Making Information Infrastructure Work (In)visible As University Campuses Reopen

Introduction

The current public health emergency of COVID-19 poses numerous challenges in the workplace, many of which lie still ahead as the leadership of myriad worksites interpret state and local guidelines for reopening while considering the conflicting desires of clients and employees with economic pressures. The response of university systems across the United States has been far from uniform. In a survey of 985 colleges, 65% have announced the decision to return to in-person learning this fall while 14% are choosing a hybrid model. Whether fully in-person, adopting a hybrid model, or, as the entire University of California system has announced, adopting a fully online learning model, higher education and campus cultures will see drastic shifts in the coming months. Protocols will be enacted to more vigilantly monitor the spread of the virus on campus, including more testing, contact tracing, and temperature screening. While much of the news coverage has focused on the student experience upon returning to campuses this fall, less has been said about the state of work on campuses, much of which did not stop when the students left in the spring. One such workforce is the combined efforts of IT (information technology) and facilities teams who have continued to work on campus as necessary throughout these shutdowns to maintain critical information infrastructures.

The early findings presented here demonstrate changes underway in the various units that maintain university information infrastructures. This work is currently considered as “other duties as assigned” but this designation is understating what in reality is work necessary to the functioning of an effective and secure university. Efforts to make this work visible predate COVID-19, but early evidence shows how these efforts can work in concert with those meant to control the spread of the virus. I will demonstrate how new university protocols to control COVID-19 are also making this labor visible, but through mechanisms that necessitate critical analysis in relation to labor rights, privacy, and surveillance concerns. Growing concerns about the invasiveness of new protocols that rely on biometric data collection (i.e. temperature readings) and tracking (i.e. contract tracing armies being deployed), while merited, may miss the more naturalized forms of worker surveillance that accompany such maintenance work. Concerns about these protocols are fortified with the dual purpose of making maintenance work more measurable in light of resource scarcity and heightened vigilance in tracing who is working where. These surveillance apparatuses predate COVID-19. And yet, this paper will argue, it will be important to continue to observe and analyze the means by which COVID-19 responses in the workplace leverage existing surveillance apparatuses as they call into question whose work is deemed “essential” and to what degree this designation results in heightened workplace surveillance.

This paper concludes that these processes that make invisible work visible demonstrate the paradox of labor visibility as theorized by Star and Strauss [1]: that making work visible can both mitigate labor exploitation while also providing opportunities for new forms of exploitation.

Bringing the work of Star and Strauss into conversation with emergent findings on the implementation and maintenance of information infrastructures and requisite changes to university workflows due to the pandemic, the paradox of (in)visible labor can be conceptualized anew with insights into the potential risks of greater worker surveillance. These early findings are part of a three-year study of universities' built environments and the coordination and collaboration taking place therein to address IoT (Internet of Things) device implementation and related cybersecurity maintenance.

Prior Work

Information infrastructures and invisible labor are intertwined [1, 2]. IoT in the built environment, as a growing contingent of the information infrastructure of universities, is thus intertwined with invisible labors that span across IT and facilities organizations as well as across campuses. Some of these invisible labors are generated by the introduction of novel technology into existing infrastructures [3]. IoT is particular in both function and aesthetic terms because it is inherently infrastructural as it is embedded in the built environment and is meant to facilitate better control of the space without drawing attention to itself. It is built to blend into what has been naturalized as, in this case, the university built environment.

This paper will use the term infrastructure in two senses. First, infrastructure is a system that includes all the "mundane mechanisms within, beneath, and supporting the maintenance of quotidian life" [4]. Second, I use infrastructure, following the work of Susan Leigh Star, Anselm Strauss, and Geoffrey Browker [1, 2, 5], as a theoretical framework for interrogating the tools, materials, relationships, and processes that often exist out of sight for many, are integral to the day to day operations for some, and emerge with new meaning in key moments in which the status quo is disturbed. COVID-19 is one such key moment.

Maintenance work, the labor that includes the upkeep, repair, and sustaining of the human-built world, is integral to the everyday functioning of a university campus. However, in light of new regulations and social distancing mandates, this labor has become more visible as it requires greater oversight. Drawing on early ethnographic evidence from an ongoing inquiry of the coordination and collaboration practices of internal organizations within a large university to improve IoT security, the (in)visibility of maintenance labor responding to critical information infrastructure needs has emerged as an important challenge for the members of these organizations.

