Surveillance, Technology, and American Conceptions of Freedom

MIKE GRIFFIN
Amazon

This paper traces the role of ideology in shaping the beliefs and situated knowledge used by information technology and security managers to make sense of and justify systems of surveillance they oversee. In particular, the analysis explores the role of the contested meanings of the ideology of 'freedom' as an important resource in this process of meaning construction, providing a ground-level account of the process of interpellation, described by Louis Althusser as the subjectification of individuals by ideology made available from dominant discourse.

INTRODUCTION

In conversation, the head of security of a school district in the suburban United States described a project that he was in the process of implementing across his schools. He had tied together a number of security technologies into a single centrally managed system that he explained was known as a PSIM ("pee'-sim")—a physical security information management system. The technology components consisted of automated cameras with a view overlooking school buildings and areas of the surrounding neighborhood, automated locks on classroom doors, "mini command centers" at reception desks, "duress pendants" worn by secretaries, geo-fenced social media monitoring, and cell phone tracking systems within buildings. All of these fed into a central command center at the district office with wall-sized banks of monitors enabling security staff to look in on and manage situations they were alerted to by people on campus or automated notifications. He described the benefits of the PSIM implementation enthusiastically, portraying students and teachers as being "empowered" by their emergency drill training, and their ability to call lockdowns from any intercom box across the campus. He went on to explain how these components "when they're deployed correctly and right, enhance your learning environment and your school." In his depiction, there was no sense of concerns often expressed in discussions of surveillance, for example about tradeoffs between privacy and security. Instead, he summarized his positive assessment of the system saying, "I believe this technology enhances our freedom. That's just my thought." The statement was jolting.

In many further conversations with managers involved in projects of surveillance, ruptures in meaning arose like the one described above, clashes between the 'common sense' perspectives of researchers and participants, and among participants. As Louis Althusser argued in "Ideology and Ideological State Apparatuses" (1971), such commonsense beliefs often come to be seen as "obvious" through the process of interpellation, whereby subjects freely incorporate ideology into their conceptions of self. In our conversations about surveillance and security, the concept of 'freedom' emerged as an important resource for participants in making sense of their own practices and systems. As the historian Eric Foner (1998) has shown, the ideology of freedom has been a continuous site of contention in the

United States, and has produced multiple, often opposing meanings over time and among actors. This paper demonstrates an approach interrogating participants' statements through the lens of ideology, and further through the prism of the popular discourse and historical contestation that accompanies the ideology of freedom, which allowed us to resolve otherwise puzzling statements, like the one above. Additionally, this paper makes the case that such analysis can lead to a deeper understanding of the epistemes of managers of surveillant systems, placing those statements in the context of a process of cultural reproduction of surveillance.

An Exploratory Project

As part of a technology-focused new business incubation organization focused on computational optics and machine learning, I participated as a researcher on a team whose goal was to assess potential markets for a new generation of 'smart cameras.' This burgeoning class of products combines digital cameras with sensors and advanced computing approaches to enable a range of capabilities that extend security and business intelligence applications in public spaces.

Marketing materials for products in this area illustrate applications as simple as people counters generating heat maps in retail spaces, and as sophisticated as facial recognition, gait identification, gender identification, age estimation, gaze detection, and affect approximation. At industry conferences, it's easy to find live demonstrations of any of these capabilities, along with more fundamental innovations like extreme low light sensitivity, and high order optical magnification.

What followed from this focus was an interest in learning from people at various positions involved in making buying decisions related to classes of products we had an interest in—cameras, networks, video management systems, monitoring services, and services like system installation and management. Because of the preliminary nature of the project, we adopted a lightweight method employing semi-structured, remote, in-depth interviews with informants interestingly positioned in the space of buying and deploying surveillant systems. We developed a protocol, conducted interviews, and also participated in interviews conducted by extended team members, anticipating that further engagement would involve participant observation, an approach researchers on the team have used in the past. Our reliance on interviewing led naturally to a focus on discourse, the narratives of our participants used in describing how they understand their role in surveillance processes, including in terms of attitudes, beliefs, and perceptions.

This project brought many of us on the team into contact with, and implicated us within, the domain of surveillance for the first time in our careers. As members of the US public, we have broad exposure to narratives that emphasize the negative dimensions of increasing state and corporate surveillance. At the same time, we found ourselves enlisted in a project of technological extension of surveillance. Our position placed us in a state of alternation between imagining futures for, and resisting the expansion of surveillance, in new roles as both surveilled citizen-consumers and not-yet-producers of surveillance technology.

In the end, we spoke with nearly 30 participants, including the chief security officer at a multinational retail chain, the director of information technology (IT) and security for a medical marijuana dispensary, the head of IT for a metropolitan sheriff's office, a franchise

owner of several snack shop chains, the head of security for a school district, regional managers for apparel retailers, and a vice president of marketing for a retail analytics startup.

Multiple authors have pointed to a need for more investigation into the realm of surveillance using methods that examine surveillant experiences from the ground up to complement predominantly structural accounts in which "personal accounts and circumstances are often indirectly assumed rather than empirically solicited" (Smith 2015). As Lee (2015) noted, this has motivated an increase in qualitative research, including study of the experiences CCTV camera operators (Smith 2015), analysts involved in online consumer surveillance (Andrejevic 2002), computer based performance monitoring (Ball 2001), and in young people's negotiations around surveillance (boyd 2014).

Our project had the effect of opening lines of visibility into the ways surveillance is produced in part as a result of everyday beliefs of IT project management and security management. Rather than focusing on the perspectives of the surveilled or the surveillant as such, this data illuminated the administrators and managers of surveillant systems—those charged with buying, installing, deploying, maintaining, justifying, and only rarely manipulating such systems themselves.

BACKGROUND

By most accounts, we are living in a state of near-total surveillance by government and private interests (Lyon 2001, Murakami Wood et al. 2006, Green 2015, Haggerty 2000). In a description representative in the surveillance literature, one researcher explained that "the creation, collection and processing of data is a ubiquitous phenomenon. Both private corporations and government agencies take advantage of the increasing technical capability of information systems to gather, process, and store consumer and citizen data" (Dinev 2005). Surveillance is pervasive. And yet its extent is veiled.

Much has been written in the popular press about the rise of technological surveillance. In the wake of the 9/11 attacks in the US, there was significant debate about the USA PATRIOT Act, which established a new regime of communications monitoring (among other measures) in the hopes of providing intelligence that would prevent future similar attacks. In recent years, press attention has focused on dimensions of online surveillance, especially in light of revelations stemming from Edward Snowden's 2013 release of documents describing extraordinarily comprehensive systems developed by the NSA and GCHQ for tracking citizens' communications. In the US, attention has more recently focused on transactional data captured by retailers both in store and online, along with profiling and ad targeting that's become a pronounced feature of Internet-mediated life. The dark potential of aggregating this kind of data has been highlighted in numerous reports of credit card and social networking data hacks, including identity theft.

In 2012, a New York Times Magazine article detailing Target's predictive analytics team was amplified by a Forbes article titled "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did" (Duhigg 2012, Hill 2012). The story advanced a theme familiar in media accounts that a kind of total knowledge is becoming (or has already become) available to states and corporations. Last year a company in U.K. gained some notoriety for deploying psychographic profiling to identify Facebook users for targeted messaging that the company leaders claimed (against significant pushback) may have turned the tide in the latest US presidential election. The promise or fear is that those with access to the tools or data may

understand ourselves better than we do. Even further, with that imagined level of insight, it would seem a trivial step to manipulate behavior to benefit these actors unconsciously.

The emergence of extensive and highly visible camera surveillance in public spaces in the UK also received a great deal of press attention starting in 2013. Camera surveillance is used extensively in US public and private spaces as well, but hasn't garnered quite the same level of attention.

