the air: thermocultures of the cloud − Asta Vonderau. *Culture Machine*. Available at: https://culturemachine.net/vol-18-the-nature-of-data-centers/storing-data/

Waldman AE (2021) *Industry Unbound: The inside Story of Privacy, Data, and Corporate Power*. Cambridge: Cambridge University Press.

Waldrop MM (2002) *The Dream Machine: J.C.R. Licklider and the Revolution That Made Computing Personal*. 1st ed. London: Penguin Books.

Walsham G (1995) Interpretive case studies in IS research: nature and method. *European Journal of Information Systems* 4(2): 74–81.

West SM (2019) Data capitalism: redefining the logics of surveillance and privacy. *Business & Society* 58(1): 20–41.

West SM (2022) Survival of the cryptic: tracing technological imaginaries across ideologies, infrastructures, and community practices. *New Media & Society* 24(8): 1891–1911.

Wodak R and Meyer M (2009) *Methods for Critical Discourse Analysis*. Thousand Oaks, CA: SAGE.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st ed. New York: PublicAffairs

Author biographies

Britt Paris is a critical informatics scholar studying the political economy of information infrastructure. Her current research focuses on cases alternative Internet infrastructure and what they suggest about the opportunities and obstacles to overcome to build a people-centered Internet. Paris is an assistant professor at Rutgers University's School of Communication & Information in the Library & Information Science Department, and an affiliate at Data & Society Research Institute.

Corinne Cath is an anthropologist studying internet infrastructure politics. Her current research is focused on computing cultures, in particular the cloud computing industry and the emergent harms of its expansion into the public sector. Cath is a research affiliate at Minderoo Centre for Technology & Democracy, University of Cambridge, UK & Critical Infrastructure Lab, University of Amsterdam.

Sarah Myers West is the Managing Director of the AI Now Institute. She recently served a term as a Senior Advisor on AI at the Federal Trade Commission. She holds a decade of policy and research experience in the political economy of the tech industry, and her forthcoming book Tracing Code (University of California Press) examines the origins of commercial surveillance.