Following the work of Star and Straus, the process of making labor visible comes with tradeoffs:

> "On the one hand, visibility can mean legitimacy, rescue from obscurity or other aspects of exploitation. On the other, visibility can create reification of work, opportunities for surveillance, or come to increase group communication and process burdens." [1]

Stories from the field suggest that this paradox is playing out in the negotiation of resources to both IT and facilities departments within the university as they respond to a rapidly changing data acquisition and surveillance environment with the increasing number of IoT devices being introduced to the built environment and the information infrastructure to which they are responsible for maintaining.

The historical precedent of invisibility of this labor is being challenged, through making it visible, in an effort to justify the time and resources this work requires. This has benefits for the organization and the workers. However, it also has drawbacks that include the increasing levels of worker surveillance that result from increased visibility. Star and Strauss [1] as well as Ball [5] illuminate the ways in which this increased surveillance can actually disempower the worker even as it is done in an effort to empower them, or at least make their work more recognized. There is an ongoing negotiation of labor in response to the pandemic, notably, the classification of some work as “essential.” This classification, albeit, ambiguous, illuminates concerns of making invisible labor visible that may result in even more substantial surveillance of workers than before the pandemic. Many campuses remain closed and protocols for reopening are largely still under review, however, this moment of widespread uncertainty provides a lens through which we can center the worker as the subject of investigations regarding the paradox of invisible labor and the sociotechnical responses to keeping campuses safe during a pandemic and beyond. These are conversations that have to consider both public health and privacy, for the individual as well as the larger organization.

Methods

This research is part of an ongoing ethnographic study on the coordination and collaboration efforts toward the secure implementation and maintenance of IoT into the built environment of the university campus. The larger project is funded by the National Science Foundation (NSF #1932769, "SaTC: CORE: Medium: Knowledge Work and Coordination to Improve O&M and IT Collaboration to Keep Our Buildings Smart AND Secure." The findings presented in this paper are based on early ethnographic evidence from observations of various interdisciplinary meetings that take place at a large public university located in the Pacific Northwest United States. The foci of these meetings are interdisciplinary and cross-campus meetings which bring together both technicians and manager/director level supervisors into conversations about IoT implementation, cybersecurity, and the critical infrastructures of the existing built environment as well as new construction projects. This analysis is based on approximately 51 hours of observation data and artifact collection from shared meeting documentation, as well as insights from 13 expert interviews with cybersecurity professionals, about half of which were employed at the same university where these observations occurred, the other half spanning across a diverse range of universities in the United States as well as other industries.

The rich ethnographic data gathered from the meeting observations were supplemented by interviews conducted with many of the meeting attendees and offered a context for the larger scope of the distinct organizations represented at the meeting and their relationships with each other. These meetings bring individuals together from across the university institution, especially those who work in centralized facilities and IT organizations. These individuals represent various specializations in a high-level strategy capacity for the central university administration, code compliance to mandates by outside entities (i.e. state legislation) and perform daily maintenance work to both keep critical infrastructure running as well as respond to these top-down requirements.

Making the Visible Invisible

Spanning observations and interviews before and during the COVID-19 university closures, state stay-at-home orders, and emerging plans to reopen, there is evidence for the paradox of (in)visibility of labor, specifically in the maintenance of universities' built environments. However, as the following analysis will show, this labor surveillance apparatus merits greater attention as COVID-19 surveillance protocols begin to roll out. While much attention has been paid to the more novel and provocative surveillance protocols emerging in response to a return to worksites in the midst of a pandemic, it will be important to remain vigilant about continuing to investigate the more naturalized mechanisms of surveillance that predate COVID-19 responses and that disproportionately affect "essential" workers whose labor necessitates their physical presence on campus. In what follows I will draw upon early ethnographic evidence to illustrate these mechanisms.

Reporting tasks, and self-reporting specifically, is a quotidian activity for many workers, and yet, in efforts to interrogate whose work and what specific tasks are "essential" (a designation marred in ambiguity) the necessity for interrogating the specifics of these tasks is heightened as a mechanism for rationalizing higher public health risk. What follows is a story from the field that begins with such self-reporting measures before the pandemic, continues through the stay-at-home orders, and continues to develop as reopening strategies emerge.