These revelations have had an influence on the American public's beliefs about surveillance. In the wake of the Snowden stories, for example, Pew polling found that 87% of respondents were aware of the NSA program (Madden 2015). In spite of the increased level of concern, however, Americans didn't seem to know what to make of the knowledge, and didn't report making significant changes in behavior. Again according to Pew, combining findings from a number of studies over three years, 93% of US adults say that being in control of who can get information about them is important, and 88% say it is important that they not have someone watch or listen to them without their permission, while only 9% say they feel they have "a lot" of control over how much information is collected about them and how it is used. More than half of Americans – 56% – say it is important to them not to be monitored at work, while 81% agree that surveillance cameras are hard to avoid (Madden 2015).

The Pew report also included summaries of focus group session quotes that surfaced some of the emotions and attitudes that corresponded with these beliefs. One participant invoked George Orwell's *Nineteen Eighty-Four*, an unavoidable reference in any discussion of surveillance, saying, "Big Bro is always watching." Another respondent expressed a sense of resignation at the totality of the embrace of the surveillance society, saying, "Anything digital can record, even a car today tells everything, your cell phone even when it is off is still sending info to the towers" (Madden 2015).

Frames of Surveillance: *Nineteen Eighty-Four* and The Panopticon

By design, surveillance systems introduce and enforce an imbalance of power between subjects of surveillance and observers. Such systems establish lines of sight for observers which are obscured or invisible for the observed.

As Kevin Haggerty and Richard Ericson (2000) emphasized, the writing of two authors dominate discussion of surveillance and each serves to reinforce this top-down framing of "asymmetrical (il)legibility." George Orwell's *Nineteen Eighty-Four* elaborated a vision of a society in which most citizens are under constant state surveillance. This vision, as seen in the quote above, resonates today. Michel Foucault's depiction of the panopticon provides the other dominant metaphor (though less established in popular discourse), analyzing Jeremy Bentham's design of a prison in which a single observer can observe every prisoner, while no prisoner can know when, specifically, he is under observation. Foucault then explained how that kind of surveillance led to an internalization of discipline, in which the prisoner's relationship with himself is transformed, a new model of power relevant for analysis of a broad array of modern institutions. This metaphor continues to be used as surveillance regimes expand rapidly, extending to terms like 'electronic panopticon' and 'superpanopticon' "in line with a general tendency in the literature to offer more and more examples of total or creeping surveillance" (Haggerty 2000). Both of these metaphors

suggest a kind of totalizing bureaucratic efficiency, in which no citizen or prisoner goes unseen.

Anyone who has experience working in almost any kind of public or private bureaucracy would be forgiven for suspecting that this kind of totalization might be *prima facie* an incomplete account. Even in the press accounts of surveillance programs noted here, there's been significant pushback against their claims of extreme efficacy. Commentators have noted, for instance, that the Target pregnancy story seems, on further inspection, a bit implausible. The father cited in the article remains anonymous, and the idea of Target sending mailers with only pregnancy-related offers to any customer—even legitimately expectant mothers—carries such a risk of offending customers that the likelihood of its having occurred as recounted in these stories seems low (Piatetsky 2014). Even so, true or not, the story and others like it inform public understanding of the state of surveillance in commercial spaces.

Kate Crawford (2014), in a close reading of the documents surfaced in the Snowden articles, pointed out how they seemed to reveal the imprecision, ontological slippage and bureaucratic anxiety of those organizations through the clip art-ridden PowerPoint slides created by managers of GCHQ's Squeaky Dolphin program to pitch their capabilities and bid for funding.

In fact, our conversations with managers supports this skepticism of accounts that characterize surveillance programs as excessively efficient or total. Just as surveilled subjects have limited lines of sight into these systems, so to do the managers responsible for establishing and maintaining surveillant systems.

Terms of Surveillance: Privacy, Security, Control, and Trust

Popular discussions of surveillance tend to frame the issues using a limited vocabulary of terms that tend to be ill-defined. As Gavin Smith (2015) puts it, surveillance is "a thoroughly equivocal term" used to arouse hysteria, emphasize security enhancements or reductions in liberty, and highlight instances of discrimination or thwarting of threats.

A recent study (Watson, Finn, and Barnard-Wills 2017), identified four key terms that were used repeatedly in public surveys related to surveillance that they argue frame public discourse in the space: privacy, security, control, and trust. Further, the study found that surveys on privacy suffered from "vague definitions, a narrow focus in conceptualisation of terms and a missing link in the exploration of the intra-relationship between" those terms. For example, only 11 of 17 surveys on privacy defined the term 'privacy,' and 9 of 12 surveys on surveillance use examples rather than definitions (of which the Pew surveys referenced above, emphasis on privacy and control, provide a nice example). These themes were also explored at depth by Christena Nippert-Eng in her book *Islands of Privacy*, which provided detailed interpretations of interviews with suburban Americans making sense of their own experiences of under surveillance (Nippert-Eng 2010). The notion of privacy was brought up directly and indirectly by a number of participants, in ways can be seen to have a close relationship with notions of freedom.

Althusser's Theory of Ideology

Ideas that circulate in popular discourse, including ideas about surveillance, can be understood as articulations of ideology. Louis Althusser in "Ideology and Ideological State Apparatuses" (1971) established a theory of ideology within Marxist theory, as a key resource enabling reproduction of social phenomena, as well as the formation of subjective identity. Althusser described ideology as the representation of imagined relations individuals hold about their real (material) conditions of existence. In this sense, he saw them as an 'assemblage' of concepts drawn from ideas made available from dominant discourse. Specifically, Althusser argued that these ideas are inculcated in individuals through their engagement with Ideological State Apparatuses (ISAs) including the educational system, the media, the church, and the family, for example, colorfully describing how the mass communications contribute in "cramming every 'citizen' with daily doses of nationalism, chauvinism, liberalism, moralism, etc, by means of the press, the radio and television."

Althusser described the process through which individuals internalize ideology as one of *interpellation*. In this model, ideology *hails* an individual, calling out to them in a way that the individual recognizes the ideology as intended, and fitting, for her. Althusser used the metaphor of a policeman calling "Hey you!" on the street. The appropriate individual, sensing the tone of the interjection, turns around in response, thereby making herself subject to the ideology—that is, turning from an individual into a subject. Althusser made the point that that the notion of the subject in this process is ambiguous, possessing a dual nature. On the one hand, the subject is ruled by the ideology which has interpellated her (and thus made herself subject to the overarching ideology of the ruling class). In another sense, the subject has freely chosen the particular hailing of the particular ideology she's responded to, in that sense demonstrating agency in making distinctions among positions available in her social world. While the temporal framing described above is helpful in explaining the process of interpellation, Althusser further argued that subjects are, in fact, always already-interpellated. In his view, this subjectification begins before birth, when an imagined subject's family name, individuality, and class position is determined. Since interpellation cycles continuously as subjects encounter and reproduce ideological articulations, it can also be understood at the level of the subject as a theory of learning, and of identity construction.

We saw evidence of this process in our conversations with managers, in their roles both as assemblers of surveillant systems themselves (i.e., technologies and practices of surveillance), and as assemblers of the ideology representing the relations that support those systems. In recognizing their own identities in common background beliefs, and leveraging them justify the implementation, perpetuation, and expansion of specific systems, these managers also contributed to the reproduction of the social relations supporting the broader social phenomena of surveillance.

Foner's History of 'Freedom' in the United States

While Althusser stated that ideology in general "has no history, or, what comes to the same thing, is eternal," particular ideologies can be shown to take different forms over time and place. In *The Story of American Freedom*, Eric Foner elaborates a framework describing the ways that the concept of 'freedom' has been used throughout American history.

Drawing on Isaiah Berlin's (and Kant's) notions of positive ('freedom to') and negative ('freedom from') liberty, Foner evaluates the competing meanings of freedom in American political discourse in periods from the Revolution through the mid-1990s, paying special attention to sorting out which groups of people stood to gain and lose power in each formulation. Such a framework can act as a prism that reveals the notion of freedom as one that can be refracted from many angles at once, often putting the same word, "freedom" (or its twin, "liberty"), to opposing ends.

For example, Foner cites a 1645 speech by Massachusetts colonial governor John Winthrop that exemplifies a conception of freedom that seems counterintuitive to modern ears. Winthrop focused on the importance of "moral liberty… a liberty to do only good," which represented a kind of inner freedom of self-abnegation "compatible with severe restraints on freedom of speech, religion, movement and personal behavior…" and ultimately with submission to secular authority (Foner 1998).

After the Revolution and Declaration of Independence, freedom was only truly available to "those within the circle of free citizens" which was limited to white, property owning males. As Foner writes, "the Revolution did not undo the obedience to which male heads of household were entitled from their wives, children, employees, and slaves."

In the period leading up to the Civil War, the notion of freedom was bent to the purpose of defending and justifying its diametric opposite, the institution of slavery. In the writings of southerners John Calhoun and George Fitzhugh, these arguments took the form of a critique of relations between capital and labor. Calhoun (1856) described the situation in this way:

> The fact cannot be disguised that there is and always has been, in an advanced stage of wealth and civilization; a conflict between labor and capital. Slavery exempts Southern society from the disorders and dangers resulting from this conflict. This explains why the political condition of the slaveholding States has been so much more stable and quiet than that of the North.

In those terms, slavery was posited to free Southern society from the discord caused by labor's alienation. Fitzhugh (1857) took the tortuous logic of this line of reasoning to its logical conclusion, in an essay called "The Blessings of Slavery," writing:

> The negro slaves of the South are the happiest, and in some sense, the freest people in the world… The free laborer must work or starve.

In this argument Fitzhugh directly asserts slavery as itself a form of freedom—a freedom *from* the anxiety associated with self-determination (positive freedom) in a capitalist system. Such diabolical flexibility anticipates the concept of doublethink associated with *Nineteen Eighty-Four*, in which a slogan of the book's English Socialist Party of Oceania reads: "Freedom is Slavery."

Given the plasticity of the term, it's clear that any assertion about freedom is worthy of at least some level of inspection and interpretation. This framework for untangling the contradictory and oppositional conceptions of freedom became a critical resource in making sense of the divergent and counterintuitive views that emerged from interviews with our managers of surveillance.

EMERGENT THEMES AMONG MANAGERS OF SURVEILLANT SYSTEMS

Our conversations with IT and security managers made available the language they used to describe their organization's use of video in stores, workplaces, and civic spaces, and the beliefs and attitudes they expressed about its use, potential, and meaning. These conversations, then, enabled us to see areas of convergence and divergence among respondents' descriptions of surveillant systems. As will be seen, throughout these conversations, the ideology (and in fact, multiple competing ideologies) of freedom played a particularly prominent role.

Surveillance of Employees

Language managers used to describe their tracking of employee activity was striking in the ways they revealed tensions between managers and workers. While the levels of pervasiveness of tracking varied, most managers expressed sensitivity to the risks of making that surveillance visible to employees. The head of security for a marijuana supplier described their practices as mostly retrospective, but carrying significant consequences for employees.

> Employee activity, we don't monitor unless there's a situation, then we'll go back and review tape. I have a guy in South Carolina that does random spot checks, my super-secret guy in South Carolina that does all my spying for me… Mostly the video and audio that we get from it is almost entirely used for human resources. The HR department always needs a good reason to fire somebody.

The head of security for a pharmacy chain used similarly hidden approaches to track down cases of employee theft.

> At the support office, we have a team that data mines data from the point of sale POS… and they then look at anomalies that would indicate fraud or theft. And then if they get to the point that indicates that what they may have then they use the video to determine what they have. And very often, every day, on the front end they're sending out investigative packages via email that contain the data and video to a guy in the field that says basically saying "Hey this employee is doing this bad thing, stealing, go get him." And then the field guy goes out and talks to the guy and finishes the investigation.

Both of these depictions indicate that these organizations go to some trouble to create infrastructures to definitively respond to employee theft, and at the same time keep surveillance hidden from view of employees. At the same time, the marijuana security had suggested that he believes employee anxiety about the potential of surveillance can impact their behavior, presumably for the better.

> Our employees think they're being watched 24/7. There's something about perception you know what I mean... [uncomfortable laughter]

A marketing lead for a retail technology startup expressed similar sentiments:

> You know these days I think almost everyone involved in retail has that feeling [that they're being watched], because in a lot of cases it's true, so... [uncomfortable laughter]

For managers, awareness of surveillance was imagined to temper unwanted employee behaviors, but too much exposure was imagined to potentially lead to backlash and confrontation. One of our informants, a regional manager for an apparel company, whose office was based in a store, and had close working relationships with his store staff, explained his concerns:

> Undercover Boss could never happen here. We can monitor video, but it's a double-edged sword. If you use it in a review it can go bad on you pretty fast, a little too Big Brother... Referencing it in conversations can feel micromanaged.

The COO of a retail fashion manufacturer described his staff's reaction to the installation of cameras in the workplace.

> People got a little excited that we installed cameras in warehouse. If you're behaving appropriately why worry?

The phrasing used by these managers indicate a preference for keeping employee awareness of surveillance beneath the surface, out of sight of employees and out of discussions with them, to prevent uncomfortable conversations. In effect, the fact that employees were never fully aware of the extent of their subjection to surveillance meant that they couldn't directly address or change the situation. Surveillance persists with a slow-burning tension in relations without becoming openly contentious. Secrecy is a privilege of management that both emerges from and maintains imbalances in power.

Other practices managers described included using methods that didn't connect with video monitoring. Rather than direct observation of bodies, these methods relied on proxies for work done, like an apparel store operations manager tracking the number of units processed (here meaning boxes unpacked) per man hour. Similarly, the CEO of a chain of ' better burger' restaurants described tracking sales per server in his restaurants.

The security lead for a pharmacy chain depicted a team in his headquarters office who use video data from the pharmacy to plan labor workflows and training protocols for pharmacy staff.

> They used to go out into the pharmacy with a clipboard and take notes and you can imagine how that corrupts the data, so to speak, cause you know people behave differently, when there's someone standing there with a clipboard. Now they watch video from here, out in the stores, and can kind of make annotations.

On the other end of the spectrum were owners of smaller businesses who kept tabs on their workers using methods that were more persistent and invasive. The general manager of a family-owned commercial equipment repair company described how she tracked repair trucks using GPS, and reviewed open job logs in their ticketing system during the day to assure herself that her repair people were active and productive.

Even more extreme was the owner of a number of pastry franchise locations. He laid out his biography as a series of rational economic decisions. Having assessed his

opportunities while studying for a CPA in Chicago, he relocated to Phoenix ("the fastest growing city in the US at the time") to start a food business ("it's easier to scale a food business–everybody needs to eat"), particularly as a franchise with a company "with a good track record." He described the multiple methods he employed to keep tabs on his stores, to "get a good pulse." In addition to getting data from his point of sale (POS) system, and occasional "unannounced quality restaurant inspections," he described his practice of pulling weekly employee audits to see how employees were performing and to make sure that there was no indication of fraud, like "no-sales."

> It's not always about punishing, it's also about rewarding… whoever gets the highest sales, most drinks, we give them a gift card. That's how we spin it to employees. Really, it's more like, checking everything, making sure there's nothing fishy going on, people not pulling their weight.

He also described how he leverages the video security systems he installed in each store. He described being able to access these systems from his home office, or even an app on his phone. He described being able to check in on one of his stores is in a mall, near a children's play area:

> I was checking our cloud-based POS and saw that one store was really busy, so I turned on the cameras for the store to find out why. Are we doing something right, or is just busy at the mall? I use that reverse method. I'll say, "You got through that line really fast, you're killing it out there." But really, you should know that I'm using that camera… They know it's good that I make those calls so they know that I'm always watching but they don't know when.