Carl is part of the central facilities staff for a large public university in the Pacific Northwest. He is part of a unit that is responsible for the IT needs for the larger facilities organization. This unit is responsible for the aggregation, maintenance, and dissemination of data collected by various facilities assets. Carl previously held a position within the facilities organization of the university in which he was tasked with utilizing his geographical information system (GIS) skills to map out the assets managed by facilities. This previous role was well-defined with concrete goals and objectives. However, upon moving into his current role in the IT unit of the facilities organization, his role is still emerging, or, as he puts it, "kind of being defined." He thinks it will involve more client-facing work. These clients are often vendors whose products include "smart" sensors and other IoT devices to be introduced to the university buildings as well as contractors and subcontractors who procure and implement such devices. As a liaison between the university facilities organization and these vendors, contractors, and subcontractors, Carl foresees his role to include relationship management and bringing a perspective toward the acquisition of these devices that focuses on the control and maintenance of the devices themselves and the data they collect by the university after they are implemented.

Carl is a regular attendee at a cross-campus, interdisciplinary meeting that brings together various facilities and IT professionals that work with critical infrastructure on campus. The meetings are held monthly and are ad hoc in their nature. Coordinated by a senior leader in the Chief Information Security Officer's (CISO) office who specializes in IoT cybersecurity, the group consists of other central IT organization representatives as well as various central facilities representatives. Usual topics include metering for building energy use, policy, and code compliance changes that impact existing critical infrastructures, and coordination and communication of needs to senior leaders who are not present at these meetings. The meetings are usually held in a central administrative facility building on campus, but in light of COVID-19 closures, have been moved to an online meeting platform.

The nature of the meetings is collegial, and most participants enable video. The conversation is often punctuated with dad jokes. Since moving entirely online, some, but not all participants have been calling in from home. The meetings now start with a work from home (WFH) check-in. The meeting leader asks for a report on any critical infrastructure problems related to the workflow changes due to the pandemic, thus creating an open forum style at the beginning. In a meeting soon after a statewide stay-at-home order was issued, Carl responded to this question noting that he was granted permission by his direct supervisor to come onto campus in order to deal with a connectivity issue with the networks that central facilities require. This network is critical for campus buildings to function and support administrative, residential, teaching, and health service needs. What was particularly interesting about this exchange was the extra emphasis on validation of his return to campus that was sought out and provided by his supervisor. Knowing that working on campus, at the time of this meeting, was limited to "essential" workers, Carl made sure to not only note the permission he received but also diligently recorded his activities on campus while troubleshooting the network repair. This record was made available to the workgroup after it was determined by the leaders of the group that it could be useful in efforts to request more funding from senior leadership.

However, this record-keeping activity was not new to Carl's workflow. While it is not standard protocol across the organization, Carl has made a practice of taking on the extra work of creating a record-keeping system in hopes to someday make it accessible to others as a means for improving efficiency in this type of repair work. This type of additional labor and recording pertains to what has been identified by this interdisciplinary group as the "other duties as assigned" problem. While this documentation was brought up as a means for legitimizing the hours spent on campus during the COVID-19 closures, other participants in the meeting saw this documentation as an opportunity to communicate with senior leadership the resources necessary to comply with incoming code requirements and generally, the maintenance of a secure information infrastructure. This documentation thus has three purposes. First, it allows the worker to maintain a record to justify their being on campus during a pandemic. Second, it can be used to coordinate with other workers with an aim towards more efficient repair processes. And third, it can be used to justify greater budgetary support for the work that is necessary to maintaining secure networks on campus but is presently invisible to senior leaders who control the allocation of these resources.

The third reason, the "other duties as assigned" problem, has been an ongoing topic of discussion in departments across campus. These conversations are happening in response to increasing implementation of IoT in the built environment. Director-level leaders in both facilities and IT are aware of the growing call for more IoT on campus as disproportionate to the amount of support their organizations have for staffing and labor needs this growth requires. Namely, there is a perception that senior leadership is inclined toward the adoption and installation of new devices but is less willing or unable to provide the resources this infrastructural change requires on an ongoing basis for maintenance work. In order to gain access to more support for this labor, and thus to move it from invisible labor hidden in the "other duties as assigned" line of the job description to visible, compensated, and recognized duties, the director-level leadership must rely on record-keeping like Carl's to communicate the scope of this work to senior leadership. The growing number of IoT devices on campus, as increasing network endpoints, and thus cybersecurity vulnerabilities are the real driver making visible previously invisible labor. As the leader of the aforementioned meeting stated:

> "We should keep talking about this and work to further articulate it, because this "other duties as assigned thing," in the past we could squeak by because a couple of folks were doing extra stuff, but with this higher endpoint count, that just doesn't scale and we need to work on how to articulate that. I think everybody on this call knows that. But it would be good to start to think about how to articulate that so we're not giving senior leadership a bunch of one-offs."