This video security system replaced less expensive "nanny cams" that came with built-in microphones and speakers. In describing how he had used that system he shared this story:

> These cameras didn't record, I just had them on the counter pointing at customers, and it allows for audio, had the two-way audio thing going, and from my phone I called "There's no one at the front, we need somebody here now!" They thought it was a ghost. But I was just messing with them.

The manager also described his greatest challenge in being the difficulty of hiring and retaining staff. It's tough, he explained, "finding those right people, people you can trust, count on, especially at the manager level."

These approaches of measuring and monitoring employee exemplify forms of "scientific management" that would be recognizable to the original proponents of Taylorism, who similarly counted (and prescribed using arguably arbitrary calculations) the tonnage of pig iron Hungarian steel workers carried to trains in the course of a working day (Stewart 2006).

The worldview that underlies scientific management is built on a belief that labor, once freely exchanged for capital and in submission to oversight, abandons some aspects of liberty in relation to labor. As Louis Althusser (1971) stated it in Marxist terms, "all the agents of production, exploitation and repression, not to speak of the 'professionals of ideology' (Marx), must in one way or another be 'steeped' in this ideology in order to perform their tasks 'conscientiously.'"

In the history of the United States, multiple positions have adopted the language of liberty. Even today, Melissa Cefkin (2014) pointed out that in discourse around emerging

forms of peer and open work, 'freedom' from hierarchies in the workplace can also be seen as leading to the "neo-liberal feudalism, the demise of job security."

In the late 19th and early 20th century "freedom of contract" was used to denote an ideology that governments ought not interfere with companies' right to make contracts freely with individual workers. In competition with this concept, "freedom of labor" was used to describe "freedom to participate in decision-making through strong unions, freed from management hostility and court injunctions" (Foner 1998).

The head of security for a pharmacy invoked another kind of freedom in justifying employee surveillance, harkening back to the Puritan model of "moral liberty," here in the form of freedom from "bad choices."

> So we have video pointing at all the cash registers, because we know this is retail, and sometimes people make bad choices sometimes, and they either take money, employees, or they might pass merchandise to a friend of theirs...

This type of freedom, the freedom from making bad choices, has roots in the early history of the US as well. As Foner (1998) explains it, "Puritans were governed by a "moral" liberty, "a liberty to that only which is good," which was compatible with severe restraints on speech, religion, and personal behavior."

In each of these examples, it's clear that competing definitions of liberty are at play in justifying systems of surveillance in the workplace. For many of these managers, the freedom workers have to chart their own course as agents in the labor market (in accepting terms of employment and accepting wages) means abandoning freedom to do as they choose within the confines of the work environment, and thereby submitting themselves to ongoing surveillance by management, on management's terms.

Backstopping of Surveillance by Police

It's become natural, living under the implacable gaze of cameras, amidst visible signposting and prominent monitors above store doorways, and among narratives shaped by narratives like *Nineteen Eighty-Four* and the panopticon, to presume that an operator at some remote location may be actively watching our every move. While managers described relatively intensive surveillance of employees, many reported expending much less energy monitoring the behaviors of consumers or the general public, whether to generate business intelligence, or even to prevent theft. Based on manager accounts, that is not typically the case. Most participants reported looking only occasionally at video footage, and then only after the fact, when alerted to a problem. As the vice president of a large coffee chain explained, "We don't touch that. We're not looking at LP (loss prevention) from the customer side at all." While the occasions were rare, managers' stories did highlight the connection between private and state assemblages of surveillance, through practices that included of handing off video footage to police in support of investigations.

A marketing executive for a bank provided an explained how footage his company captures can end up being used by law enforcement organizations:

> I haven't looked at it in a long time. Except the time we had a robbery. Actually, over time we caught a bunch of them. I'm not gonna say we have 'em all the time. A few a year. Usually we just

> give police snippets, and they make photos that they give to the FBI. The Cross-Dressing Bandit, they name 'em, not sure if that comes from the news media, or the FBI, not quite sure.

The security lead for a pharmacy chain explained that his company's footage is shared with police as well, rarely but according to established protocol:

> In the course of a year there are gonna be a half dozen things that can happen, theft, slip and falls, they're gonna have to be able to pull the video, burn it to CD, send it to the police, if the police are out there, if it's a robbery they'll—so they have it there.

The head of maintenance and facilities for a regional transportation agency described his organization's connections to local police as well:

> We do supply video to the sheriff's office when there's an incident that requires it… we review incidents that happen on the bus, whether it's a trip and fall or graffiti or any kind of damage to the bus to ferret out who did what.

The owner-operator of a pastry chain provided a recent example:

> I had to look at some like a month ago, we had someone who was stealing from us. I had to get police involved, copied some footage for them. It was a shift manager. Deposits in cash were there, but credit cards were not. When they sent the workbook at end of the week, didn't reconcile to POS.

The connections and enunciations between private and state systems of surveillance is not trivial. As Althusser (1971) explained, "the State is explicitly conceived as a repressive apparatus… which enables the ruling classes… to ensure their domination over the working class." The practices connecting private and public systems of surveillance—transmission of data, copying of tapes, phone calls and practices of collaboration—enable the expression of the system's inclination toward furthering enclosure. In Althusser's depiction, the distinction between public and private is a false one on its face, since so-called private institutions in any case serve the interest of the state, and the ruling class. More importantly for this analysis, in the accounts of managers these traversals appear as mundane, taken-for-granted facts in their social worlds that don't require further explanation or justification. They are simply common sense.

Limited Surveillance of the Public, and Abbreviated Ethics

Managers did grapple with the meaning of surveillance of the public. Their responses displayed a wide range of attitudes about the ethics of public surveillance, and situated those attitudes in a kind of balance with other concerns.

Even in sheriff's jails, video wasn't likely to be monitored live.

> Yes, we have security cameras for guarding and watching facilities. Mostly for security. Most of the cameras aren't monitored live. It's for going back and reviewing later if there are concerns.

The head of IT security for a marijuana dispensary had no qualms with monitoring the public.

> They're in a public place they have no expectation of privacy, nor do my employees. I record audio, I record video. They shouldn't have any expectation of any privacy or any type of anything.

The head of security for a pharmacy chain described a tangle of beliefs. In the first place, he felt the public is given fair warning that they'll be surveilled.

> There's lots of signage. When you walk in the front door, there's a public view monitor there if you look up. It should either have a sign on it that says "video recording in progress," or the new ones have an embedded sign on the video itself that pops up that says video recording in progress. Then we have these public view monitors in four locations in every store: one at the front, one at the pharmacy pickup window, one on the drug wall, and one in cosmetics wall and all of them have that same sign. And then we also have a sign at many stores on the front door, for safety and security, video monitoring, alarms, time delay safe.

Though minimal, he did describe some dissatisfaction with customers in being watched, that also hit at the uncertainty some members of the public hold about the potential power of surveillant technology.

> In the retail space, everybody knows there are cameras monitoring activity. I have a hard time thinking of any time we had issues with that. The pharmacy space, we have had an occasional customer… that says "Hey that camera can see my prescription!" And we can very, very easily demonstrate to them that it can't read it.

Prompted about extending the capabilities of his deployments to track customer activity for marketing purposes, the same pharmacy manager described concerns about public reaction, *Nineteen Eighty-Four*, and the pharmacy's brand.

> A lot of that has been discussed, and obviously there's technology issues there, there's privacy issues there, there is perception issues there. We talk about you know the cell phone data and tracking that data, that person, and even if it is anonymous so to speak remember, we're a healthcare company when you walk back into that pharmacy, HIPPA [US federal privacy] laws apply. So we're very, very sensitive to that. We give thought to those things. One, we're always compliant with HIPAA and then we want to appear to do the right things for our customer, even though it might not have to do with HIPAA, we don't want to give the appearance that we're not doing the right things with our customers data. So that tracking of cell phones and that Big Brother and all that kinds of stuff we really have to think about, ah... um, a lot.

The chief information officer of a sheriff's department invoked the publicity around CCTV deployments in the UK, and Las Vegas, to describe the relative limits of deployments he manages in public space.

> It's not like England where we have constant facial recognition. Here there are specific legal requirements, and also civil liberties concerns. Ironically, people fear what government and law enforcement do, but we are the least progressive. In retail and gambling there's a lot more identification going on. You can't walk anywhere is Las Vegas without being recognized.

A bank vice president responsible for marketing described the challenges she faced when rolling out a remodel, and the balance she tried to strike between crime deterrence and branding.

> We had to incorporate cameras into branches, so we had to design cameras and branding. Sometimes it was a little off. Like we have the big red wall as part of branding, and sometimes the cameras were in awkward places, uneven, or standing out in a weird spot, but they want their cameras in certain places. It's very important.
>
> I don't know how the customers feel, I guess they're being video'd anyway. I wonder how the employees feel, but cameras capture employees anyway. But showing that data to a wide variety of people? Probably want to limit that. It's somewhat an invasion of privacy, though employed.
>
> Could we repurpose it for customer tracking? I haven't thought of that but it's a good idea. It's a little Big Brother. There are all these privacy requirements.

In these accounts, managers invoked a broad array of ways of justifying the deployment of surveillant systems on the general public, in relational rather than moral terms—relative to 'expectations of privacy' (a narrowly legal definition), relative to surveillant interventions (like Las Vegas) deemed to be more intensive and widespread, relative to its visibility (i.e., the fact that it's literally signposted in public spaces), and in relation to brand expectations. Concerns about civil liberties were construed through the lens of regulatory compliance, which served to domesticate ethics as a form of technical requirement familiar to managers of information technology projects.

These statements also can be seen as underlain by claims about the nature of freedom under regimes of surveillance, in a way that connected with the notion of privacy. We saw that 'privacy' tended to be invoked in alignment with 'civil liberties,' and in opposition to 'Big Brother,' a shorthand for top-down, 'creepy' surveillance. In that sense, privacy could be seen as a stand-in for a commonsense type of freedom—freedom from being made visible to agents of institutions of power. Put simply, privacy is equated with freedom from surveillance.

Reviewing popular discussions of surveillance, key terms like 'control' and 'trust' can also be seen as relating to this definition of freedom, specifically as a desire to choose which agents are able to negate a freedom from visibility to the powerful.

In these conversations, the metaphor of Big Brother was invoked as a kind of line in the sand, a stigma to be avoided. The threshold for crossing into that arena, however, appeared to be set by the imagination managers held about the perception of the surveilled public rather than on the basis of an internal moral distinction. This seemed to be operationalized as an assessment about how a given surveillance intervention would compare to what managers imagined public to find 'expected' or commonplace.

Managers under Surveillance

Managers expressed a range of attitudes about their own perceived exposure to surveillance, demonstrating a mix of stances from insouciance to resignation. While very aware of the limitations of their own systems, they didn't seem comfortable dismissing the possibility that

systems run by others—who were not within their own lines of sight—could be more sophisticated, efficient, or totalizing.

The security lead for a marijuana dispensary demonstrated resigned savvy.

> I mean on a personal level, I mean heck you're on camera the minute you drive out your driveway pretty much. Can't get away with much...

The vice president of marketing for a sensor startup shared a similar view.

> I can't remember the exact numbers, but they're shocking. It's like the number of times somebody's captured on video was insane, it's like 200 or... [laughter] I was counting them last night driving home. I was at a major intersection and there were, sure enough, 12 cameras on one intersection! Like, "Wow, I can't believe…" Palo Alto's a very secure city I might say.

Asked about his own concern about being surveilled, the chief security officer for a coffee chain explained flatly, "I don't care."

The chief financial officer of an apparel company wasn't sure about his own subjection to surveillance within the company, saying "I don't think I'm being monitored. I'm not aware that it's happening to others, but anything's possible."

As mentioned earlier, the sheriff's chief information officer also referenced privately owned sites of intensive surveillance, saying "You can't walk anywhere is Las Vegas without being recognized."

For one informant, his experience coordinating retail technology conferences tempered his assessment of the state of the art, and represented a divergent view of the capability of systems that weren't under his direct supervision.

> Are these systems widely adopted? No, not at all. People are playing so close to the vest in terms of what they release to the public. I think there's a wide gap between what we see and what is actually in the marketplace... The science fiction stuff that we get excited about is not widely adopted yet.

These accounts highlight a picture of surveillance that is more complicated than common top-down models that posit two primary actors—agents of surveillant institutions with power, and the citizen-consumers subject to their gaze. Instead, these narratives show managers entangled within the surveillance of others, connecting the dots and reading into what they imagined was happening behind the scenes, their lines of sight limited in their role as surveilled subjects in in the domains of property owners. Managers here applied a similar logic in making sense of their own surveillance to that which they applied over their own organization's employees, and the public. As employees themselves, they understood that they were possibly trading away freedom from surveillance as a contractual term of their employment (though to what extent was unclear), and as members of the public, they had little expectation of privacy for themselves. Though they understand the limits of their own technical systems, they were capable only of imagining the potential of systems beyond their lines of sight.

The Mundanity and Intensity of Surveillance Management

Managers' stories indicated that many of the workplace challenges our participants explained were mundane, representing the familiar everyday challenges of any information technology project manager, from wrangling contracts, to acquiring budgets approvals, managing resources, and meeting deadlines.

The head of security for a marijuana dispensary described a new building project to overcome his biggest challenge—bandwidth—which he had begun planning and budgeting to address through a custom buildout. His language was typical of participants.

> Biggest thing holding me back is bandwidth in some of the locations I have… Everything is on Comcast broadband but one site is on microwave. I'm building my own 100-ft tower and building my own wireless network. The ROI will be within a year, even if I spend 50k building all this out.

Bandwidth limitations were echoed by many of the managers we spoke with, including a project manager for a pharmacy, the head of IT for a lumber company described being behind the curve, and the IT director for a fast food chain. The sheriff's CIO also described challenges managing fiber bandwidth and network architecture but also detailed the headaches of complying with IT regulations that enforce civil liberties protection.

> Keeping up with technology trends is important. Cloud is complicated because we deal with PII, PHI, restricted law enforcement info, intelligence. You need clearance to look at this information. Dealing with all of these different data with different access structures, is complicated. Custody is complicated. Lots of information is crossing boundaries, including health, intelligence and all these other categories.

And yet the mundanity of IT abuts the responsibility these managers take on for preventing extreme violence on behalf of their organizations. Asked about his top urgent project priority, the chief security officer for a coffee retailer flatly explained:

> I'd like to get more predictive about terrorist attacks.

The top priority for the pharmacy's head of security was preventing robbery.

> The biggest problem we have on the security side is robberies. Robberies are a stick up… where someone pulls a weapon. We're throwing everything we have at it but we still have a problem we're always looking for anything with technology that will stop those things. Alarms, safes, always looking for ways to do things better because those can be very bad for our employees.

In the sheriff's department, even for the chief information officer, shootings were a top concern.

> If I have an employee involved in an incident. I have a deputy who got involved in an off-duty shooting, or it could be part of my managed operation, like a rogue IT person doing something they weren't supposed to do.

Haggerty described the will of surveillant assemblages "to bring systems together, to combine practices and technologies and integrate them into a larger whole" (Haggerty and

Ericson 2000). The fact that physical violence hangs in the balance for managers in their everyday responsibilities looms large in the decision-making that goes into choosing and deploying technological systems of surveillance, and can feed a tendency to move continuously toward more extensive interventions, and more complete enclosure of surveillant systems.