What this perspective misses about the sociotechnical change this shift in labor and IoT implementation produces is the fact that, like Star and Strauss present, with this greater visibility comes greater surveillance of the worker. The work that goes into this surveillance is largely being shifted onto the worker themselves through self-reporting measures, like that which Carl has illuminated. In more recent observations, network engineering representatives have suggested contact tracing protocols be put in place as the university moves to open. Curiously, while the IT staff person who brought this up made a point that "there is privacy to think about," the responsibility and decision-making is relegated to "higher-ups" and the technicians and managers of the systems for which these new protocols may impact (i.e. occupancy sensors, access controls) are informed rather than consulted as to how this may impact their maintenance work.

What this signals, especially in light of changing protocols due to the pervasive changes to worksite relations in response to the COVID-19 pandemic is the potential for self-reporting activities and contact tracing protocols to increase worker surveillance in both the hopes of keeping worksites healthy and safe, but also as a means for justifying the allocation of funds to wages/salaries for workers, thus compounding their impact. In the story above we see the potential for this shift, though continued data gathering will be needed to understand the scope of this impact. As we move forward in our data gathering and analysis, it will be important to parse the intent behind such reporting measures as well as the application of this increased visibility, and therefore increased surveillance and the ways in which those workers whose visibility is most dynamic in this period are being impacted.

Symptom Screening

Drastic changes to the worksite and the workflows across the university have taken place in the months following the COVID-19 spread throughout the United States. This continues to be an evolving situation. Tracing these changes and the questions about worker surveillance and visibility that they pose; I argue there is an underlying structure of surveillance for information infrastructure maintenance work that predates higher-profile COVID-19 related measures. This cohort of maintenance workers simultaneously works to maintain the cybersecurity of the institution for which they work, and in so doing, are under heightened surveillance themselves as a result of both efforts to increase visibility for better resource allocation and emerging public health concerns. Their efforts toward securing the information infrastructure of the university require a loosening of their own privacy and security in the workplace as the adoption of contact tracing and other protocols emerge. This underlying structure requires more investigation in light of its potential to amplify worker surveillance in conjunction with emerging protocols for reopening during a pandemic.

By mid-April 2020, in response to increasing concerns about university liability, the university's human resources team mandated that all employees of the university complete a brief survey reporting any COVID-19 symptoms they may have. If they reported having none, they would be allowed to record their hours and, thus, get paid for their labor. If they reported having symptoms, they would be asked to stay home, and they would not be able to enter those hours on campus. An audit of these data is made available to supervisors to account for who has worked on-site and if symptoms are reported that proper time-off or sick leave is also recorded. This sets up an interesting division among university employees. First, as we are now becoming increasingly aware, some work can be done remotely, and some cannot. Second, especially as it relates to information infrastructure workers, that often work side by side with vendors, contractors, and subcontractors, there is a higher level of liability and control for those workers who are employed by the university. For instance, in a new construction project on campus, many university employees who are responsible for maintaining the implementation of new IoT devices and other network-related construction, were not able to come to campus (the worksite) while those who were not direct employees of the university were able to continue their work as usual. Furthermore, we see that those who do have to come to campus to work with these outside workers as well as troubleshoot the devices themselves, there is an increased burden to attest for their presence on campus. This burden is attended to with increased reporting and oversight by supervisors. At the time of writing, the campus has not yet returned to in-person learning models. It will be instructive to make sense of what public health and safety protocols are put in place at that future time and to what degree they align with this noted disproportionality in self-reporting and surveillance.

Surveillance is not new to the workplace. Clocking in and out, logging hours, providing progress reports are all part of a wide array of technologies that work to help supervisors manage workers' labor. Administrative scholar Henri Fayol [7] outlined control and monitoring efforts (read: surveillance) as an integral part of the role of the supervisor. Kirstie Ball [6] provides an overview of workplace surveillance tactics and typology that greatly expands on those measurements previously mentioned. Returning to Carl's story, his record-keeping behaviors, while serving various purposes, align with what Ball has designated a performance surveillance technique as it measures output, location, and communication of this labor. However, as Ball addresses, workplace surveillance often also involves "'function creep': how one particular surveillance technique can reveal more than one kind of information about employees" [6]. As we collectively move into a new phase of the COVID-19 pandemic in which many workers are able to return to their worksites, it may become easy to slip into a 'function creep' toward greater worker surveillance under the guise of public health. While symptom tracking and contact tracing will remain imperative to the global response to the pandemic, it is also imperative that we think through these methods with a consideration of worker surveillance and privacy at the outset. This will require that vigilant observation of this process continues with an eye toward the disproportionate levels of surveillance certain workers are subject to.