SCHOOL SECURITY: ENHANCING OUR FREEDOM

Many of the themes traced above were evident in depiction of the physical security information management system (PSIM) provided by the school district's head of security at the opening of this paper. He summarized the array of machinic components of the system that had been deployed in that time. These included automated cameras with a view covering areas of the surrounding neighborhood, automated locks on classroom doors, intercom systems, motion detectors in classrooms to confirm rooms are cleared during SWAT team sweeps, "mini command centers" at reception desks, "duress pendants" worn by secretaries, along with buttons installed in their desks, and cell phone tracking systems within buildings. All of these fed into a central command center at the district office with wall-sized banks of monitors enabling security staff to look in on and manage situations they were alerted to "aggressive situations" by people on campus or automated notifications. He also touched on themes of surveillance of the public and employees, ethics, and the mundanity and intensity of managing security and surveillance projects. But while most participants justified surveillance in terms of tradeoffs (for wages, or public safety, for example), he evinced a unique approach to making sense of the program of surveillance he had instituted, justifying it as a freedom-enhancing, positive good.

At the beginning of our conversation, the director gave an overview of his career. He was in his 27th year at the district, having worked there since a four-year stint in the Army as a military police officer. It's notable that in Althusser's terms, his career began as a member of the Repressive State Apparatus (doubly as military officer and police officer), and moved to the most crucial of Ideological State Apparatuses (the school). He described his district in terms of the number of schools in the district, the area covered, number of students, the educational awards the district had won, and the fact that their response times to an active shooter event was estimated to be in the range of "immediate to two minutes."

The Active Shooter Incident

One devastating incident loomed in the background of this conversation, though he alluded to it mostly in passing references. Four years previously, at a high school in his district, a student brought a gun to school, unfortunately using it to murder a classmate. While the systems and procedures he and the district had implemented were credited by an investigatory committee with preventing more extensive violence, they were not able to prevent the tragic event. Further, these systems were deemed to have broken down in important ways. For one, the network was overwhelmed as multiple law enforcement jurisdictions attempted to access the school's cameras. Secondly, the video management system's time stamps proved to be out of sync, so review of footage after the fact was hindered as the events were being investigated.

In large part as a response to that traumatic event, over the last few years, he worked with the school board to raise funds to increase staffing and invest in a new technology infrastructure. Surveillance researchers have argued that this type of security response after the fact of tragedy amounts to a kind of "'actionism,' in which surveillance's advocates consistently argue that doing something—CCTV installations, pat-downs, shoe-scanners—must be better than doing nothing" (Hannah 2010).

The director described the PSIM as "open" in terms of its technical architecture, which allows the use of cameras from any manufacturer, and is easily extensible. In addition, following the guidelines set out by a partnership between two industry lobbying groups, the Security Industry Association (SIA), and the National Systems Contractors Association (NSCA), he began training the entire school community in incident response protocols, bringing together all of his technology assets, along with the school community into a unified technical and human system. In his telling, this system involves the neighborhood, the parent community, teachers, staff and students in a unified mission.

Empowering Teachers

A key theme the security director returned to was the idea that the installed system "empowered" the members of the school community.

> The empowerment piece is, for example, I mentioned all those staff members we have working for us, we also have everybody is technically a staff member and every student is potentially a security officer for the school district.
>
> They are also empowered to have their own mini command stations or security interactive, or how do I say, security technology that they use on a daily basis to keep their school safe. So those 175 people, even though they don't work directly for us, they—we have 175 additional eyes using the technology we have out there.
>
> [In a] lockdown, where anybody can call a lockdown, I mean a staff member or a high school aged student, or middle school, where they see something that is potentially violent or could bring harm to them, they can call that, it's not just something that can be you know the old traditional way, you're empowering people to react to things that might be detrimental to them.

He further described the change of attitudes in the district in recent years, with people who may have initially rejected a stronger surveillance system now finding value in the protection it afforded.

> When we started in the 1990s, there was a lot of pushback to it, surveillance. "That's Big Brother," when we started installing call boxes and visitor management. We don't get that pushback now because it's keeping their kids safe… people who were apprehensive about it kinda retired, it's like a team.

The PSIM in Action

The director provided a few examples of how the system, now fully implemented, operated in concert to react to potential threats to the campus. These examples proved rather

extraordinary. In one instance, a person not associated with the school attempted to gain entry during school hours, which triggered an alert and action by the school staff.

> This person tried to get into the school, maybe intoxicated, and he collapsed on street. They got him help, and it turns out he was mentally challenged, and very nervous about starting his first job. He collapsed, they got him help—hey, that's what the technology and practices are there for, He was not a potential threat, and they got him help.

In another example, the automated systems detected another disturbance after hours, this time in the community surrounding a school, rather than the school itself.

> We had domestic violence this past weekend, abusive drinking, this couple had 32-ounce bottle of Coors Light, they were fighting on street. The intercom started recording their argument, and a neighborhood patrol and law enforcement all respond.

The following night, the system detected a false alarm, with an amusing result.

> The next night a guy and a girl with paint brushes were picked up on camera. The analytics picks it up, alerts us, we respond, but it turns out they're not bad guys—they're people who study spiders! They're in there in the cracks of wall with brushes, to get spiders to come out. But from the video you can't tell what they're up to, it's bizarre.

His final example occurred the very first weekend they installed automated cameras at a school, resulting in the arrest of thieves posing as construction workers.

> The first day we put cameras in place, part of the school was a construction site. The cameras went online, and pick up guys taking roofing materials, welding equipment. The cameras hadn't been tuned, but they picked up motion. They auto-tracked them, these guys were disguised as constructions workers, and tracked their car out of the lot. They were caught by 6pm, with no analytics, awesome. So my job's tremendously easier.

These anecdotes demonstrate the director's understanding of the power of a tightly integrated system of surveillance, linking motion-detecting cameras, monitoring by school staff and security personnel, and connections to local police departments.

Relations with the Community

The PSIM system, as described in the examples above, engages the community in multiple ways, beginning with the security and surveillance provided by the cameras, microphones, and motion detectors that cover neighborhood areas beyond school campuses. Again, the director provided an example.

> The security cameras are quite noticeable, a deterrent in themselves. we're seeing reduced vandalism. In the 1990s we got tagged almost every night, windows broken. It was usually a student or something, but since cameras have gone up that's been reduced by 95 percent. A neighborhood could be Grafittiville, but not on the school! There's a perception that cameras see into the neighborhood, so those parts of the neighborhood don't get hit.

Schools are also of course an important part of the fabric of the community. One dimension of this relationship is economic support. When funding was required order to build out and maintain the PSIM system, the district proposed a US$5M bond measure which was passed with citizen support. This funding was supplemented by a federal grant secured by the director and his team. The director explained the positive economic feedback loop between school and community.

> Property values are tied to safe and high-performance schools, which leads to higher equity for the community. That was an important part of the pitch to raise money.

At the same time, he described efforts to prevent security interventions to present a negative impression of the school or the neighborhood.

> Signage is critical, to have it at strategic points, every school ground has it at entrance points, and on the structure of the building there's another sign that says 'Attention video surveillance, trespassers prosecuted.' But it's not like a prison… Administrators are like, "I don't want my school to be turned into a prison."

He also described ways in which community members were entrained in the program of surveillance.

> Our surveillance system is also empowering the community. We have neighborhood watches that we call Watch Dads. Our school buses report back when there's any kind of issue, and we're working to build apps to get information about threats or concerns from parents and the community.

At the same time he described ways in which the schools provided resources for the community, to a point.

> After hours, 10pm to 4am people are gonna walk dogs. It's important they're not getting too close to the bricks, not throwing things at the window. We're not gonna go harass them, but if somebody's got a can of spray paint we want an alert… We don't have a problem with taking a walk at night, even though it says 10pm

> It's an open campus, students can come and go. But walking down street and you need to use bathroom, go into a K-5 school, those days are done.

Descriptions like this, told from the point of view of an administrator of school security, have implications beyond the vantage point of IT project management. Between the lines of his depictions of community and police relations, are resonances of issues like public space, economics, race, and power that call to mind Mike Davis' *City of Quartz* (1990), which described the social history of Los Angeles. In Davis' telling, the "suburbs demand segregation and ghettoization" where "neomilitary syntax of contemporary architecture" keeps "good citizens at home in private spheres of consumption, bad citizens on streets illegitimate," and "sheriffs relentlessly restrict public space, hurt freedom of movement of the young."

In the story of the spider hunters mentioned in the previous section, it's clear that the ideology the director has assembled for himself fails to anticipate the desire, on the part of

members of marginalized communities, for freedom from violence that can accompany encounters with police—agents of the State Apparatus authorized to deploy sanctioned violence. What was an amusing story in this instance could easily have a much less amusing outcome for another group of neighbors.

Manufacturers as Collaborators

In multiple instances, the director expressed an enthusiasm for vendors, integrators, and manufacturers of security components, at one point saying to an interviewer, "keep improving the industry. It's just fantastic to see. I feel like I'm in Star Trek world." He continued:

> I used to dread manufacturers coming back when I had no budget now. I'm open to it. With all this new technology, feel like a kid in a candy store.
>
> I'm open to integration, always wowed by things, envious. We have an open architecture system, the whole point is I have one VMS [video management system], but I can buy whatever fantastic camera you have, even if I can't afford your VMS.

He also mentioned the role of industry groups in supporting his efforts.

> [The industry group], they provide a tiered continuum that helped us immensely, they helped us to get our funding.

This connection with industry, along with his enthusiasm for industry partnership hints at the practices and relations that support the reproduction of the broader phenomenon of surveillance.

Looking to the Future

Asked about what he saw in store for the future of his district's school security program, he again expressed enthusiasm.

> It's a Renaissance period. Every day there's something new, I'm hoping that the industry continues to do that. I'd love to see more user-friendly Android apps, more integration of VMS and visitor management. I'm a huge proponent of video.

He imagined future scenarios enabled by further integration.

> But what about… you take a picture for a background check, but what about before they enter the building? We could work with [vendors] and integrate a driver's license swipe or whatever background check before they enter the building. That's the final frontier for great access control, to identify the sex offender… that's my dream, not saying any perverts got in.

He further imagined scenarios in which the PSIM system could provide automated warnings to people identified as potential threats, imagining what amounted to buildings acting autonomously as agents of security.

> It could be like, "You in the red jacket!" An automated response. That's exactly what we're looking at once the [new] system is online, those kinds of features. "Welcome to the school." But if you stay too long, a voice comes over and says something, that to me is wonderful.

These depictions suggesting futures imagined for the surveillance system he manages demonstrate not only his plans (in cooperation with members of the security industry), but also the will of the assemblage itself to become both more integrated and totalizing, and more agential.

RESOLVING DISSONANT CONCEPTIONS OF FREEDOM

The pivotal statement in the conversation with school district security director was this surprising and puzzling assertion.

> I believe this technology enhances our freedom. That's just my thought.

In that moment, his characterizations seemed to have gone past the point of euphemism into the territory of 'doublespeak,' of *Nineteen Eighty-Four*. In summarizing the effect of the array of technologies that comprised the systems that he'd implemented in the schools—and perhaps slightly more broadly, the array of technologies made available by industry to people in his position to bring, both now and increasingly in the emerging future, new levels of security (and surveillance) to schools—it was difficult to see how increasingly circumscribing civil liberties in public places could be seen to enhance or advance freedom. The most peculiar aspect of the statement, and that which most diverged from that of other managers, was the positive relationship he posed between surveillance (an imposition of power over the surveilled) and freedom (associated with privacy, or the freedom to act without visibility to the powerful). To help make sense of this statement, it is helpful to think of the statement through the lens of ideology—as a commonsense belief, drawn from concepts made available by dominant discourse. Further, the fact that this statement represented a site of ideological contention is supported by its inconsonance with the many other narratives relayed by other participants. His language represented an inversion of the typical rhetoric in this space which tends to construe security and privacy (a kind of freedom) in opposition with each other, or seeks to find some sort of appropriate balance between the two. His statement moved to align the concepts, in an unproblematic relationship of mutual reinforcement.

Tamara Dinev (2005) has pointed to the rise of rhetoric "consolidating security and privacy ("security and privacy") rather than antagonizing ("security vs. privacy") these two seemingly polar values." That rhetoric was deployed in a 2001 speech delivered by President George W. Bush in response to the September 11 attacks, in which he announced the creation of the Department of Homeland Security (followed shortly by the USAPATRIOT Act which dramatically expanded the ability of governments and police to surveil the American public). In that speech, Bush stated, "I will not relent in waging this struggle for freedom *and* security for the American people." This language joined freedom and security (and implicitly, surveillance), but stopped short of saying one actually enhanced the other. A reasonable interpretation would allow that those values might be pursued with a sensitivity to balancing or managing trade-offs between them.

More recently, there have been some signals emerging in popular discourse that support the director's assemblage of freedom. As one Fox News commentator put it recently, "The civil liberties faction who hate surveillance operate on a lie: that security infringes on freedom. No, security enhances freedom, which insures [sic] our survival." (Gutfeld 2016). A writer in Security Magazine (also a security industry executive) provided what might be a clearer interpretation, writing "Basically, 'security' is 'freedom from danger.'" (Mech 2006).

Freedom from death, freedom from danger, freedom from trauma. All of which, put in such terms, seem like worthy, if not the ultimate forms of freedom. As Hong (2017) has pointed out, "The 'right to be let alone' appears a relatively indulgent, bourgeois quibble when placed into such stark conflict with the 'right to be free from death and violence.'" Further, given the director's first-hand experience with, and sense of responsibility for, the trauma that accompanies unpredictable violence, make a great deal of sense that he would draw on and reproduce a narrative strongly bolstering his justification for action.

CONCLUSION

This paper demonstrates an approach to making sense of interview data by focusing on commonsense assertions as expressions of ideology. Understanding these statements as part of a process of cultural reproduction, in which subjects internalize ideology as part of their own identity construction, enables these statements placed in relation to popular discourse, as well as in relation to historical context.

In these discussions of surveillance, freedom emerged as a key concept, and as a site of contestation. In some cases, the concept of freedom was invoked directly by participants; in others, freedom could be seen to underlie other concepts like privacy and trust. Focusing on these contested meanings of the ideology of freedom enabled an analysis of the key themes that arose in our discussions of surveillance and to resolve apparent contradictions. Foner's framing highlights three aspects of any assertion about freedom: evaluation in positive or negative terms ("freedom to" or "freedom from"), characterization of the social conditions that give it definition, and identification of the group of people inscribed in the circle of its entitlement. Seen through this prism, it became possible to think more flexibly about potential variations of meaning, and to investigate sources that can clarify ideological assertions. In this case, one can see the ways in which the security provided by surveillance (through the PSIM system), represented a kind of freedom from arbitrary violence and trauma. Freedom (as perhaps any ideological signpost) indeed can function as 'doublethink' or even 'multi-think,' enabling a subject to internalize conflicting meanings within the same concept and identify the term as their own, as part of a process of developing or maintaining an epistemic identity. Because these meanings continue to thrive in modern discourse, attention to this history helped to resolve ruptures in meaning encountered in these discussions, making visible the particular ideologies managers brought to bear in making sense of their own experiences.