Discussion

Workplace surveillance in the form of self-reporting and contact tracing may seem rather benign in light of more invasive measures being taken up globally, including widescale use of mobile data to track citizen's movements, temperature scans via body camera upon entry to various establishments, and facial recognition AI using CCTV footage to monitor individuals in public spaces (see Kitchin for a survey of myriad pandemic surveillance tech applications [8]). However, this self-reporting of symptoms or of tasks met in compliance with emerging protocols like contact tracing, create a context ripe for "function creep." Consideration of these emerging protocols in context with existing protocols affords a purview to consider the complex data traces that, taken together, are concerning in their potential breach of privacy. These emerging practices need to be interrogated and perhaps interrupted, holistically, as they mark a pervasive shift toward more covert surveillance of the worker outside of the COVID-19 context that is being magnified in response to it. The distinction between self-surveillance as evidenced by Carl's record-keeping, and institutional surveillance as evidenced through new workplace attestation requirements, is less clear than previously thought. What distinguishes these surveillance protocols are, on one hand, the level of invasiveness they require. Self-reporting your fever is much less invasive than having your temperature checked by a thermal camera upon entry to the worksite. On the other hand, these protocols are distinct in the labor they require. For instance, many who work at home are not required to report the minutia of the workday tasks, while some workers are being asked to take up the labor of reporting in greater detail. These early observations are indicative of a trend toward "function creep" as theorized by Ball [6]. This is to say that while the impetus for this self-reporting of tasks may serve a strategic goal for more funding or better-allocated resources, it also has implications on the surveillance of the body at work and the impacts of this are disproportionately weighted on those whose work requires them to enter the worksite during a pandemic: the "essential" worker.

The rapidly changing critical infrastructure of university campuses due to the implementation of large numbers of IoT devices, met with the even more rapidly changing health accountability measures in response to COVID-19 should give us pause in the consideration of why and how certain aspects of labor are becoming visible. What early evidence suggests is that labor, once systematically made invisible in the information infrastructure of the university institution, is being made more visible in a dual effort to increase resources for cybersecurity efforts and to maintain a safe and healthy environment as campus moves to reopen. In response to both drivers of this visibility, it is imperative that analysis of the impact of increase visibility, as it tracks with increased surveillance, are impacting workers.

When surveillance measures, which may also serve visibility and accountability efforts, go unchecked, the burden of the risk involved in surveillance and privacy concerns that may accompany these technologies rests on the worker. We need to be diligent in our investigations about the ways in which labor becomes visible. As workers transition back to the built environment of their worksites, be that a university campus or otherwise, further interrogation of the means by which these spaces are negotiating the public health concerns of occupants of the space, the cybersecurity of their networks, and the privacy concerns of their workers must be simultaneously held.

References:

[1] Susan Leigh Star and Anselm Strauss. 1999. Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work. *Computer Supported Cooperative Work (CSCW)* 8, 1 (March 1999), 9–30. DOI:https://doi.org/10.1023/A:1008651105359

[2] Susan Leigh Star. 1999. The Ethnography of Infrastructure. *American Behavioral Scientist* 43, 3 (November 1999), 377–391. DOI:https://doi.org/10.1177/00027649921955326

[3] Beyer, Osburn, & Snider, Emerging Technologies, Existing Infrastructure: The Other Duties as Assigned Problem. [Forthcoming].

[4] Howe, C., Lockrem, J., Appel, H., Hackett, E., Boyer, D., Hall, R., Schneider-Mayerson, M., Pope, A., Gupta, A., Rodwell, E., Ballestero, A., Durbin, T., el-Dahdah, F., Long, E., & Mody, C. (2016). Paradoxical Infrastructures: Ruins, Retrofit, and Risk. *Science, Technology, & Human Values*, *41*(3), 547–565. https://doi.org/10.1177/0162243915620017

[5] Geoffrey C. Bowker and Susan Leigh Star. 1999. *Sorting things out: classification and its consequences*. MIT Press, Cambridge, Mass.
[6] Kirstie Ball. 2010. Workplace surveillance: an overview. *Labor History* 51, 1 (February 2010), 87–106. DOI:https://doi.org/10.1080/00236561003654776
[7] Fayol, Henri. 1949. *General and Industrial Management*, trans. C. Storrs. London: Sir Isaac Pitman.
[8] Rob Kitchin. 2020. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity* 0, 0 (June 2020), 1–20. DOI:https://doi.org/10.1080/13562576.2020.1770587