Mobilizing this framework, in addition to providing improved lines of sight into the worlds of our participants, allowed us as researchers to reflect on our own positions within fields of contestation. This reflexivity brought into clearer view the values at stake in a commercial and technological project with distinct ethical and political dimensions. Reframing the interests of disparate stakeholders—including managers, students, the surveilled public, and our team members—using a single set of terms in turn opened the

possibility of enabling those interests to be evaluated, discussed, and balanced or differentially advanced in a more coherent way.

The data analyzed here arguably also demonstrate a bottom-up, phenomenological account making visible the structural process of interpellation described by Louis Althusser. In these cases, interpellation of individuals by competing ideologies within a society could be seen to give rise to dissonance among 'commonsense' interpretations of freedom. Recognizing interpellation as a key process in social reproduction, the consequence of the director's assertions about surveillance technology enhancing freedom can be understood more clearly as well. In his puzzling statement, it could be argued that he both borrowed from dominant discourse and, as a leader in his community and his field, contributed to and reinforced that discourse. Much as the director imagined a future in which surveillant school structures might call out to would-be criminals, the director himself has already been hailed by a particular ideology of freedom. Seeing the director's statements as both drawing on and reproducing this ideology of freedom-through-surveillance can be seen as signal of an emerging form of justification of not just the sustainment of existing regimes of surveillance, but expansion of the scope of surveillant enclosure.

Recognizing articulations of common sense as statements of ideology—representations of imagined relations to material conditions of reality and assemblages of beliefs and knowledges situated in the identity of subjects—allows those statements to be evaluated in the context of popular discourse, and as sites of historical contention and contestation. In addition to providing practical assistance in resolving ruptures of meaning arising among participants and researchers in qualitative research, this framing additionally allows those statements to be analyzed at a structural level. As examples of the process of interpellation, whereby individuals are made subjects through their recognition of their own identity in ideology, these statements can be read as moments of cultural reproduction, drawing on and reproducing narratives that support existing social phenomena, in this case he phenomenon of surveillance. The ideology expressed in the director's statements can in particular be seen as a signal of an emerging rhetoric justifying intensification of surveillant practices in the name of a new form of freedom.

While this approach to analysis proved particularly well-suited to making sense of interview data, which consist largely of knowledge claims, Althusser emphasizes that ideology is manifested in practices and acts, not just narratives. This analysis suggests that much more investigation is warranted in making sense of the worlds of those involved in administering surveillant systems, especially as the systems of surveillance continue to grow, align and connect, extending the lines of sight of the apparatuses power.

Mike Griffin is a user researcher working on special projects at Amazon. With a background in design and social science, he has engaged in early-phase development of technology products in a wide range of situations.

Acknowledgments – I would like to express my appreciation for the thoughtful comments and support provided by Tiffany Romain and Jamie Sherman in their curation of this paper and the session of which it was a part. Disclaimer: The work presented in this paper has no connection with Amazon Corporate LLC, or related companies. Further, any opinions expressed here are solely those of the author.

REFERENCES CITED

Althusser, Louis
1971 Ideology and Ideological State Apparatuses (Notes towards an Investigation). Lenin and Philosophy and Other Essays: 121–173.

Andrejevic, Mark
2002 The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure. Critical Studies in Media Communication 19(2): 230–248.

Ball, Kirstie S.
2001 Situating Workplace Surveillance: Ethics and Computer Based Performance Monitoring. Ethics and Information Technology 3(3). Kluwer Academic Publishers: 209–221.

Boyd, Danah
2014 It's Complicated: The Social Lives of Networked Teens. It'S Complicated: The Social Lives of Networked Teens: 296.

Calhoun, John C.
1857 The Works of John C. Calhoun. Richard K. Crallé, ed. New York, D. Appleton.

Casey, Catherine
1995 Work, Self, and Society : After Industrialism. Routledge.

Cefkin, Melissa, Obinna Anya, and Robert Moore
2014 A Perfect Storm? Reimagining Work in the Era of the End of the Job. Ethnographic Praxis in Industry Conference Proceedings 2014(1): 3–19.

Crawford, Kate
2014 Big Data Anxieties: From Squeaky Dolphin to Normcore. *In* Proceedings of the Ethnographic Praxis in Industry Conference (EPIC).

D. Haggerty, Richard V. Ericson, Kevin
2000 The Surveillant Assemblage. British Journal of Sociology 51(4): 605–622.

Davis, Mike
2006 City of Quartz : Excavating the Future in Los Angeles. Verso.

Dinev, Tamara
2008 Internet Users' Beliefs about Government Surveillance—The Role of Social Awareness and Internet Literacy. *In* Proceedings of the 41st Hawaii International Conference on System Sciences P. 275. IEEE.

Duhigg, Charles
2012 How Companies Learn Your Secrets - The New York Times. The New York Times. http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?mcubz=0, accessed September 13, 2017.

Fitzhugh, George
1857 The Blessings of Slavery. *In* Cannibals All.

Foner, Eric
1999 The Story of American Freedom. 1st edition. W.W. Norton.

Graeber, David
2013 On the Phenomenon of Bullshit Jobs. Strike! Magazine.

Green, Nicola, and Nils Zurawski
2015 Surveillance and Ethnography: Researching Surveillance as Everyday Life. Surveillance and Society 13(1): 27–43.

Gregg, Melissa
2013 Work's Intimacy. John Wiley & Sons.

Gutfeld, Greg
2017 Gutfeld: The Importance of Security and Surveillance. Fox News, June 7. http://www.foxnews.com/transcript/2017/06/07/gutfeld-importance-security-and-surveillance.html, accessed September 12, 2017.

Hannah, Matthew G.
2010 (Mis)adventures in Rumsfeld Space. GeoJournal 75(4). Springer: 397–406.

Hill, Kashmir
2012 How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/amp/, accessed September 13, 2017.

Hochschild, Arlie Russell, and Anne Machung
2012 The Second Shift : Working Parents and the Revolution at Home.

Hong, Sun Ha
2017 Criticising Surveillance and Surveillance Article Critique: Why Privacy and Humanism Are Necessary but Insufficient. Surveillance and Society 15(2): 187–203.

Irwin, Alan, and Mike Michael
2003 Science, Social Theory and Public Knowledge. Berkshire England: Open University Press.

Lee, Ashlin
2015 Linking Surveillance Experiences to Social Patterns Using Ethno-Epistemic Assemblages. Surveillance and Society 13(3–4): 385–399.

Lyon, David
2001 Surveillance Society: Monitoring Everyday Life. Society. Open University Press.

Madden, Mary, and Lee Rainie
2015 Americans' Attitudes about Privacy, Security and Surveillance. Pew Research Center: 47. www.pewresearch.org.

Mech, Gary
2006 Access Control: Risk Complexities – Lessons for Everyone. http://www.securitymagazine.com/articles/78220-access-control-risk-complexities-lessons-for-everyone-1, accessed September 12, 2017.

Nippert-Eng, Christena E.
2010 Islands of Privacy. University of Chicago Press.

Piatetsky, Gregory
2014 Did Target Really Predict a Teen's Pregnancy? The Inside Story. KD Nuggets News. http://www.kdnuggets.com/2014/05/target-predict-teen-pregnancy-inside-story.html, accessed September 13, 2017.

Smith, Gavin J. D.
2015 Opening the Black Box : The Work of Watching. Routledge.

Stewart, Matthew
2011 The Management Myth. The Atlantic: 1–10. https://www.theatlantic.com/magazine/archive/2006/06/the-management-myth/304883/, accessed September 13, 2017.

Watson, Hayley, Rachel L. Finn, and David Barnard-Wills
2017 A Gap in the Market: The Conceptualisation of Surveillance, Security, Privacy and Trust in Public Opinion Surveys. Surveillance and Society 15(2): 269–285.

Wood, David Murakami, Charles Raab, Nicola Green, and Jason Pridmore
2006 A Report on the Surveillance Society. Polity 70(September): 102.